The Hong Kong Polytechnic University

Department of Computing

An Approach to the Usability Evaluation of the Human-computer Interaction of a Heterogeneous Safety-critical Complex Socio-technical System

TUNG Yip Wai

A thesis submitted in partial fulfillment of
the requirements for the degree of

Doctor of Philosophy

August 2011

CERTIFICATE OF ORIGINALITY

I hereby declare that this thesis is my own work and that, to the best of my knowledge and belief, it reproduces no material previously published or written, nor material that has been accepted for the award of any other degree or diploma, except where due acknowledgement has been made in the text.

_____ (Signed)

Tung Yip Wai

_____ (Name of student)

Abstract

In this thesis a Usability Evaluation Approach (UEA) is presented. The purpose of UEA is to analyze and evaluate the human-computer interaction (HCI) design for a heterogeneous safety-critical complex socio-technical (CST) system.

Heterogeneous safety-critical CST systems play an important part in the operations of socially important infrastructure, such as a mass-transit railway system. CST systems mostly consist of heterogeneous domain specific systems, mainly due to the enormous scale of complexity and other commercial considerations. A CST system typically operates in an interactive environment with safety-critical context. Safety is a property of a system that it will not endanger human life or the environment; safety-critical context assures the safety of equipment within the system is demonstrated. Usability is defined as the extent to which a product can be used by specific users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use. In the context of a heterogeneous safety-critical CST system, operability is defined as the ability of human operators to cope with various operational conditions (normal and emergency) without endangering the safety of the system when working together as a unified system; this definition implies the conformance of safety and usability requirements. Compliance to operability is happening to be a common criterion for CST system certification. With few exceptions, the design of individual domain specific systems is aimed to comply with technology-driven functional requirements; HCI of each domain specific system may well satisfy its own design guidelines and usability criteria, but there is no guarantee they can meet the

overall operability requirements when working together as a unified CST system.

UEA aims to facilitate HCI experts, system operators and safety specialists to analyze HCI requirements and formulate evaluation criteria for heterogeneous HCI design. By discovering interaction problems, UEA seeks to identify design aspects that can be improved, to set priorities, and guidance for how to make changes to a design that confirms the coherence of heterogeneous HCI. UEA extends the usage of scenario concept from the Usability Engineering and further considers human factors and situation awareness perspectives, to create a Unified HCI Requirements Analysis Framework (UHRAF), which generates Problem Scenarios, Network of Scenarios and associated Interaction Models for requirements analysis, and a Safety and Usability Model (SUM) as evaluation criteria, for which the heterogeneous HCI are assessed for compliance to operability. UEA addresses the heterogeneous HCI from three major Building Blocks: (i) Characteristics of Work Environment; (ii) Human Performance and Hazard; and (iii) Cognitive Characteristics of Human Operators. Each Building Block consists of aspects for evaluation criteria from safety and usability perspectives. The benefit of UEA is that it does not prescribe specific analysis tools; instead it enables common analysis tools to be deployed for analysis and evaluation.

A usability test is illustrated to analyze HCI requirements and assess the design of heterogeneous HCI for the control room of a mass-transit railway system. The results suggest that UEA is capable of analyzing and evaluating heterogeneous HCI issues in complex environment.

Publications Arising from the Thesis

TUNG, Y.W. (2008).
Decision-support Tool for Tunnel Train-fire Scenario, MTRC Lok Ma Chau (LMC) Spur Line (Hong Kong). In *Proceedings of the International Conference on Railway Engineering,* 2008, pp213-128.

TUNG, Y.W. AND CHAN, K. C. C. (2010).
A Unified Human-Computer Interaction Requirements Analysis Framework for Complex Socio-technical Systems. *International Journal of Human-Computer Interaction, 26 (1), 1-21, 2010.*

Acknowledgements

I would like to take this opportunity to express my sincere gratitude to my supervisor, Professor Keith Chan, for his support and guidance throughout my study in the past years. More importantly, his tolerance and acceptance to students with full-time work, like myself, is much appreciated. Without such kind consideration, the thesis would not be able to be completed.

I would also like to acknowledge the information and supports provided by MTR Corporation Limited for the development of this thesis.

Lastly, I must thank my wife Meran, two daughters Janice and Jacqueline, for their understanding and support for the completion of the thesis.

Table of Contents

CERTIFICATE OF ORIGINALITY ..... **I**
Abstract ..... **II**
Publications Arising from the Thesis ..... **IV**
Acknowledgements ..... **V**
Table of Contents ..... **VI**
List of Figures ..... **IX**
List of Tables ..... **XI**
Abbreviations ..... **XII**
Chapter 1 Introduction and Motivation **1**
1.1 Overview 2
1.2 Issues of HCI of Heterogeneous Safety-critical CST Systems 7
1.3 Motivation 10
1.4 Research Statement of Problem 11
1.5 Research Focus and Approach 14
1.6 Research Contribution 16
1.7 Outline of the Thesis 16
Chapter 2 Background and Related Work **18**
2.1 Human-computer Interaction (HCI) 19
2.1.1 Human-computer Interaction versus User Interface 19
2.1.2 Cognitive Psychological Framework and Mental Model 22
2.1.3 Distributed Cognition 26
2.1.4 HCI Modeling 29
2.1.5 Usability – Evaluation of HCI 30
2.1.6 Situation Awareness 38
2.1.7 Safety Aspects of HCI in CST Systems 41
2.2 HCI Development Methodologies 44
2.2.1 Definition of User 46

2.2.2 Context Analysis 49
2.2.3 Task Analysis 50
2.2.4 Scenario-based Analysis 54
2.3 Summary Remarks 55
2.3.1 Underlying Paradigm 56
2.3.2 Open Issues 57
2.3.3 Requirements and Suggestions 58
Chapter 3 Operational Perspective of Heterogeneous Safety-critical CST Systems 60
3.1 Complex Socio-technical System 62
3.2 Operational Processes of Heterogeneous Safety-critical CST System 67
3.3 Human Operators, System Operability and HCI in Heterogeneous Safety-critical CST Systems 71
3.4 Mass-transit Railway System 75
Chapter 4 Methodology for Developing the Usability Evaluation Approach 80
4.1 Overview 82
4.2 Unified HCI Requirements Analysis Framework 85
4.2.1 Scenario-based Approach of UHRAF 86
4.2.2 Typical HCI Model of Heterogeneous Safety-critical CST System 90
4.2.3 Processes of UHRAF 94
4.3 Safety and Usability Model (SUM) 101
4.3.1 Characteristics of Work Environment 102
4.3.2 Human Performance and Hazard 105
4.3.3 Cognitive Characteristics of Human Operators 109
4.3.4 Safety and Usability Assessment Process 113
4.4 Summary Remark 115
Chapter 5 Application of the Usability Evaluation Approach 117
5.1 Overview of the Operational Environment 118

5.2 Heterogeneous HCI Design Problem 121
5.2.1 Tunnel Ventilation and Its Design Concept 121
5.2.2 TVS Emergency Modes 123
5.2.3 Train Control System and Monitoring of Train Position ... 126
5.2.4 Integrated Control and Communications System 128
5.2.5 HCI Design Issues of Heterogeneous Domain Specific Systems 131
5.3 Application of the Usability Evaluation Approach 133
5.3.1 Operational Scenario Creation Process 134
5.3.2 Interaction Modeling Process 139
5.3.3 Safety and Usability Assessment Process 143
5.4 Summary Remark 155
Chapter 6 Assessment of the Usability Evaluation Approach 159
6.1 Approaches of Assessment 160
6.2 Achievement of the Research Statement of Problem 161
6.3 Applicability, Acceptability and Effectiveness 163
6.3.1 Applicability 163
6.3.2 Acceptability 165
6.3.3 Effectiveness 167
6.4 Accuracy, Constraints and Limitation 171
6.5 Summary Remark 173
6.5.1 Generality of UEA 174
6.5.2 Time and Cost Requirements of Using UEA 175
6.5.3 Criteria for Resolving Conflicting Views and Defining Success of the System 176
6.5.4 Ramifications and Challenges of Using UEA 178
Chapter 7 Conclusions and Suggestions for Future Research 180
7.1 Conclusions 180
7.2 Suggestions for Future Research 182
References 185

List of Figures

Figure 1-1: Focus of the thesis – the Usability Evaluation Approach 15
Figure 2-1: Fundamental building blocks of HCI 20
Figure 2-2: An overview of broad HCI issues [Zhang & Galleta, 2006] .. 22
Figure 2-3: An interaction model within a multi-agent environment 28
Figure 2-4: Norman's Action Cycle 32
Figure 2-5: Overview of the Scenario-based Usability Engineering Framework proposed by [Rosson & Carroll, 2002] 34
Figure 2-6: Scenario elements in a diagrammatic representation of a mass-transit railway control room 36
Figure 2-7: Model of Situation Awareness [Endsley, 1996] 39
Figure 2-8: Details of the V-Model [Storey, 1996] 45
Figure 2-9: Hierarchy of users in mass-transit railway system 47
Figure 3-1: A social's perspective of a CST system 62
Figure 3-2: The interaction relationship within a heterogeneous safety-critical CST system 69
Figure 3-3: The concept of system operability from the statutory authorities' perspective 74
Figure 3-4: Environment of a mass-transit railway system 78
Figure 3-5: Heterogeneous domain specific systems in a typical mass-transit railway system 79
Figure 4-1: Basic concept of the methodology for developing UEA 83
Figure 4-2: Skeleton of the Unified HCI Requirements Analysis Framework (UHRAF) 90
Figure 4-3: A typical HCI model for a heterogeneous safety-critical CST system 91
Figure 4-4: Interaction model within the operational environment 92
Figure 4-5: Shared operator knowledge 93

Figure 4-6: Implementation processes of UHRAF 94
Figure 4-7: Scenario Identification task 96
Figure 4-8: Schema of Scenario Description 97
Figure 4-9: An example of signs in the HCI display of a mass-transit railway system 105
Figure 4-10: Safety and Usability Assessment process 113
Figure 5-1: Layout of the control room of MTR East Rail Line 120
Figure 5-2: Layout of TVS zones in the tunnels of LMC Spur Line 122
Figure 5-3: TCS HCI display showing the real time signaling and train information 128
Figure 5-4: ICCS TVS HCI display showing a list of emergency modes for up tunnel 130
Figure 5-5: ICCS TVS HCI display showing the real time status of TVS equipment in SSVB 130
Figure 5-6: ICCS TVS HCI display showing the real time status of TVS equipment in CTVB 131
Figure 5-7: Network of Scenarios for the Problem Scenario: handling of tunnel train-fire incident 137
Figure 5-8: TVS overview display 151
Figure 5-9: TVS emergency mode reference overview display 152
Figure 5-10: Track Circuit Box 153
Figure 5-11: Example showing an incident train stalled in the tunnel 154
Figure 5-12: Details of TVS Emergency Mode F3 155

List of Tables

Table 2-1: Summary of the definition of usability 31

Table 2-2: Scenario elements of user interaction scenarios in a mass-transit railway control room 34

Table 4-1: Definition of Scenario Elements 98

Table 4-2: Definition of Level-1 Interaction of the Interaction Model .. 100

Table 4-3: Definition of Level-2 Interaction of the Interaction Model .. 101

Table 4-4: Safety and Usability Matrix 114

Table 5-1: TVS Zone description for the LMC tunnels (both up tunnel and down tunnel) 123

Table 5-2: Emergency modes for the tunnels of LMC Spur Line 124

Table 5-3: Summary information of the Operational Scenario Creation process 134

Table 5-4: Scenario Description for the scenario: selection of TVS emergency mode 138

Table 5-5: Summary information of the Interaction Modeling process . 140

Table 5-6: Result generated from Level-1 Interaction Model 141

Table 5-7: Result generated from Level-2 Interaction Model 142

Table 5-8: Summary of assessment (***Italic Bold*** represents deficiency conditions) 148

Table 6-1: Comparison of HCI design based on UEA approach and conventional approach 169

Abbreviations

ATO	Automatic Train Operations
ATP	Automatic Train Protection
CCTV	Closed-circuit Television System
CERN	European Organization for Nuclear Research
CO	Control Officer (one of the operators in the control room)
CSCW	Computer Supported Cooperative Work
CST	Complex Socio-technical
DC	Distributed Cognition
E&M	Electrical & Mechanical
ECO	Electrical Control Officer (one of the operators in the control room)
EN	European Standard
FMEA	Failure Modes and Effects Analysis
FRC	Fault Report Center
GOMS	Goal, Operator, Method, Selection
GTA	Groupware Task Analysis
HAZOP	Hazard & Operability Analysis
HCD	Human-centered Design
HCI	Human-computer Interaction
HKSAR	Hong Kong Special Administrative Region
HRA	Human Reliability Analysis
HTA	Hierarchical Task Analysis
ICCS	Integrated Control and Communications System
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
LLA	Long Line Announcer (one of the operators in the control room)

LMC	Lok Ma Chau
MHP	Model Human Processor
PA	Public Announcement System
PI	Passenger Information System
PLC	Programmable Logic Controller
PRC	People's Republic of China
SBD	Scenario-based Design
SCADA	Supervisory Control And Data Acquisition
SCRAM	Scenario-based Requirement Analysis Method
SIL	Safety Integrity Level
SOP	Standard Operating Procedures
STC	Senior Train Controller (one of the operators in the control room)
SUM	Safety and Usability Model
SWEBOK	Software Engineering Body of Knowledge
TA	Task Analysis
TC	Train Controller (one of the operators in the control room)
TCS	Train Control System
THERP	Technique for Human Error Rate Prediction
TPC&MS	Traction Power Control and Monitoring System
TRN	Train Run Number
TVS	Tunnel Ventilation System
UCD	User-centered Design
UE	Usability Engineering
UEA	Usability Evaluation Approach
UHRAF	Unified HCI Requirements Analysis Framework
UML	Unified Modeling Language

Chapter 1

Introduction and Motivation

We live in a complex society. This society consists of a variety of large-scale, complex socio-technical (CST) systems, which are ubiquitously provided in our society to facilitate our daily life. The term "complex socio-technical systems" was originally coined by [Emery and Trist, 1960] to describe systems that involve a complex interaction between humans, machines and the environmental aspects of the work system. A complex socio-technical system, which associates with safety-critical context, is named as a safety-critical CST system. Safety is a property of a system that it will not endanger human life or the environment [Storey, 1996]; safety-critical context assures the safety of equipment within the system is demonstrated. Furthermore, safety-critical CST systems in today's real world applications are mostly packaged with heterogeneity of numerous domain specific systems, mainly due to the enormous scale of system complexity and other commercial considerations. In this thesis a safety-critical CST system with heterogeneity of domain specific systems is named as a heterogeneous safety-critical CST system; common examples are air traffic control systems, power generation & energy management systems and mass-transit railway systems.

These systems, should they go wrong, due to either system malfunctions or operational errors, could lead to various degrees of social impacts and, more seriously, endanger the safety of the personnel who operate the systems, the general public and our environment. For instance, in a mass-transit railway system (a typical heterogeneous safety-critical CST system) if the safety-

critical signaling system is failed, the consequence could jeopardize the safety of the passengers. Today's heterogeneous safety-critical CST systems are heavily equipped with sophisticated computing & automation devices and human-computer interaction (HCI) facilities and artifacts; the primary objective is to automate a large number of control processes and monitoring functions within the system and thus to deal efficiently with it. The pervasiveness of and dependency on heterogeneous safety-critical CST systems in our society impose a significant responsibility on the designers and operators of such systems. Ironically, the more powerful technologies are available, the more complex are the design and operations of the systems.

1.1 Overview

Heterogeneous safety-critical CST systems are vital to people daily life and therefore must be designed and operated robustly against system abnormality. However, designing safety-critical CST systems is a challenging task, in part because such systems are concerned with complex problems, uncertainty, incomplete and diverse sources of information, multiple logical and situational factors, and with competing and sometime contradicting demands from numerous stakeholders [Mirel, 2004], but, importantly, also because these systems typically make use of a variety of heterogeneous domain specific systems. With few exceptions, current design solutions for heterogeneous safety-critical CST systems by taking a technology-driven design approach, in which specific functionalities are provided by heterogeneous domain specific systems; for example, a safety-critical CST system for mass-transit railway operations typically consists of a signaling system, tunnel ventilation control system and radio communication system within a railway system, to name but a few. More importantly, despite the technological development in computing, communications and automation have significant advancements in recent years, and full scale automation in a heterogeneous safety-critical CST

system is universally implemented, they fail to suitably enhance the operational paradigm of heterogeneous safety-critical CST systems, for which human operators continue to play a vital role in the system supervisory loop [Riera, 2001]. The HCI associated with domain specific functionalities may not necessarily be coherent or mutually consistent, which are attributable to the deployment of heterogeneous domain specific systems. Usability, the extent to which a product can be used by specific users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use [ISO 9241-11, 1998], becomes a design challenge for a heterogeneous safety-critical CST system. Furthermore, from the perspective of regulatory authorities that certify the safety-critical CST systems, the operability of a safety-critical CST system becomes the most important aspect that regulatory authorities are focusing on. In the context of a heterogeneous safety-critical CST system, operability is defined as the ability of human operators to cope with various operational conditions (normal and emergency) without endangering the safety of the system and its stakeholders when working together as a unified system [Bourne & Carey, 2001]. According to this definition, safety and usability are the fundamental constituents of operability. Compliance to operability is happening to be a common criterion for system certification.

To comply with operability, the achievement of safety and usability is essential. However, in a typical heterogeneous safety-critical CST system that consists of various domain specific systems, each domain specific system has its unique concept and implementation of HCI; therefore human operators are required to interact with numerous HCI facilities and artifacts in a heterogeneous environment. Two design questions become apparent: (1) how the HCI of heterogeneous domain specific systems can be designed with unified concept that allows human operators to possess coherent understanding of the system operation; and (2) how the HCI design can be

evaluated with respective to the operability. These questions become a critical design issue of a heterogeneous safety-critical CST system.

Ultimately, all of these problems fall within the purview of requirements analysis, yet the HCI analysis of heterogeneous safety-critical CST systems remains to date a neglected area of study, even though many problems in requirements engineering originate from complex social problems [Sutcliffe & Minocha, 1999]. Despite methodologies or models are available for the analysis of CST systems requirements, the very complex task of analyzing and specifying requirements for HCI continues to depend on individual analysts' interpretations of domain knowledge. In short, current approaches to HCI requirements analysis and evaluation methods do not adequately address issues of operability. This leaves legacy of inconsistent HCI implementations, which include divided representations, information gaps, and incoherence of concepts, exists between heterogeneous domain specific systems within a safety-critical CST system. This situation is not only inefficient but adds an extra cognitive burden to operator tasks, giving rise to ambiguity and misinterpretation and potentially affecting the overall performance of operators and, ultimately, system safety and usability.

Furthermore, the achievement of safety and usability for safety-critical CST systems through system reliability and availability continues to be a common misconception amongst the systems' operators, maintainers and designers. Almost all safety-critical CST systems are built with hardware redundancy to achieve high reliability and availability, so that if one should fail another can take over. However, this form of redundancy only addresses a portion of the problem; it is because the safety and usability are not covered by any of the redundancy provision. Reliability is operation in conformity with specification, and the specification may not have taken account of all possible safety implications [Redmill & Rajan, 1997]; similar situation also applies to usability. In many occasions, the failure of

hardware components only constitutes a small percentage of the total system problems. Duplicated hardware systems running identical software will not be able to provide protection against operational errors due to poor usability of the HCI and lack of human-centered safety design consideration. Achieving safe and usable performance, therefore, requires explicit attention to be given to the human requirements within the system design. Unfortunately, the operational reliability of human operators has not drawn adequate attention and is still considered as one of the weakest components in CST systems [Piccini, 2002]. The design collaboration of HCI between heterogeneous domain specific systems within a safety-critical CST system is nevertheless seldom exercised during the system design stage. By the time when problematic system-operator interaction issues are identified, the respective heterogeneous domain specific systems' HCI and information hierarchy have already been designed and it is too costly and too late to alter it. The price for this is that the greatest asset of human operators – adaptability is sacrificed to facilitate the incoherence of interactions between heterogeneous domain specific systems.

A fundamental step in the design of human-system collaboration is to acquire a thorough understanding of the complexity of the work for which human operators need to perform. Task Analysis [Diaper, 2004] is one of the common approaches to, as the name suggests, analyzing work arrangements in a complex system environment. It enables rigorous and structured characterizations of user activities and also provides a framework for the investigation of existing practices [Crystal & Ellington, 2004]. The Scenario-based Requirement Analysis Method (SCRAM) [Sutcliffe et al., 1998] is another approach to analyzing the system requirements. Scenarios, instances of actual user experience with a system, are captured to describe the behavior of system operations. From these, scenario-based models are built to mimic the system environment, which can then be investigated for connections and dependencies between the system and its environment.

These approaches provide essential methodologies for analyzing generic HCI requirements; however they do not address the coherence of multiple HCI associated with domain specific systems in a heterogeneous safety-critical CST system. Similarly, common usability evaluation methods are abundant but few offers approach to tackle usability issues raise from a heterogeneous environment. A basic requirement of achieving operability is to resolve the HCI design problems associated with heterogeneous domain specific systems, so as to create a unified operational environment. Beside, even thought a number of HCI development methods exist and many suggested practices of coupling these methods with software development processes, the applications of these methods continue to be an afterthought in the production of software; there is little integrated approach between software engineering processes and HCI development methods [Jerome & Kazman, 2005].

We argue that the HCI issues of a heterogeneous safety-critical CST system need to be fully analyzed and captured from system safety as well as usability perspectives; in addition, usability evaluation criteria need to be established for the heterogeneous HCI designs, so as to eliminate the mismatch of design aspects and minimize the system-operator interaction gap amongst the heterogeneous domain specific systems. To tackle these problems, this thesis proposes a Usability Evaluation Approach (UEA) as a methodological approach to resolve the problem. UEA develops a Unified HCI Requirements Analysis Framework (UHRAF), which extends the usage of scenario concept from the Usability Engineering (UE) advocated by [Rosson & Carroll, 2002], to capture and analyze the requirements related to the design of HCI for heterogeneous domain specific systems within a safety-critical CST system; it also offers a Safety and Usability Model (SUM) to define the criteria for safety and usability, and to evaluate the safety and usability of HCI designed by heterogeneous domain specific systems, in accordance to the interaction requirements analyzed by UHRAF,

with the aim of optimizing the operability of a heterogeneous safety-critical CST system in a control room environment.

The thesis undertakes an applied approach to the HCI requirements and usability evaluation of mass-transit railway system – a typical heterogeneous safety-critical CST system, in considering a problem related to handling a railway tunnel train-fire incident scenario in the Lok Ma Chau (LMC) Spur Line Project in the Hong Kong Special Administrative Region (HKSAR) of the People's Republic of China (PRC). The majority of the research reported within this thesis was conducted in the railway's control room environment for which the heterogeneous HCI facilities are provided. This offered an exceptional opportunity to develop research activities in partnership with industrial users of the research products.

The rest of this chapter provides further context to the thesis, identifies the issues, states the problem statements, highlights the motivation of the research, describes the research approach and contribution, and outlines the structure of the remaining parts of the thesis.

1.2 Issues of HCI of Heterogeneous Safety-critical CST Systems

There are internationally accepted industrial system development standards, such as EN 50128 [CENELEC, 2001] and IEC 61508 [IEC, 1998], for electro-technical safety-related systems. For instance, IEC 61508 applies to safety-related systems when one or more of such systems incorporate electrical and/or electronic and/or programmable electronic devices [IEC, 2002]. These standards identify mandatory processes and outcomes for software design, implementation and testing for various situations defined under a Safety Integrity Level (SIL) scheme. In addition, there are a

number of methods, which have been applied in the industry to analyze the system, software and operational safety issues. These methods include risk assessment methods, such as Hazard & Operability Analysis (HAZOP) [McDermid & Pumfrey, 1994] & [Lawrence, 1995], and Failure Modes and Effects Analysis (FMEA) [Stamatis, 1995] and [Goddard et al., 2000] etc. But most of these methods are adapted for design orientation [Earthy, 1995], and focus on functional, hardware or software components and do not directly address the HCI issues [Hollnagel, 1993], [Storey, 1996] and [Palanque et al., 2004]. Relatively little work has dealt with the requirements of HCI issues for safety-critical CST systems except in the context of human reliability assessment [Hollnagel, 1998].

Furthermore, despite being compliant with international standards for the development of safety-critical CST systems is widely mandated, the software requirements have been repeatedly recognized to be the most problematic within the software development lifecycle [Lamsweerde, 2000]. These problems are primarily due to the fact that although what is being developed is highly interactive software with significant HCI components, most software engineering methodologies offer no mechanisms to explicitly and empirically identify and specify user needs and usability requirements. Even though most software projects start with some form of requirements analysis and specifications, but the initial requirements are not done well because those involved have inadequate understanding of the human factors that should be paramount in requirement analysis [Diaper & Sanger, 2006]. They also fail to test and validate requirements with end-users before, during and after the development. On the other hand, analysis methods offered by HCI experts and existing software engineering practice are often discordant. The report of Stone Man version of SWEBOK (Software Engineering Body of Knowledge) [SWEBOK, 2000] lists HCI and related knowledge as “related disciplines” in software engineering field; however the importance of HCI assigned is not proportional to the actual usage of

HCI in real life, especially in the safety-critical CST systems. The report regards all HCI aspects as relevant at the testing phase of software engineering only, which are treated as supplementary to other evaluation measures. The report also considers human factors input is only needed to verify that the look and feel of the user interface matches user needs and does not relate to requirements and design issues. As a result, the developed systems generally meet all functional requirements, and yet are not effective, efficient and satisfactory for use. The frequent situation where large numbers of requests to modify are made after the systems are deployed [Seffah & Gulliksen, 2005] can be attributed to such inadequate methodologies.

Human-centered Design (HCD) has been advocated as a way to resolve the usability issues for highly interactive systems. It is intended to tackle the software development from the users' perspective, i.e. it applies a user-driven rather than a technology-driven philosophy. In some respect, this is not surprising as usability engineering and software engineering share some common goals and techniques, yet they do have primary focuses [Seffah & Metzker, 2004]. Software development is driven by the specification of functional requirements and these requirements are tied to the system, which corresponds to the application itself; HCI is only one of the many components that have to meet the requirements. On the other hand, HCD is more concerned with the theme of quality of use, where the over-riding requirement is that users can perform tasks with the application. These two perspectives can have major impact on the software development process, in particular the requirements management and quality control activities [Seffah, Desmarais & Metzker, 2005]. The situation is even more complicated in a heterogeneous safety-critical CST system because in most cases domain specific systems within the CST system have their own functionality, and more importantly their unique approach to HCI design. This makes the achievement of system operability for a heterogeneous

safety-critical CST system a great challenge, and it is also difficult for system designers and relevant stakeholders to evaluate the HCI usability.

1.3 Motivation

CST systems satisfy people's social needs. A heterogeneous safety-critical CST system consists of numerous technological domain specific systems and applications; and if these go wrong there can be serious injury, loss of life and damage to the environment. In the past, these systems relied on electrical and mechanical components; the design properties and characteristics of which were well understood. Today, more and more heterogeneous safety-critical CST systems depend on computer-based systems and this has introduced numerous complexities which must be taken into account when designing and operating the systems. In particular, as they are currently presented, the complexities of modern computer-based system can outstrip the abilities of humans to manage them. Despite HCI research and usability studies are abundant, relatively little research work has been done on the particular requirements of heterogeneous HCI and usability issues in safety-critical CST systems. We argue that HCI is one of the most critical factors to the success of a heterogeneous safety-critical CST system. In addition, we regard the HCI as a realization of the entire system-operator interaction within the context of use. Therefore, this research is motivated by the importance of HCI in a heterogeneous complex system environment; and consequently the methodological approach to evaluate the HCI in order to ensure the safety is accomplished and usability is achieved, which imply the operability is demonstrated.

This thesis describes a methodological approach, the Usability Evaluation Approach (UEA), to support the safety and usability evaluation of HCI of a heterogeneous safety-critical system. UEA develops a Unified HCI Requirement Analysis Framework (UHRAF) and a Safety and Usability

Model (SUM); and is aimed to resolve the research statement of problem and the research questions as stated in *Section 1.4 – Research Statement of Problem* below. In the context of this thesis, we adopt the definition of "framework" previously defined by CERN (European Organization for Nuclear Research) Engineering Data Management Service, which stated that a framework is an extensible structure for describing a set of concepts, methods, technologies, and cultural changes necessary for a complete product design and manufacturing process. Framework products are most common in the area of electrical and electronic design. A framework provides the mechanism that guides users through a proper order of steps, applications, and data conversions via a common interface to the process being followed [CERN, 2006]. Although this definition of framework is based on the conventional design of electrical and electronic systems, today heterogeneous safety-critical CST systems involve many computing and communications technologies that are inherited from conventional electronic design. Therefore the definition of framework should equally apply to the development of HCI for such systems.

1.4 Research Statement of Problem

In the development of a heterogeneous safety-critical CST system it is common practice that major system designs and development of domain specific systems are completed independently before the HCI issues are collectively addressed and consolidated. This discordant between system development and HCI issues can lead to a failure of compliance to system operability and make the system unsafe and less usable. To resolve these issues, the HCI requirements for a heterogeneous safety-critical CST system must be fully analyzed and understood by system stakeholders before the system design is finalized. This thesis provides a methodological approach to resolve these issues by proposing a Usability Evaluation Approach (UEA) to tackle the problem. UEA offers a Unified HCI Requirements Analysis

Framework (UHRAF) for requirements analysis; and also a Safety and Usability Model (SUM) to define the criteria for safety and usability, and to evaluate the safety and usability of HCI designed by heterogeneous domain specific systems, in accordance to the interaction requirements analyzed by UHRAF, with the aim of optimizing the operability of a heterogeneous safety-critical CST system in a control room environment. In addition, UEA forms the basis for integrating the HCI development process into the software engineering development process for a heterogeneous safety-critical CST system.

The research statement of problem for this thesis is formulated as follows:

A heterogeneous safety-critical CST system is built by integrating a set of domain specific systems, which are constituted structurally by objects, human operators, artifacts, physical surroundings, data, processes and operating rules and procedures. The heterogeneity of HCI in a heterogeneous safety-critical CST system environment involves a variety of complex human activities with safety contexts. However, the concurrent development of domain specific systems in a heterogeneous safety-critical CST system does not address the coherency and compatibility issues of HCI requirements from a unified operational perspective and it does not describe the overall users' activities and associated system-operator interaction. Consequently the safety and usability of the system will be jeopardized. Therefore new analysis and evaluation approach needs to be explored to address the challenges faced by the development of HCI in such environment.

To meet the research objective of resolving the research statement of problem, the operators of a heterogeneous safety-critical CST system must be positioned in the center of the analysis and evaluation approach. From the system operator's perspective the usability of a system is the realization

of its HCI; therefore the ultimate system usability is determined by the operators' acceptability of the HCI. The issues are to determine how to achieve the research objective and what kinds of analysis activities are needed to achieve the research objective. This raises the following research question:

Research question 1 – How can we formulate the requirements analysis activities to facilitate the design of HCI from a number of domain specific systems in a heterogeneous safety-critical CST system?

The observations presented in the above sections indicate that current system development approaches fail to address the HCI issues of a heterogeneous safety-critical CST system. With few exceptions, HCI issues are considered independently for each domain specific system. In reality, most heterogeneous safety-critical CST system developments are under time pressure and cost constraints and it is almost impossible to modify the software to cater any lately identified HCI requirements, as this would seriously impact the completion of project. An effective analysis of HCI requirements will enable designers to address the system-operator interaction issues at the early stage of the software design phase. This leads to the second research question, as follows:

Research question 2 – How can the heterogeneous HCI requirements be represented explicitly from the operator's perspective of a unified system operation?

Finally, it is important to ensure the results from the first two research questions provide a validated solution that satisfies the research objective. This leads to the final research question:

Research question 3 – How to validate the HCI analysis result and its representation can provide a solution towards the achievement of safety and usability for a heterogeneous safety-critical CST system?

Underlying the research objective and research questions is a paradigm that considers the HCI of a heterogeneous safety-critical CST system to be paramount in the system operations.

1.5 Research Focus and Approach

This thesis examines the impact of the heterogeneity of HCI on the behaviors and cognitive characteristics of operators of a safety-critical CST system, and considers how these characteristics can be integrated into HCI requirement analysis process and evaluation criteria. The thesis develops a Usability Evaluation Approach (UEA), which has the following key features:

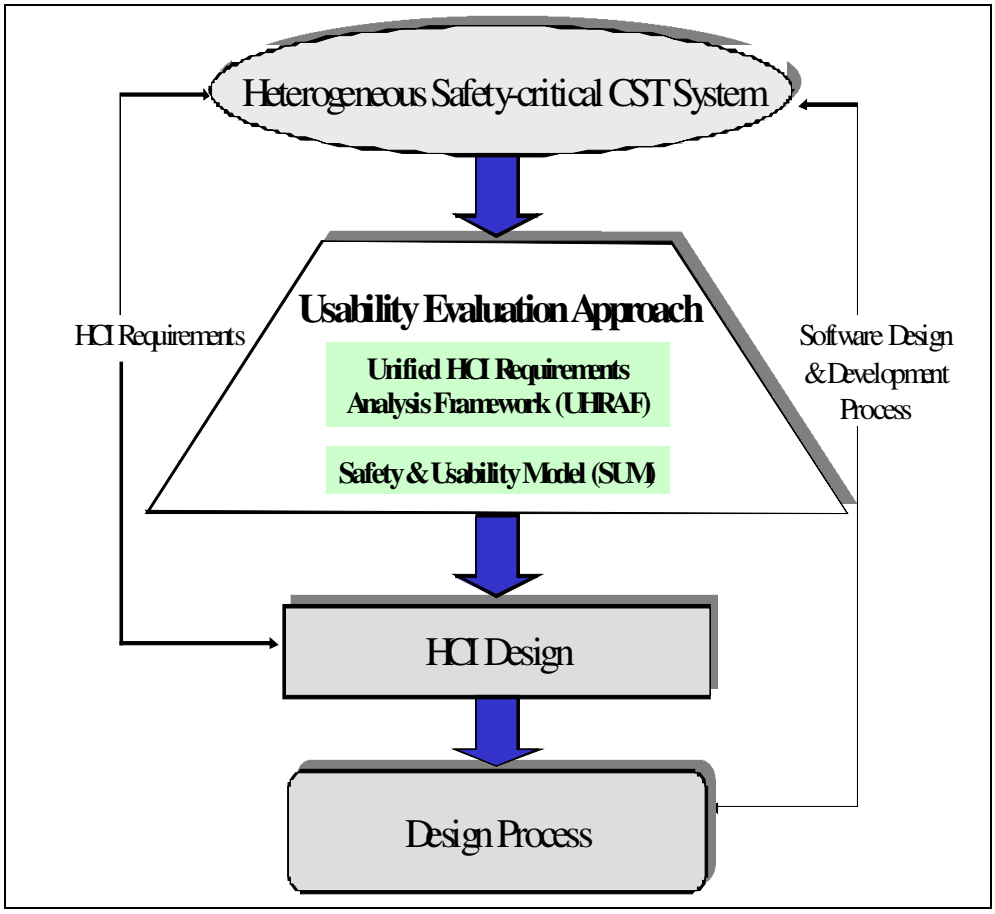
- To examine the orchestration of heterogeneous types of system-operator interaction; and based on the result, to identify the HCI requirements to support operator's tasks in spatial and temporal domains;
- To analyze the operational safety and incorporate the safety requirements into the HCI model;
- To model heterogeneous system-operator interactions in various level of abstraction of usage; and
- To establish the heterogeneous HCI evaluation criteria from a unified operational perspective.

The scope of the research focuses on the HCI issues, rather than the complete functional requirements of a safety-critical CST system. Figure 1-1 shows the focus of the thesis: the blocks "Heterogeneous Safety-critical CST System", "HCI Design" and "Design Processes" are external scopes to

this research. This thesis neither goes into the detailed functional aspects of a safety-critical CST system nor the CST system design processes.

The research uses a mass-transit railway system as a typical heterogeneous safety-critical CST for usability testing of its HCI design. UEA allows us to focus on the operational environment, the control room of the mass-transit railway, of a real heterogeneous safety-critical CST system, so that we can obtain a rich and detailed insight into the operational environment's actual context of use and its complex relationships and processes.

Figure 1-1: Focus of the thesis – the Usability Evaluation Approach



1.6 Research Contribution

The Usability Evaluation Approach (UEA) proposed in this thesis specifically aims to support and facilitate the systematic development of HCI of a heterogeneous safety-critical CST system by providing safety and usability evaluation from system operator's perspective. UEA developed from the research will provide a high level of utility for HCI design and allows designers to directly predict the outcomes of their designs on user performance variables under the specific environment. The contribution of this thesis enables system developers and relevant stakeholders to identify key interaction, safety, and usability issues that domain specific applications in a safety-critical CST system need to address. The ultimate goal is to involve HCI in optimizing the operability of a heterogeneous safety-critical CST system.

1.7 Outline of the Thesis

Chapter 2 – Background and Related Work provides an extensive review on the literature and material related to the HCI, usability and development methodologies of HCI.

Chapter 3 – Operational Perspective of Heterogeneous Safety-critical CST Systems describes the CST systems and the operational processes of a typical heterogeneous safety-critical CST system. The description mainly focuses on how human operators work in a control room environment with heterogeneous domain specific systems and the system operability requirements in such environment.

Chapter 4 – Methodology for Developing the Usability Evaluation Approach formulates the core conceptual development of the methodology

for UEA, its Unified HCI Requirements Analysis Framework (UHRAF) and Safety & Usability Model (SUM), and establishes their skeletons. This chapter also depicts the implementation of UEA and explains the processes developed for UHRAF and SUM.

Chapter 5 – Application of the Usability Evaluation Approach demonstrates the application of UEA to test an operational railway environment, which is a typical heterogeneous safety-critical CST system, to resolve a heterogeneous HCI issue – handling of tunnel train-fire incident scenario in a mass-transit railway system.

Chapter 6 – Assessment of the Usability Evaluation Approach assesses the applications of UEA with respect to the outcome of the actual implementation, and assesses the applicability, acceptability and effectiveness of UEA in practical and applied nature of the heterogeneous safety-critical CST environment. This chapter also reviews how well it meets the stated objectives; and the accuracy, constraints and limitation of UEA, based on its application demonstrated in the test scenario reported in the previous chapter.

Chapter 7 – Conclusions and Suggestions for Future Research concludes the research work presented in the thesis, examines its contribution, and suggests which directions the research work could take in the future.

Chapter 2

Background and Related Work

Regardless of application domains, the field of Human-computer Interaction (HCI) is concerned primarily with the design of a system that match the needs and capabilities of the people who interact with the system. The most noticeable deliverable of the HCI research is the design of the user-interface. However, a considerable amount of effort has been directed towards the design of the interactive systems in general, rather than just the user-interface. This approach to system design has originated from the cognitive science; and the shared interest of computer science and cognitive science was called Human-computer Interaction [Rosson & Carroll, 2002]. Usability, on the other hand, concerns with user experience of system usage; since users interact with the system through the HCI, consequently usability evaluation involves the assessment of the HCI. This thesis concerns with the development of an approach, which aims to analyze HCI requirements and evaluate the usability, for the development of heterogeneous safety-critical complex socio-technical (CST) systems. Before starting on the research work, it is necessary to clarify what are required. The purpose of this chapter is, therefore, to provide the background on the subjects and investigate what are the requirements that the proposed approach needs to satisfy. To do this, this chapter reviews some fundamental principles of HCI, its development methodologies and research issues.

2.1 Human-computer Interaction (HCI)

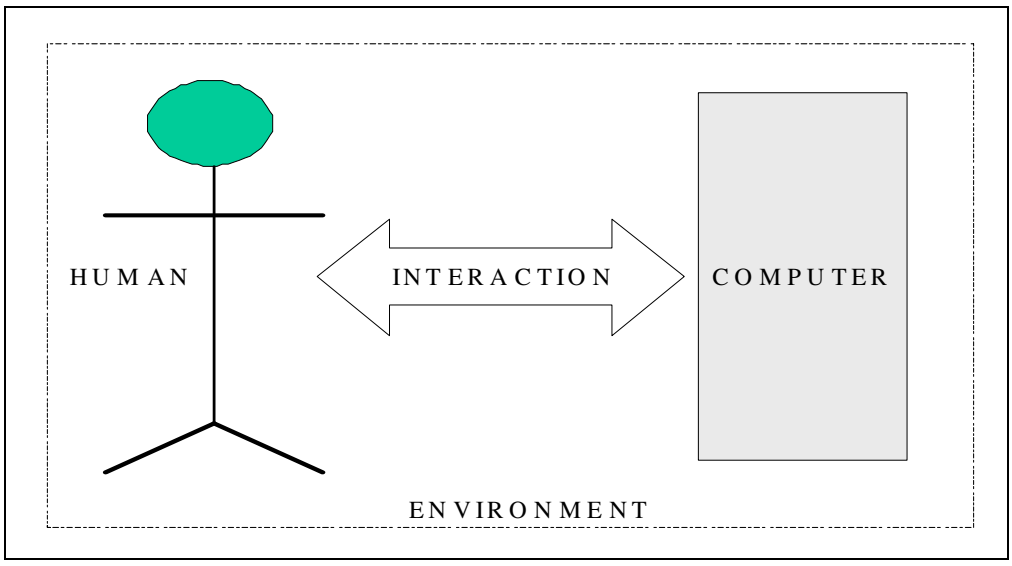
HCI consists of multi-discipline knowledge. It is emerging as a specialty, which concerns several knowledge domains and each with different emphasis. Computer science focuses on application designs and engineering of human interfaces. Psychology concentrates on the application of theories of cognitive processes and studies the empirical analysis of user behavior. Sociology and anthropology investigate the interactions between technology, work, and organization. Industrial design mainly develops interactive products [ACM, 1997]. The multi-discipline nature of HCI makes the terms and definitions used in the discipline confusing. It is mainly because different domain experts have different interpretations to the same term. Before we further review the related work, we clarify in the next section our interpretation of the terms within the context of this thesis.

2.1.1 Human-computer Interaction versus User Interface

The term "Human-computer Interaction" has not been widely used until approximately four decades ago. Summary reviews of the growth and evolution of the HCI can be found in [Shackel, 1997] and [Grudin, 2005]. Many people consider HCI concerns itself exclusively with the interface of a computer application, i.e. the windows, buttons, and graphics used to present the application. This view is formulated from the significant amount of early researches that focused on interface techniques and tools for interface design and implementation. In this thesis, however, we concur with Diaper's [Diaper, 2002] interpretation that the "I" in HCI stands for "Interaction", and not merely for "interface". Interaction is a form of communication, positing analyzes and perspectives far wider and richer than

concerns with the use of color or screen fonts. The interaction is concerned with a system composed of users and tools, integrating in the context that is both physical and social, with intentional manifest in the human's pursuit of goals [Dillon, 1997]. The reality is that HCI is evolved from a number of well-established disciplines. Ergonomic [Bridger, 2009], a study of the physical characteristics of machines and how people working on them, is one of the disciplines that has important influence to the development of HCI. As the computer became a form of machine, ergonomic on computer had started to draw attention from researchers [Shackel, 1959]. HCI is concerned with the entire system usage experience, not just the outside of it, simply because the whole application influences the use and usability, not just the interface at the outside of the application. The entire HCI can be viewed analytically using a basic model, illustrated in Figure 2-1, which consists of three fundamental building blocks: human, computer and the interaction between them. In addition, the environment that these building blocks situated is also an important factor, which can impact the over interaction performance.

Figure 2-1: Fundamental building blocks of HCI

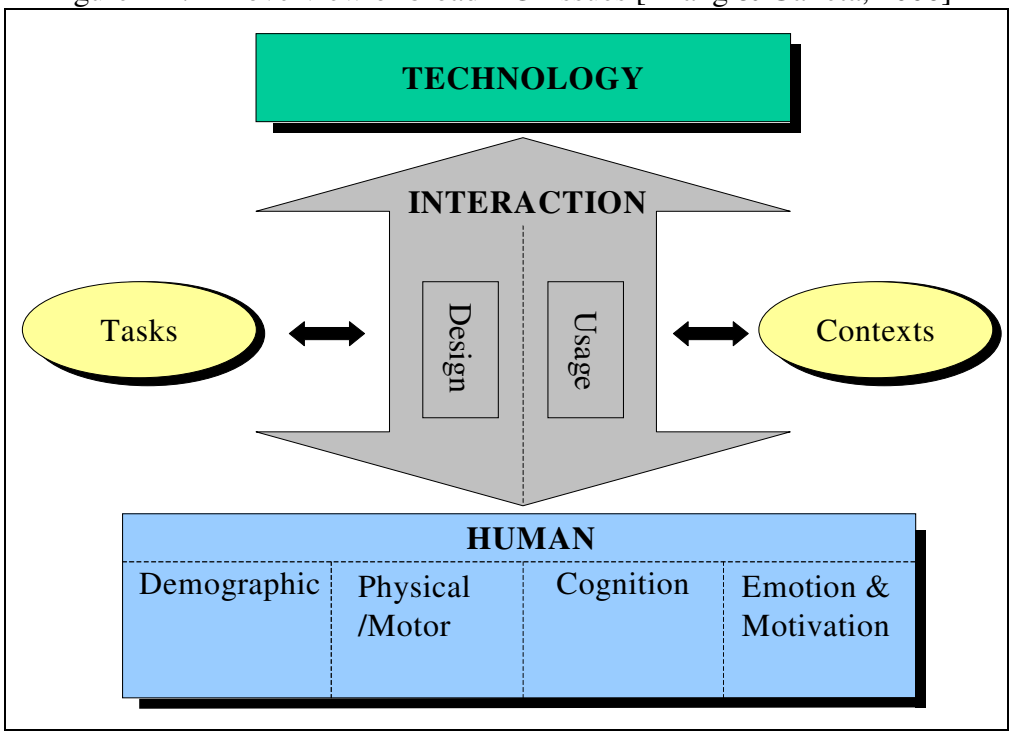


From this perspective, HCI involves the design, implementation, and evaluation of interactive systems in the context of the user's tasks and works [Dix et al., 2004]. This implies that the principles of HCI should be applied throughout the whole design cycle, from the earliest start of the design process. HCI is a science of design, it seeks to understand and support people interacting with and through technology. Much of the structure of HCI is derived from the technology, and many of the interventions must be made through the design of technology [Carroll, 1997].

[Zhang & Galleta, 2006] further expand the scope of HCI to cover the interaction between human and technology; they include demographics, physical or motor skills, cognitive issues and affective and motivational aspects on the human side. They also define the technology to include hardware, software, applications, data, information, knowledge, services and procedures. However, Zhang & Galleta argue that the interaction is the main focus of the HCI studies. People use various kinds of technologies to support tasks that help them to satisfy their business, operations or personal goals. It is not uncommon that tasks are being carried out in the contexts that impose constraints on the execution of the tasks. Therefore, contexts and tasks become two key issues when designing HCI artifacts. Figure 2-2 illustrates an overview of broad HCI issues suggested by Zhang & Galleta. They also suggest that HCI can be studied from two perspectives: during the design and development stage of the artifacts, or during the actual use of the artifacts. The studies of the HCI design and its development methodology primarily concern with designing and implementing interactive systems for specified users, including usability issues. They focus on both human and technology issues prior to the technology's release and actual use. On the other hand, the studies of how the users are actually using the artifacts address the issues of how the technologies are impacting the users, organizations and societies. Traditionally, the usage studies have focused on human factors, ergonomics, organizational psychology, social

psychology and other social science disciplines. Design studies can be influenced by what we have learned from the use of the technologies.

Figure 2-2: An overview of broad HCI issues [Zhang & Galleta, 2006]



2.1.2 Cognitive Psychological Framework and Mental Model

The evolution of HCI involves the fundamental framework from the cognitive psychology, which studies the human mental capabilities, associated psychological behavior and the formulation of cognition architecture [Newell, 1990]. In their seminal work on the psychology of HCI, Card, Moran & Newell propose the notion of Model Human Processor, at which human's mind is considered as an information processing system. This model consists of three basic modules or systems: (1) a perceptual system, (2) a motor system and (3) a cognitive system. [Card, Moran & Newell, 1983]. The perceptual system consists of sensors and associated

buffer memories, the most important buffer memories are the Visual Image Store and the Auditory Image Store, which are used to hold the output of the sensory system, while it is being symbolically coded. The perceptual system carries sensations of the physical world detected by the human's sensory systems into internal representations of the mind by means of integrated sensory systems. The cognitive system receives symbolically coded information from the sensory images stored in its Working Memory and uses previously stored information in Long-Term Memory to make decisions about how to respond. The recognize-act cycle is the basic quantum of cognitive processing. On each cycle, the contents of Working Memory initiate associatively linked actions in Long-Term memory, which in turn modify the contents of Working Memory, setting the stage for the next cycle. The motor system carries out the response. To further support the psychology engineering of HCI, the Human Model Processor is used to derive the human performance, based on task analysis, calculation and approximation.

The notion of cognitive psychology has fostered the concept of mental model. There are numerous definitions of mental model; from earlier notion advocated by cognitive scientists, for example [Craik, 1943], to recent interpretation developed to explain the phenomenon in HCI by [Carroll & Olson, 1987]. [Norman, 1983] defines the mental model as the mental presentation constructed through interaction with the target system and constantly modified throughout this interaction. Cognitive psychology suggests that a mental model consists of two major components: knowledge structure (schema) and processes for using this knowledge (mental operations) [Merrill, 2000]. In the context of a heterogeneous safety-critical CST system, the schema represents a "target system", whereas the mental operations represent of how to interact with the target system. Unfortunately, the psychological processes that create the human operator's

mental states are not directly observable; mental model can only be guessed according to the human operator's behavior [Rosson & Carroll, 2002].

Mental model is drawing more attention from HCI research community; it is based on the idea that by exploring what users can understand and how they reason about the system through the HCI, it is possible to design a system that supports the acquisition of the appropriate mental model and therefore avoiding errors while interacting with the system. However, human operator's mental model is neither complete nor correct in every detail, which makes its application to HCI design a practical limitation; consequently the concept must be used with great caution. The ultimate goal is to ensure that human operator's mental model is functionally applicable to plan and execute operational tasks, as well as functionally capable to evaluate the results of system interaction and recognize any unexpected outcomes.

Another fundamental idea that underpins the cognitive psychological framework is the levels of processing. Basically this is the dimension between concreteness and abstractness. Input and output represent low-level human information processing, as they are responsible for handling the physical external reality. High-level processing provides identification and classification of raw data, as well as their assimilation into mental representation, understanding, analysis and decision-making etc. For a specific action to be executed, abstract goals and strategies must be formulated and then transformed into concrete form, which means the information is processed in both directions: from reality to mental models and from mental models to reality. From the HCI perspective, users of the system will activate a mental model constructed in working memory from the previous knowledge (stored in long-term memory) they have with the situation and from the information they perceive from the environment [van der Veer & Puerta-Melguizo, 2003]. Since the theoretical constructs of

cognitive psychology have direct analogy to computer science, and there is minimal difference in terminology used in these two disciplines, therefore, cognitive psychology becomes playing a dominant role in the development of HCI. Cognitive psychology assumes two central roles within the context of HCI; the first role is to produce a general description for how people interacting with systems and software, a description which could be synthesized as a guideline for development; and the second role is to verify directly the usability of system and software as they are developed [Carroll, 1997]. From the traditional cognitive perspective, the HCI is a system, which is composed by two information-processing units, the human and the computer. The output of one unit links and enters the input of another unit, and vice versa. In other words, the HCI can be described as an information-processing loop. There are definite advantages of this scheme; firstly, it provides a coherent description of the whole HCI system within the information-processing framework; and secondly, it structures the problem space of HCI in a useful way. Issues of HCI, such as presentation of the information to users, the user's perceptions, mental models and the user's control of the system, input devices, and user interface versus functionality of the system, can be clearly located and isolated within the scheme.

The notion of processing levels has also influenced the studies of HCI. Many researchers adopt the hierarchical structure of the HCI proposed by [Moran, 1981]. This structure consists of five levels: the task level, the semantic level, the syntactic level, the level of interaction, and the level of physical devices. This structure is explicitly design oriented and aimed to support an analogy with top-down programming in user interface. However, this approach has some limitations. The information-processing loop is closed. It is difficult to take into consideration the phenomena that situate outside it. If we consider the HCI in a wider context, we can easily discover that people use computers for a purpose to achieve some goals that are meaningful beyond actual computer use. Essentially, the "task level",

according to the hierarchy proposed by Moran, is supposed to put computer use into the right global context. However, the relevant concepts and procedures were not articulated specific enough by Moran, therefore HCI models based on his ideas are just models of the closed information processing loop. There is a consensus that the cognitive approach to HCI may be limited and does not fully provide an appropriate conceptual basis for studies of computer use in its social, organizational and culture context, in relation to the goals, plans, and values of the user or in the context of development. As a consequence, current studies of HCI concentrate not only on low-level events of computer use, but also on high-level events as well.

2.1.3 **Distributed Cognition**

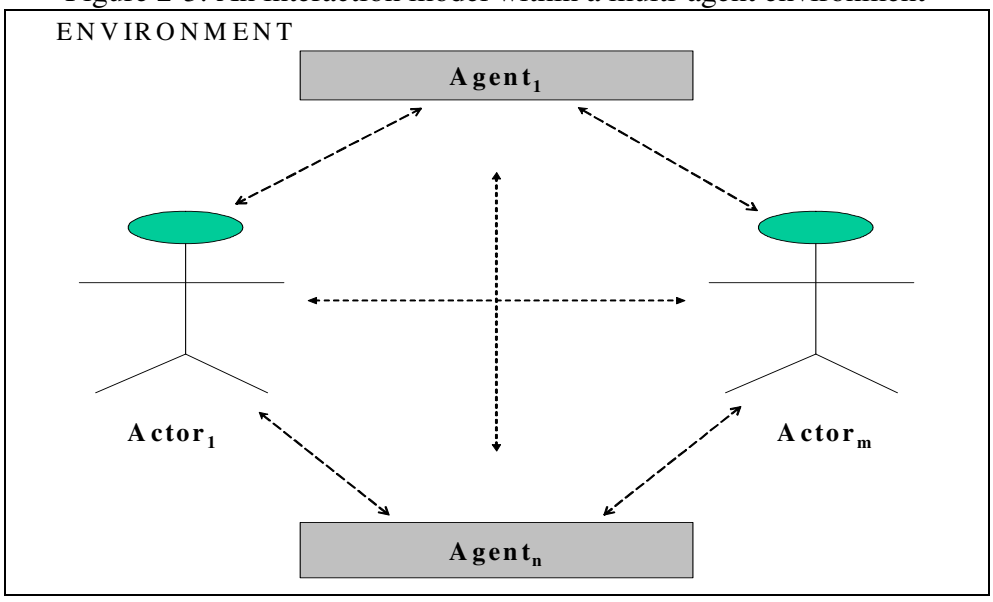
The conventional HCI is mainly concerned with individuals interacting with applications derived from decompositions of work activities into individual tasks. As computation becomes ubiquitous, and our environments are enriched with new possibilities for communication and interaction, the field of HCI is confronting with difficult challenges of supporting complex tasks, mediating multi-agents collaborated interactions (where agents can be intelligent devices or domain artifacts), and managing and exploiting the ever-increasing availability of digital information [Hollan, Hutchins & Kirsh, 2000]. It is apparent that the conventional cognitive psychology that addresses the organization of cognitive system within the boundary of individual actor (human) becomes unable to explain the phenomenon of multi-agents interaction. Distributed cognitive psychology, however, extends the focus beyond individuals to encompass dynamic interactions between actors and other artificial agents within the environment. Distributed cognition is a framework that describes and explains group cognition in order to understand how collaborative work is coordinated to achieve the common goals [Melguizo et al., 2004]. It studies the way in

which the information and knowledge is propagated, transferred and transformed through different representations around the network during system's activities [Wright, Fields & Harrison, 2000]. Hutchins [Hutchins, 1994 & 1995] applies distributed cognition framework to analyze how a cockpit remember its speeds, and the cognitive analysis unit includes the network of people and technologies. The distributed cognition framework proposed by Hutchins was developed primarily with the Computer Supported Cooperative Work (CSCW) in mind, using techniques that focus on the mapping of information flows that related to design requirements. To analyze humans' behaviors in a complex system using distribution cognition, it requires the inclusion of all significant features in the environment that contribute towards the accomplishment of tasks, which is one of the key reasons why individual disciplines – psychology, sociology and anthropology fail to achieve the same result. Increasing the coverage of cognitive activity investigation beyond individuals and with combination of external artifacts and other people is a far more appropriate approach to analyze human behaviors in a collaborated environment. Distributed cognition not only addresses the issues suggested by the science of the artificial [Simon, 1996], in which the structure of the physical environment is studied to examine how it interacts with the users' tasks, but also explores people's internal processes of how organizational and social setting are contributing to the structuring of activities in their environment.

There are two fundamental principles, which make the difference between distributed cognition from the conventional cognitive theory. The first principle is the boundary of cognitive process. In traditional views of cognition the boundaries are limited to individuals within the domain environment; distributed cognition, on the other hand, concerns cognitive processes on the basis of the functional relationships between actors and agents that collaborate in these processes. Therefore, in distributed cognition, a cognitive process is delineated by the dynamic functional

relationships among the actors and agents that participate in the process, rather than their spatial co-location. The second principle is the analysis mechanisms of cognitive process. Traditional views of cognitive process analyze the symbolic manipulation within individuals, whereas distributed cognitive demands for a larger scope of cognitive events, which may not be encompassed by individual human actors within the environment. Therefore, in order to have a complete picture of the interactions, the distribution and communication of human actors' knowledge need to be analyzed. In a complex socio-technical environment, there are three issues need to be addressed: the first issue is the social distribution, i.e. the interaction among actors; secondly, the technological distribution, i.e. interaction among actors and agents; and thirdly, the interaction among actors, agents and work environment [Sharp, Rogers & Preece, 2007]. Figure 2-3 shows an interaction model within an environment, which consists of multi-agent interactions.

Figure 2-3: An interaction model within a multi-agent environment



The interaction takes place between [$actor_1$ to $actor_m$] interacting with [$agent_1$ to $agent_n$]. Furthermore, actors' knowledge can be divided into two different types; the first type is the distributed knowledge – each individual

actor has specific knowledge, which represents a part of the complete knowledge that need to accomplish the tasks. The second type is the shared knowledge – all individual actors involved in the activities share a part of the knowledge necessary to complete the tasks [Rogers & Ellis, 1994]. For example, in a mass-transit railway system, operators in the control room and the train drivers in train-cabins possess shared knowledge of how to perform certain train regulation tasks, however, they do own distributed knowledge on their respective roles in control room and train-cabins.

Distributed cognition is exceptionally appropriate for investigating the dynamic interactions in a complex environment, such as a complex socio-technical system, which consists of multiple individuals as well as the domain artifacts they work with, and the cognition is distributed between them.

2.1.4 **HCI Modeling**

The concept of HCI modeling has several perspectives. The first level of HCI modeling is the user interface, for which the user of the system uses the interface to accomplish the user's tasks. It includes the layout of the computer's screens, 'windows', or a shell or layer in the architecture of a system or the application. Alternatively, the user interface can be defined from the user's point of view to the system; in many cases, the user does not distinguish the hardware and software layers of the system. From this perspective, the user interface can be developed as the "virtual machine model". The virtual machine model defines all aspects of a system that are relevant to a user; this includes not only the external appearance of the user interface that the user can perceive or experience, but also the semantics of all applications within the system.

The next level of HCI modeling is the conceptual modeling. A conceptual modeling is a collection of concepts and their relationships, which embodies users' shared view and understanding for some common domain of interests or practices [Hua et al., 2005]. The emphasis of the conceptual modeling is based on the system's functionality, i.e. how system functions are provided to solve the problems in the targeted domain. It concentrates on what the system should do, or on its functionality by means of domain and functional models; a common example is the object and use-case models in UML [Booch et al., 2005]. The conceptual model is the explicit model of the system created by the system's designers. It is a consistent and complete representation of the system as far as the users are concerned, and is presented to the users through the user interface. If the system is a single-user system then the conceptual model is equivalent to the virtual machine model. However, if the system has multiple users with different classes, such as a CST system, each class should have a corresponding virtual machine model; and the conceptual model is the combination of all virtual machine models.

The third level of HCI modeling related to the notion of mental model, which is described in details in *Section 2.1.2 - Cognitive Psychological Framework and Mental Model*.

2.1.5 **Usability – Evaluation of HCI**

The term "usability" has been in use for some time and a number of definitions exist. Table 2-1 highlights different descriptions of usability summarized by [Smith, 1997].

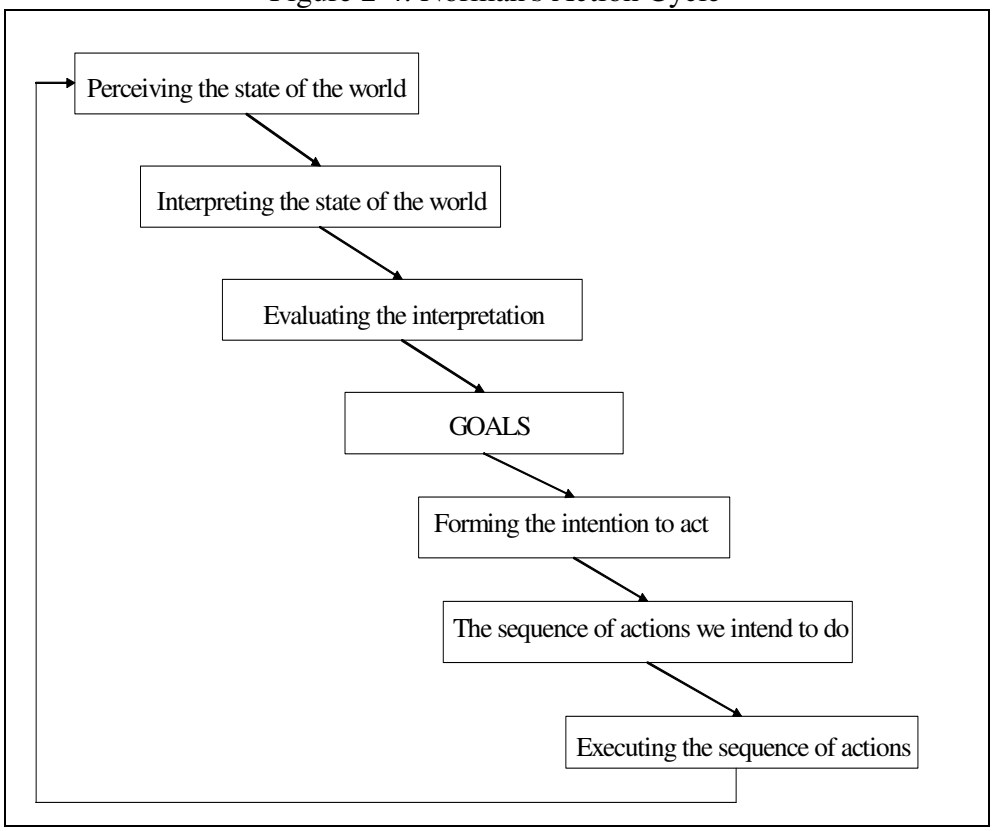
Table 2-1: Summary of the definition of usability

	Description	**Sources**
1	'Ease of use'	[Miller, 1971]
2	Offering 'functionality in such a way that the planned users will be able to master and exploit (it) without undue strain on their capacities and skills'	[Eason, 1988]
3	'The quality of a system, program or device that enables it to be easily understood and conveniently applied by the user'	IBM Dictionary of Computing [IBM, 1993]
4	'…effect, learnability, flexibility and attitude…'	[Shackel, 1986]
5	'has multiple components and is traditionally associated with five usability attributes: learnability, efficiency, memorability, errors and satisfaction'	[Nielsen, 1993]
6	'A set of attributes of software which bear on the effort needed for use and on the individual assessment of such use by a stated or implied set of users'	[ISO/IEC TR 9126-4, 2004]
7	'The effectiveness, efficiency and satisfaction with which specified users can achieve specified goals in particular environment'	ISO 9241-11 [ISO, 1998]

Although people have slightly different definitions for the term "usability", ultimately they are converged to the same theme. The concept of usability can be simply expressed as the desire and need to make things easier and more efficient for the users. Usability engineering is the process of achieving usability. Usability engineering is aimed to solve the problem of ensuring that a system is fit for the purpose for which it is designed. It does this by a process of discovering what will make an acceptable system for users and matching the delivered product against those previously agreed criteria for acceptability. By developing proper procedures and methods for

different stages of the design and development in a structured and systematic manner, the usability engineering can demonstrate that a particular product is usable and fulfils the criteria for a particular user to perform a specific task in a given environment. In the usability requirements capturing, the focus will be on goals of the users and what tasks the users need to perform in order to achieve their goals. [Faulkner, 2000] details the basic idea of user's goals. In order to do something, the user must first establish a concept of something that needs to be done. We can see this as a goal that needs to be achieved. In order to achieve a goal the user has to do something or manipulate something. The user then will look at what has been done or manipulated and decide whether the goal has been achieved. [Faulkner, 2000] explains the Action Cycle Model suggested by [Norman, 1988] as shown in Figure 2-4.

Figure 2-4: Norman's Action Cycle



The goal is translated into an intention to perform some actions. This intention has to be translated into a series of internal commands or an action sequence which, when performed, will probably lead to the achievement of the goal. After the action is executed, then it must be evaluated. This begins with perceiving the state of the world, which is then interpreted according to what the expectations of the action were. The state of world is compared with the intention of the actor. According to this model, the goal is defined as the state that the human wishes to achieve. The task is the activities required in order to bring about the state the human wishes to achieve. An action is the physical interaction with the system in order to carry out the user's goal. It is worthy to note that many goals and intentions are not well planned. [Norman, 1988] also defines the opportunistic actions as those that take place because a situation arises where it would be beneficial for the actor to perform a particular task under specific condition. The importance of this definition is that people may not always behave in a logical fashion and it would be unwise of software designers to expect people to behave logically all the time.

Norman's Action Cycle Model tries to explain the theory behind interactions; however, it does not prescribe the methodology to capture the interaction and usability requirements. To resolve this problem, the Usability Engineering Framework is proposed [Rosson & Carroll, 2002]. The Usability Engineering Framework is founded on the use of scenarios as a central representation for the analysis and design of use. The basic idea is that a scenario can be used to describe an existing or envisioned system from the perspective of one or more users. It includes a narration of their goals, plans and reactions. In the simpler term, a user interaction scenario is a story about people and their activities. Figure 2-5 shows the Scenario-based Usability Engineering Framework. Within a scenario, a number of characteristic elements will be used to depict the actions. To illustrate the concept of scenario Table 2-2 shows the scenario elements of typical user

interaction scenarios in a mass-transit railway control room, as an example of CST system. Figure 2-6 shows the scenario elements in a diagrammatic representation.

Figure 2-5: Overview of the Scenario-based Usability Engineering Framework proposed by [Rosson & Carroll, 2002]

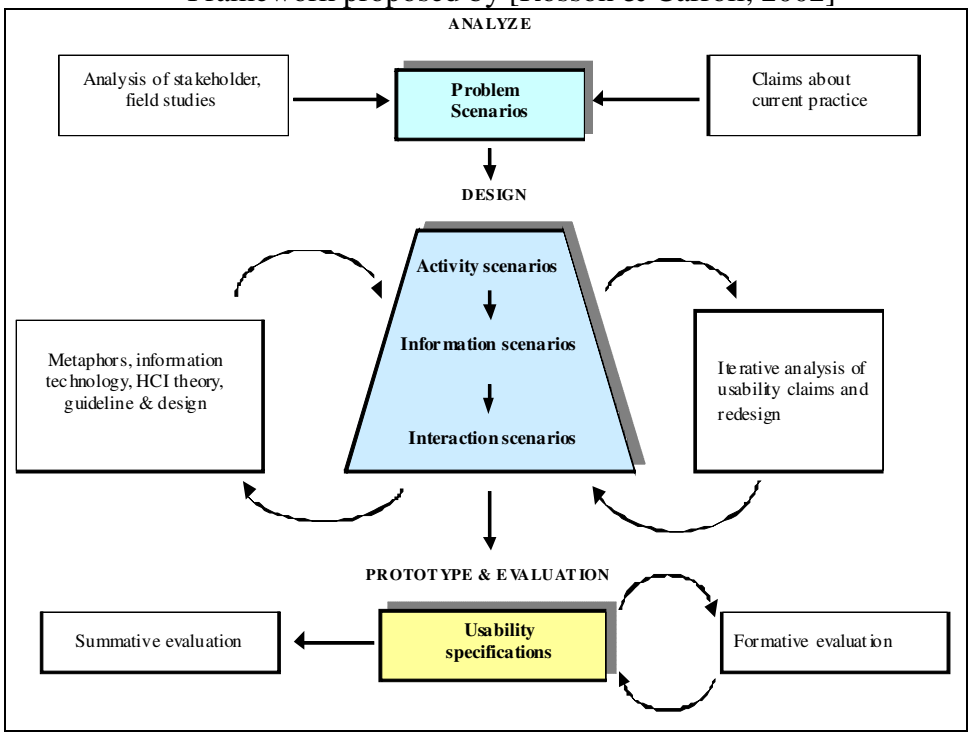


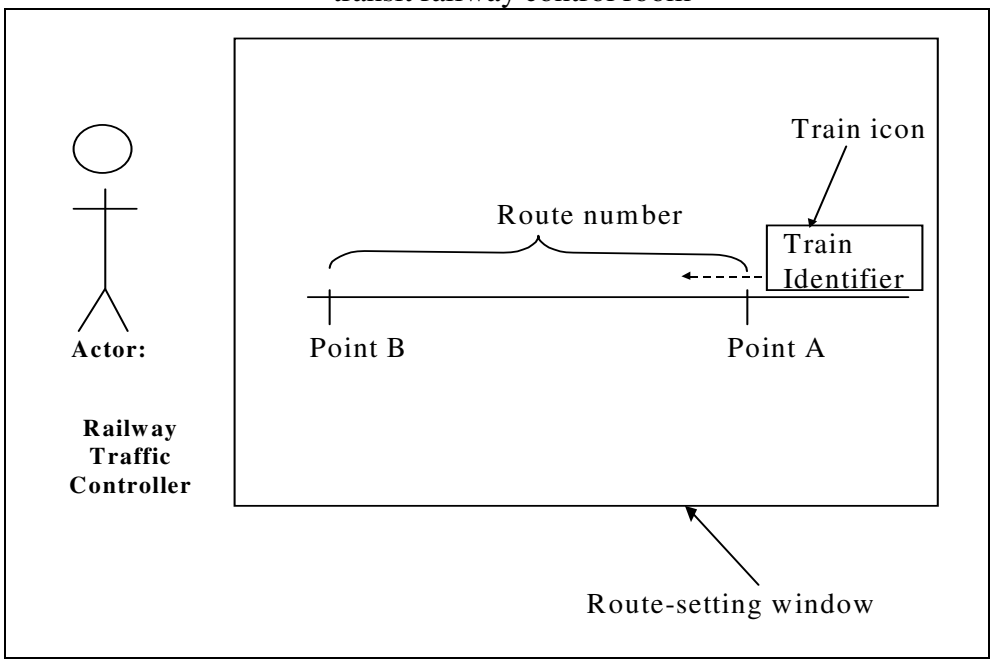
Table 2-2: Scenario elements of user interaction scenarios in a mass-transit railway control room

Scenario Element	**Definition**	**Example: Scenarios in a mass-transit railway control room**
Setting	Situational details that motivate or explain goals, actions, and reactions of the actor(s).	Control Room, which oversees the operation of a mass-transit railway network during traffic hours.
Actors	Human(s) interacting with the computer or other setting elements; personal characteristics relevant to scenario.	Railway Traffic Controller using the system to perform computer-controlled train movement.

Scenario Element	Definition	Example: Scenarios in a mass-transit railway control room
Task Goals	Effects on the situation that motivate actions carried out by actor(s).	Need to route a train from point A to point B in the railway network.
Plans	Mental activities directed at converting a goal into a behavior.	Open the "route-setting" window, which allows the Railway Traffic Controller to operate the train icon.
Actions	Observable behavior.	Input the train identifier and route number to the computer and press "confirm" button.
Events	External actions or reactions produced by the computer or other features of the setting; some of these may be hidden to the actor(s) but important to scenario.	The train icon is stepped forward and the route becomes occupied.
Assessment	Mental activities directed at interpreting features of the situation.	Assess the route occupied status and train icon stepping status from the Train Control Monitoring display.

Scenarios have a plot; they include sequences of actions and events, things that actors do, things that happen to them, changes in the setting, and so forth. These actions and events may aid, obstruct, or be irrelevant to goal achievement. For example, the Railway Traffic Controller may need to resizing the "route-setting" window in order to get right level of information display, or he/she may also needs to open another "communication" window in order to communicate with the train driver during the train movement process. By using a set of user interaction scenarios, the system can be explicitly represented and therefore the analysts and designers will have a broader view of the system's usage.

Figure 2-6: Scenario elements in a diagrammatic representation of a mass-transit railway control room



[Nielsen, 1993] describes scenarios as the ultimate minimalist prototype in that they describe a single interaction session without any flexibility for the user. As such, they combine the limitations of both horizontal prototypes (users cannot interact with real data) and vertical prototypes (users cannot move freely through the system). A scenario is an encapsulated description of the followings:

- An individual user
- Using a specific set of computer facilities
- To achieve a specific outcome
- Under specified circumstance
- Over a certain time interval (this is contrast to simple static collections of screens and menus: the scenario explicitly includes a time dimension of what happens when).

Usability studies are also approached from a practical perspective – focus on the product's user interface. [Mayhew, 1999] pointed out that usability is a

measurable characteristic of a product's user interface that is presented to a greater or lesser degree. One broad dimension of usability is how easy to learn the user interface is for novice and casual users. Another is how easy to use (efficient, flexible, powerful) the user interface is for frequent and proficient users, after they have mastered the initial learning of the interface. Over the years, usability practitioners and researchers have come up with sets of principles for software usability. The following is a set of principles developed by Nielsen & Molich in [Nielson, 1993]:

- Simple and natural dialog. Dialogs should not have any irrelevant or infrequently used information. All information should be arranged in a way that is natural to users.
- Speak the user's language. Dialogs should be expressed in text and concepts familiar to users.
- Minimize user memory load. Users should not have to remember information as they move from one part of the dialog to another.
- Consistency. Users should not have to wonder whether different words, situations, or actions mean the same thing.
- Feedback. Users should always be informed about what is happening in the system.
- Clearly marked exits. System should have visible exits so that users can leave any unwanted situation.
- Shortcuts. Accelerators that speed up tasks should be available for expert users.
- Good error messages. Massages should, in plain language, state the problem and suggest a solution.
- Prevent errors. Systems should, whenever possible, prevent problem from occurring.
- Help and documentation. Information should be easy to retrieve and should list required steps to complete tasks.

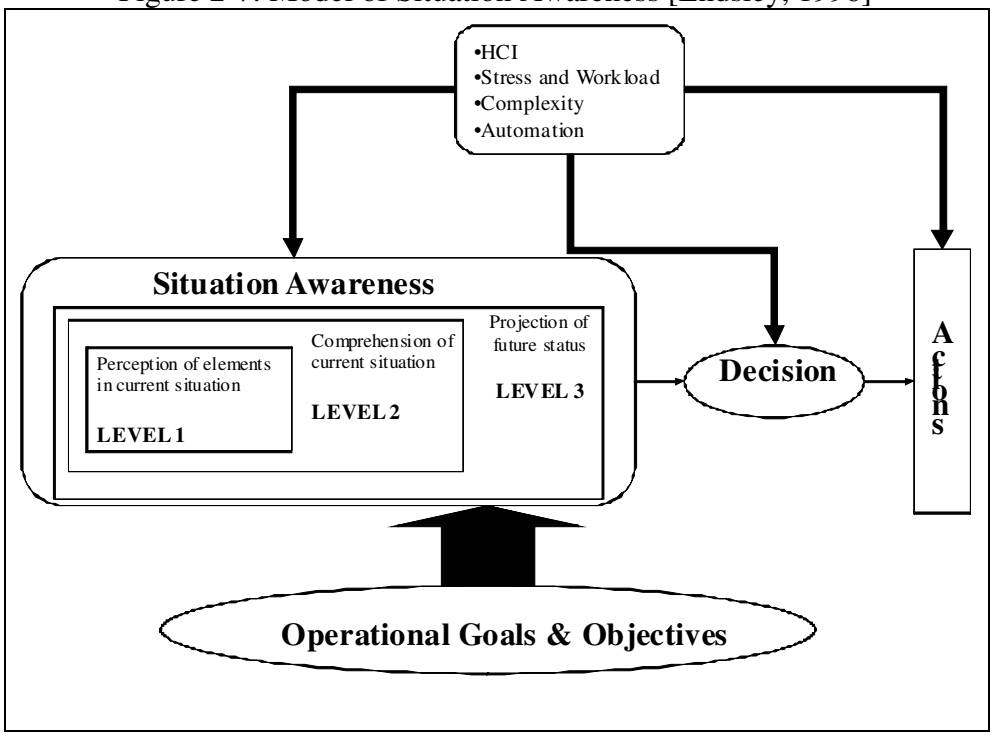
These principles provide a practical high-level guideline to measure the usability of a user-interface. However, it does not address the broader issues of multi-agent interaction within a complex socio-technical environment. Therefore further research effort is required to develop new usability evaluation mechanisms for complex socio-technical systems.

2.1.6 Situation Awareness

A typical safety-critical CST system, for example a mass-transit railway system, is usually accompanied by one or more control rooms, where operators are collaboratively working together to ensure the system functions are performed according to the operational requirements. In such an operational environment, large quantity of real-time operational status and alarms data are collected by the system and continuously reported to the control room for operators to monitor the condition and performance of the system. These dynamic field data coming from all over the domain specific systems within the safety-critical CST system and are presented to the operators through the system's HCI. This integrated picture created by the system's HCI forms the central organizing feature from which all decision-making processes and actions are taken place. Situation awareness can be considered as an internalized mental model of the current state of the operators in such an environment [Endsley, 2001]. Early research in situation awareness is originated in the aviation domain, such as pilots and air traffic controllers; however, the use of situation awareness and its application has rapidly spread to other domains typically with human operators and control room environment. In Endsley's model of situation awareness, three levels are layered to describe the specific contents of the issues, as illustrated in Figure-2.7. The first level, which is fundamental, is the perception of elements in the current situation. The second level is the comprehension of current situation, which goes beyond perception by including interpretation, consolidation and retention of information. This

level also integrates multiple pieces of information and determines their relevance and significance to the operators' goals. The highest level is related to the ability of predicting future situational events and dynamic changes for timely decision-making.

Figure 2-7: Model of Situation Awareness [Endsley, 1996]



The issue becomes increasingly serious as the gap between the data generation / dissemination and the operators' ability to digest the data and convert to useful information becomes larger. It is becoming widely recognized that more data is not equivalent to more information. Automation and intelligent systems have frequently exacerbated the problem rather than resolving it [Sarter & Woods, 1995]. One of the explanations for this adverse drawback is the limitation of the operators' mental models. With their experience in mind, the operators develop internal mental models of the system they operate and the environment in which they are situated. These models serve to filter out the irrelevant data and directly limit the attention in an efficient way, which provides a mean of

integrating information without loading to the working memory and suggests a mechanism for generating projection of the future system's states [Endsley, 2000]. The application of mental models in achieving situation awareness is considered to be dependent on the ability of individuals to pattern match between critical cues in the environment and elements in the mental models. However, the situation awareness cannot be based on the operators' perception of all the elements that exist in the real world situation. If operators had to control complex systems and monitor thousands of elements individually, they would simply be overwhelmed by the complexity of the system [Baxter & Bass, 1998]. Alternatively, a "situational model" is the current state of the mental model, i.e. an instance of the mental model. For example in the case of the mass-train railway system, the operators can have a mental model of a passenger train, but the situational model is the current state of the train, such as the current location, train's run-number, direction of travel and destination etc. This situational model describes not only the operators' representation of various parameters of the system, but also a representation of how they are related in term of system forms and functions in order to create a meaningful synthesis and a comprehension of the system state. In the above example, the situational model of the operator also includes an understanding of the punctuation of the train and whether remedial actions need to be taken, such as making public announcement to passengers for the late train. However, the use of mental model is not all positive to the situation awareness. One of the critical issues is that the mental model can lead to significant problems of biasing in selection and interpretation of information that may create errors in situation awareness. Furthermore, the quantity and format of data generated from a heterogeneous safety-critical CST system can easily go beyond the capacity of the operators' mental model.

When emergency condition happens the operators must react quickly, effectively and accurately; the situation awareness of the operators is critical

to their ability to make decisions, revise plans and act promptly to correct the abnormal situation. The HCI is the front agent for providing situational data to the operators; therefore the HCI can have a profound effect on the operational integrity of the system. This argument emphasizes the importance of designing HCI to support the situation awareness explicitly in safety-related systems. Furthermore, any suggestions for design trade-off between usability and safety may also affect the reliability of the cognitive processes involved with acquiring and maintaining a safe level of awareness of a situation. If the design intent is to develop a transparent HCI in the name of usability, the resulting automatic interactions may have an adverse effect on the awareness of the operators. This may also affect the safety of the system [Sandom, 1999]. How to design the HCI of a system that supports the situation awareness of the operators to get the needed information under numerous dynamic operational constraints becomes a challenging issue to the designers of heterogeneous CST systems.

2.1.7 Safety Aspects of HCI in CST Systems

One of the major issues that a heterogeneous safety-critical CST system needs to address is the safety and integrity of the system. There are a large number of researches from the disciplines of reliability, availability and maintainability (RAM) for computer-based systems, which are aimed to design and build the computer systems that can be deployed in safety-critical domains. We will not go into the details of such research results, as it is beyond the scope of this thesis. However, from the safety and integrity perspective, the HCI remains as one of the most critical issues to the operations of a heterogeneous safety-critical CST system. People do make mistakes! Operators can easily be blamed for negligence in making "human error" when incidents happened in safety-critical CST systems. However when we take a closer look to the cases for which the incident's cause is categorized as human error, it reveals that the problems are linked more

closely to design, rather than operations – that something in the design of human interface is at fault, something that could have been foreseen and that could have been designed in a safer way [Redmill & Rajan, 1997]. For example, a catastrophic incident happened in 1992 when an Airbus A320 crashed into a hill near Strasbourg, France. It was believed that the similarity between the display representations of flight path angle and vertical speed played a major role in causing this tragedy [FAA, 1996]. In this accident, blaming the crew pilots as negligent or incapable would not be able to discover the issue.

Human-performance hazards are well known problems and should be avoided by appropriate design, in particular the HCI design for computer-based systems. Human reliability analysis tools and techniques have been developed to predict the human error probability in a given mission; however, most of the tools and techniques are used in post-accident evaluation [Filgueiras, 1999]. Many studies have been conducted to identify the root cause of failure in the environment where human operators need to work together with automated systems. One of the main kinds of failure in human actions in complex automated environment is contributed by the loss of expertise [Hoc, 2000]. Complex and automated systems with autonomous roles make the operators become unfamiliar and unable to maintain their skills. The effect of this phenomenon has eventually reduced the level of situation awareness of the operators; as a consequence the operators become incapable of performing the functions [Endsley, 1996]. As the system functions are mostly represented through the HCI of the system, the design of the HCI becomes a critical factor to ensure the safety of the system. There are other human errors in HCI that can cause the failure of the complex computer system. Firstly, the knowledge built into software acts the role of an agent that behaves in a way, which is unknown to operators. In this circumstance, human operators may create wrong predications about the automatic behaviors and competition of conflicting

goals. Secondly, the information navigation problem will cause the operators moving through information space in order to find out necessary resources to complete their tasks. Due to the increasing availability of data, information retrieval can be very time-consuming and additional cognitive loading is required to process all data found. A third kind of operator error is related to automation of human tasks, which replaces manual, continuous work for an intellectual, intermittent work. Long supervisory periods without physical activity will cause the decrease of attention; therefore important events that used to trigger operator actions will cause misperception of events [Filgueiras, 1999].

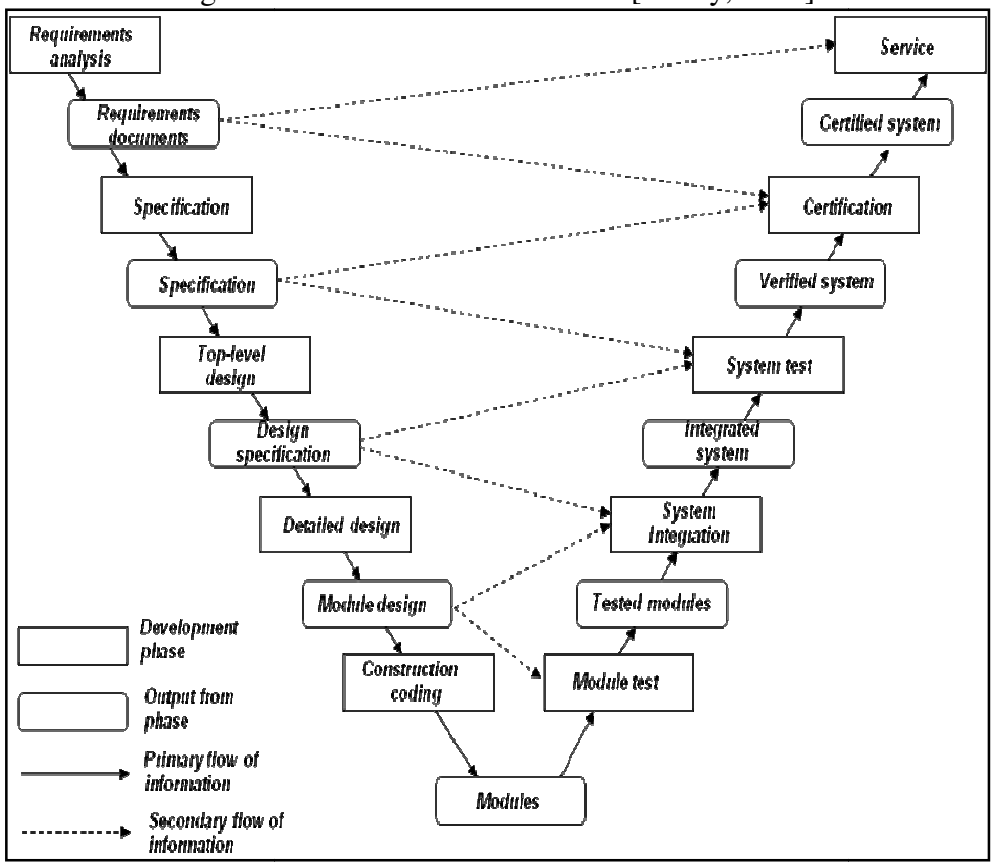
Furthermore, there are a number of potential hazards to the roles of the operators in a CST system [SEC, 2003]. If the operator plays a monitoring role to the complex processes, the speed of the changing of processes' states must be carefully considered; the monitoring tasks may not be possible for human operators if the processes being monitored require a reaction speed that human operators cannot match. If the role of the operator is only played for backup conditions, then again this may lead to a lower proficiency of the operator due to the lack of regular skills practice. In addition, lack of skills practice will eventually become lack of confidence of performing the skills; operators may become hesitant to intervene even when they should take over for failure situation. In the case of the human operators are partnering with the system, the chance is that the operators will be required to do all those miscellaneous tasks that do not fit well or too costly to be handled by the system. Another potential problem in HCI hazard is the mode confusion. Mode confusion is a general term associated with situation awareness in an automation environment, for which the operators are supervising the complex processes instead of directly controlling these processes. This changing role alters the cognitive loading on the operators; the decision-making becomes more complicated, and the need for cooperation and communication between the system and the

operators is more demanding. The advancement of computing and automation technologies enables designers to design a system with more flexibility and with mode-rich capability. The results are numerous mode indications spread over multiple HCI displays and each display contains just a portion of mode status data, which only corresponds to a particular subsystem, but not the overall system. The increasing sophistication of complex processes creates additional delays between operators' input and feedbacks about the system behavior. These changes have led to increasing difficulty in error or failure detection and recovery. How to design the HCI in such a complex environment, which matches the human capability to maintain awareness of active modes, becomes an urgent issue to resolve.

2.2 HCI Development Methodologies

Over the past years, numerous system development models have been devised to describe the methodology and various phases of a development project, some of them are generally designed for multi-disciplinary projects and some are specifically for software development projects. These models identify various components within the project and may indicate interdependencies or interrelationships amongst them. Each model has its own characteristics and advantages, and different models are used for different purposes. One of the widely adopted models in large-scale multi-disciplinary projects is the V-Model [Storey, 1996]. Figure 2-8 shows the details of the V-model. The V-Model not only defines the development processes and corresponding deliverables, but also provides information flow between deliverables and processes, which demonstrates a mechanism to measure the progress of the project.

Figure 2-8: Details of the V-Model [Storey, 1996]



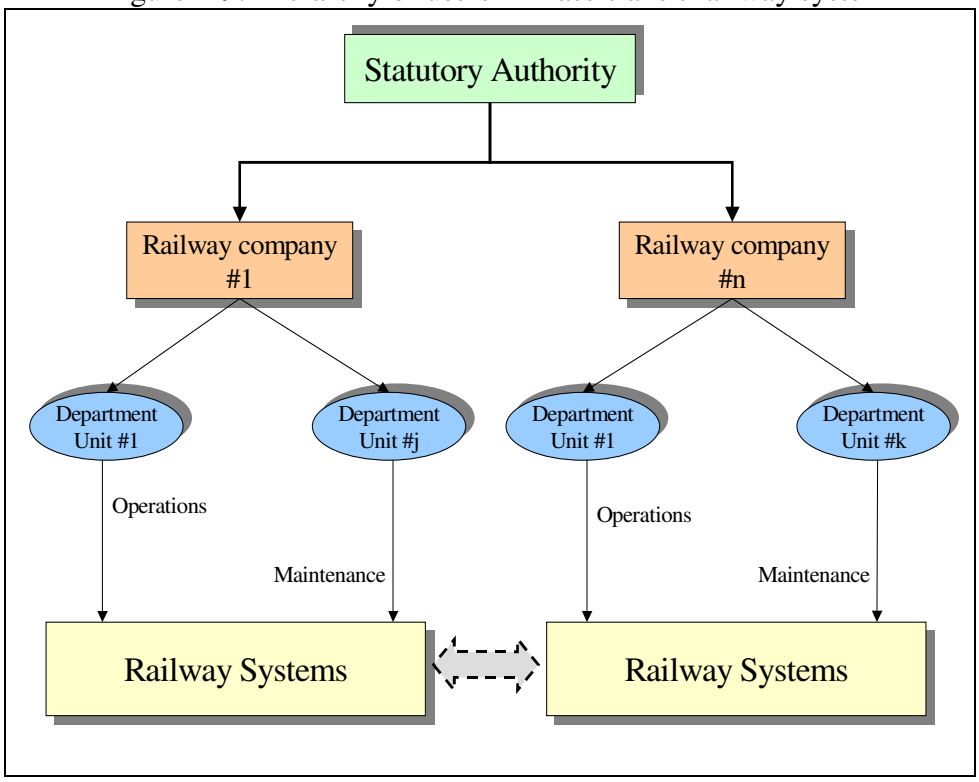
Since most projects have unique development constraints, it is not uncommon that developers modify the V-Model to tailor-make their individual development methodology. The V-Model clearly illustrates the outcome of each phase of the development process, and also indicates the flow of information between phases. However, it does not show the amount of work involved in each stage or when that effort will be required. It also lacks the inevitable iteration that commonly occurs and the specific methodology applied within each process. From the HCI perspective, the V-Model fails to provide sufficient guidelines for the development of HCI deliverables; and therefore, alternative means are required. There are several methodologies, which specifically address usability and HCI issues, including Scenario-based Development for HCI [Rosson & Carroll, 2002] and the Usability Engineering Lifecycle [Mayhew, 1999]. However, most of the existing usability or HCI methodologies emphasize the dominant

concerns for usability, which overshadow other concerns, such as organizational needs, physical concerns and affective concerns. Some methodologies focus heavily on the design stage and do not pay sufficient attention to the importance of analysis at an early stage of the system development; in fact many usability and interaction problems are caused by inadequate understandings that should be addressed in the first place, such as the analysis stage [Te'eni, Carey & Zhang, 2007]. On the other hand, despite the recent advances in software engineering, systematic and scalable requirements engineering processes for CST systems are still not widely available [Sutcliffe, 2000]. The purpose of this thesis is to explore a HCI requirement analysis framework, which bridges the gap between HCI requirements and software development methodology for CST systems.

2.2.1 Definition of User

Regardless of different approaches, the system development commences from the analysis of users and their needs. Understanding user needs is considered as a success factor in almost all product development. It is particularly important in the beginning of the development phase when most of the user requirements are elicited and defined. Research results also show that there are commercial benefits of doing that because if more time and effort are invested in the early phase of a software project, it yields faster cycle time and higher productivity [Blackburn et al., 2000]. However, the term "user" may be controversial to different people. In the socio-technical environment, for example a mass-transit railway system, the user can be the passengers or the statutory authority that looks after the transportation policy and regulations. The user can also be the railway company, department units within the railway company, or the people who physically operate and maintain the railway systems and infrastructure. Figure 2-9 shows the hierarchy of users in a typical mass-transit railway system, as an example.

Figure 2-9: Hierarchy of users in mass-transit railway system



It should be noted that it is very common for a statutory authority to oversee a number of railway companies within the same metropolitan city, and it is often inevitable for different railway companies to interface with each other, in order to provide integrated services to the community. For example, a railway inter-change station (where commuters can change railway lines for different destinations) can be co-operated by two companies. Depending on the hierarchy layer that the user is situated, the user's needs analysis will have different approaches. With respect to the context of this thesis, the "user" is referred to people who physically operate the railway systems, therefore the requirement engineering processes and techniques for user's needs analysis will be focused on this layer of users. In addition, the "needs" is primarily focused on the HCI requirements, instead of functional, behavioral and non-behavioral requirements.

Early research in user requirements analysis recommends the analysis should begin from users and tasks, perform empirical measurement, and employ iterative design [Gould & Lewis, 1983]. The concept has further been developed as the User-centered Design (UCD) approaches in which the entire system development process consists of iterative cycles of analysis, design and evaluation [Vredenburg et al., 2002]. Despite the early research recognizes that the entire system development lifecycle should progress in an iterative fashion, it is still unclear when iteration should begin and what level of granularity should be achieved in order to progress to the next stage. For example, in the case of user needs analysis, it is unclear when the analysis should stop, when feedback from users on prototypes should or can no longer be accommodated, or how to integrate new requirements dynamically. While some of the User-centered Design methodologies explicitly accommodate iterative refinement of requirements, iteration itself is typically confined to a particular stage in the development life cycle [Mayhew, 2003]. This makes it difficult to incorporate additional data collected from user needs analysis into the HCI design once the requirements capturing process is completed, given that the software engineering processes are subject to their own sets of constraints. In addition, documenting and presenting the analysis results to ensure seamless conversion into the HCI design is also a problem to the current development methodologies. Existing methodologies and techniques appear to be helpful in some, but not all aspects of the user needs analysis process [Lindgaard et al., 2006]. Thus without a robust analysis framework, the translation process from requirements into design will be at risk and difficult to complete. Before we proceed to explore the alternatives, a fundamental step is to review the current theories and practices of analysis methods for HCI so that we can develop a richer picture of the core activities of these methods. While analyzing their limitations, constraints, general weaknesses and deficiency we can also explore the possibilities for improvement.

2.2.2 **Context Analysis**

Context Analysis is aimed to understand the technical, environmental and social settings where the CST systems will be used. Context Analysis is exceptionally important to CST systems, such as the mass-transit railway system, because of their specific operating environment. It examines how the interaction between the physical/social environments and the physiological/psychological characteristics of the operator would impact operators interacting with the system [Te'eni, Carey & Zhang, 2007]. There are mainly four aspects in Context Analysis: physical context, technical context, organizational context, and social and cultural context. Overall, Context Analysis can provide ideas for design factors such as metaphor creation / selection and patterns of communications between operators and the system. Two out of four principal activities of User-centered Design in ISO Standard [ISO 13407, 1999] are related with the context identification. These principal activities are; a) understanding and specifying the context of use, including the characteristics of the intended users, the tasks that users are to perform, and the environment in which they are to use the system; b) specifying the user and organizational requirements in relation to the context of use description; c) producing design solutions iteratively by using user feedback; and d) evaluating designs against requirements at all stages in the system development life cycle. The Standard also provides guidelines for planning the user-centered design process and user-centered design activities; however it does not prescribe specific techniques or methods for the activities. The thesis concerns with issues of HCI analysis within the system development lifecycle of CST systems and therefore activity (a) and (b) of ISO 13407 (1999) will be our main focus.

2.2.3 **Task Analysis**

The foundational study of tasks in work-place can be traced back to the beginning of last century when the classic "Taylorism" was developed to measure the work performance and manufacturing productivity [Taylor, 1947]. Taylor' method focuses on workflow optimization; however it does not include human factors and limitations involved in the performance of tasks. Despite the work nature in Taylor's generation was drastically different with today's, Taylor's method is continued to be treated as an important reference; and its successful in improving manufacturing productivity and the inspiration created for future attempts to incorporate human factors into work methods simply cannot be ignored. As the nature and characteristics of work-place tasks have increasingly become more complex since the emergence of computing, communications and automation technologies, applied psychologists and system engineers need to find more rigorous, systematic and cost effective analytical techniques to deal with the complex tasks and systems. These techniques become influencing the emerging interdisciplinary practice of HCI. As computing technology becomes more powerful, HCI comes to encompass a new spectrum of human behavior; consequently Task Analysis needs to expand its scope and complexity. Today, regardless of domain applications, Task Analysis is frequently used in requirements analysis process and it is one of the most important techniques used by HCI developers to help designers to develop more usable interactive systems. The main goal of Task Analysis is to elicit the work knowledge so that descriptive models can be developed for system design. Simplistically speaking, most Task Analysis involves identifying tasks, collecting task data, analyzing this data so that the task are understood, and then producing a documented representation of the analyzed tasks suitable for some engineering purpose [Stanton, 2004]. Task Analysis exists in between a science-based and purpose-oriented method or procedure to determine what kind of elements the respective task is

composed of, how these elements are arranged and structured in a logical and effective order, how the occurrence of a task can be explained or justified, what are the driving forces to generate the task, and how the task and its elements can be aggregated to another entity, composition, or compound. Therefore, it could be argued that Task Analysis is a central activity in the system design process. An introductory description of task analysis can be found in [Diaper, 2004]. The methodology of Task Analysis covers a wide range of different approaches to analyze a work system. [Limbourg & Vanderdonckt, 2004] provides a comprehensive comparing of various task analysis models and methods, which are broadly used in practice for UCD. These models and methods enable rigorous and structured characterizations of user activity. They provide a framework for the investigation of existing practices to facilitate the design of complex systems. Task Analysis is particularly valuable in the context of HCI. Since user interfaces must be specified at very low level while still mapping effectively to users' high-level task. As HCI may not have the flexibility of human-to-human interaction, or human-to-environment interaction, this inflexibility magnifies the impact of interaction design problems, making the close integration of task structure and interaction support especially crucial.

The pioneering method of Task Analysis is the Hierarchical Task Analysis (HTA). The top-down approach of HTA focuses on the system's functionality, rather than behavioral or psychometric constructs [Annett, 2004]. HTA provides a tree-structured graphical representation of named tasks and a plan for each individual hierarchic level, which describes the possible sequences of tasks and the conditions under which the sequences are executed. Complex tasks are decomposed into a hierarchical structure with goals and sub-goals nested within the higher order goals. Each goal and its means of achieving are represented by an operation, which is a fundamental unit to identify the functional goal. The key features of an

operation are the conditions under which the goal is activated (the input) and the conditions which satisfy the goal (the feedback) together with various activities (actions) that may be deployed to attain the goal. By analyzing tasks in this way, the problem related to behavioral taxonomies can be avoided. The attention is focused on the actual facts whether the tasks are accomplished or not, rather than concerning with the operators' cognitive processes and actions. HTA approach is originated from the system theory and information-processing models of human performance for analyzing complex non-repetitive operator tasks, especially process control tasks commonly found in conventional industrial sectors such as chemical plant and power generation. However, it becomes more complex due to the emergent of computing and system automation. The strength of HTA is its system-centric perspective, in particular for the socio-technical environment with safety-critical systems. Its ability to optimize the overall system performance, by identifying the correct allocation of functions between human operators and machine in consistent with their respective performance capabilities, is one of the most important contributions. HTA recognizes the responsibility of the operator to plan the use of available resources to attain a given goal, however, it does not have specific consideration for the operator's cognitive processes, it also fails to suggest methods to understand the structure of human cognition in order to appropriately support cognitive intensive tasks, for example in the control room environment of CST systems such as the mass-transit railway system control room. These limitations require additional theoretical structure to develop a more complete understanding of human activity.

In order to fill the gap between the system-centric HTA and the cognitive processing of human operators, [Card, Moran & Newell, 1983] proposes a Model Human Processor (MHP). Based on the MHP a GOMS Model is developed to map out the constraints imposed on behaviors by the nature and features of the task environment, and to determine what human

operators know about the task and when they know it. GOMS Model is originally intended as an analytic approach to evaluating user interface's usability. However, as it develops it incorporates the idea of computational modeling of human cognition and performance, and has thus become a framework for constructing computer simulations of the subset of human activity that is especially relevant to HCI [Kieras, 2004]. GOMS Model treats all tasks in terms of a set of Goals, a set of Operators, a set of Methods for achieving the goals, and a set of Selection rules for selecting among competing methods for a specific goal. A set of goals is defined as a symbolic structure that defines a state of affairs to be achieved and determines a set of possible methods for achieving it. Operators are defined as elementary perceptual, motor or cognitive acts whose execution is necessary to change any aspect of the human operator's mental state or to affect the task environment. A method is defined as a description of a set of procedures for achieving a goal, and is one of the ways that human operators store their task knowledge. It should be noted that methods are learned procedures that should have been familiar by human operators. The selection rules in a GOMS Model determine how the human operator selects a particular method, and can be used to predict which method(s) the human operator will select on the basis of knowledge of the task environment. Task analysis results produced by the GOMS Model often in the form of a hierarchical plan, which is similar to those produced by HTA. However, the main different is that HTA generally describes high-level activities, whereas GOMS Model typically works at the low-level operations.

There are a number of other techniques and methods, which are aimed to supplement the limitations of the above described models, for example, the GroupWare Task Analysis (GTA) is developed to model the complexity of tasks in a cooperative environment [van der Veer, Lenting & Bergevoet, 1996]; the contextual facet of activity theory [Bedny & Meister, 1997].

However, lack of generalized empirical results is still remained as the obstacle to the widespread application of such techniques and methods.

The development of task analysis can be seen as the reflection of the progress of HCI research trends. HCI research has evolved over the past couple of decades from focusing on technical-ergonomic aspects, to conceptual & information-processing models, to work-process of contextual models. As they have evolved, task analysis techniques have become increasingly complex and fragmented. As a result the sophisticated forms of task analysis developed by researchers are often ignored in practice. Choosing the right criteria to determine what makes a good task analysis is also difficult to find in the literature, despite the fact that many suggestions of how task analysis should be done are available [Daabaj, 2002]. For task analysis to realize its potential, further research must be focused on its usability and degree of integration. The use of task analysis techniques in context, assessing the efficiency and effectiveness of these techniques for particular tasks, situations, work-environment design problems and organizational structures are some of the future research directions that we need to explore.

2.2.4 **Scenario-based Analysis**

Scenarios have been widely used as an effective means for communication between designers and system users and stakeholders. However, interpretation of scenarios continues to be unresolved. There are a number of proposed definitions ranging from examples of system behavior drawn from use cases, descriptions of system usage to help understanding CST systems, and experience based narrative for requirements elicitation and validation [Sutcliffe et al., 1998]. A scenario is a description that contains actors, background information about them, and assumptions about their environment, their goals or objectives, and sequences of actions and events

[Go & Carroll, 2004]. It is a shared story among various stakeholders in system design. For example, a railway train controller in the mass-transit railway system control room can make use of scenarios to explain how he/she interacts with the signaling system to set a route for the train to proceed from point A to point B. In this example, the operator task is "set a route", but the scenario describes all relevant background information, such as the conditions for the task to be successfully completed, the operators participated (train controller and train driver), and the timing for which the task must be accomplished. Scenarios can be expressed in various media and forms, such as textual narratives, storyboards or video mock-ups.

2.3 Summary Remarks

This chapter provides a literature review on HCI, its theoretical foundation, usability and HCI development methodologies. The review is divided into two parts; the first part is related to the conceptual issues of HCI and usability, and the second part is related to the HCI development methodologies.

In the first part of the review, we explain the different between HCI and user interface, and point out that HCI covers a broader scope of interaction issues, in particular the issues of user task and contexts of usage. These issues become critical in the design of the HCI. We review the concept of cognitive psychological framework, mental model, distribution cognition and HCI modeling, which provide us a theoretical foundation of HCI in complex environment. Usability, an evaluation of HCI, is studied with the aids of Action Cycle Model [Norman, 1988] and scenarios. We also look into the concept of situation awareness, especially its application in control room environment, and the safety aspect of HCI in CST systems.

The followings summarize the findings, which provide us evident that justifies the research motivation of this thesis.

2.3.1 Underlying Paradigm

Although the researches in HCI and usability are abundant, as shown in the preceding sections above; few studies touch upon safety-critical CST systems and there are still many open issues that need to be addressed to get better support for the requirements analysis and usability evaluation of the HCI for heterogeneous safety-critical CST systems. More importantly, most studies on HCI and usability are mainly based on homogeneous system environment; few studies on the characteristics of heterogeneity of safety-critical CST systems have been attempted. The CST system's HCI for heterogeneous functionalities is not necessarily coherent; it is questionable that results generated by HCI studies on homogeneous system environment will equally applied to heterogeneous system environment. Furthermore, the operational paradigm of heterogeneous safety-critical CST systems and the role of human operators, who play a critical role in the supervisory loop, remain unchanged despite the technological development in computing, communications and automation have significant advancements in recent years. Services provided by heterogeneous safety-critical CST systems continue relying on human operators to control and monitor complex operational processes. Incoherence of heterogeneous HCI becomes a critical concern to the system operability.

It should be clear by now that what our concern is not the HCI and usability of a system in homogeneous environment, instead, what unclear to us is the HCI and usability of a heterogeneous safety-critical CST system with various domain specific systems that need to be orchestrated in a unified operational perspective. This is the main issue underlying the research questions posed in *Chapter 1, Section 1.4 – Research Statement of Problem*,

which call for new approaches on HCI requirements analysis and usability evaluation.

2.3.2 Open Issues

The underlying paradigm discussed in the above *Section 2.3.1 – Underlying Paradigm* suggests that there is currently no available approach that can support the HCI design for heterogeneous safety-critical CST systems. Although the general literature review on HCI, usability and development methodologies in this Chapter does not provide solutions directly in solving the specific problems associated to heterogeneous safety-critical CST systems, it does however provide stimulus for new ideas and it also suggests directions and generic hints for new approaches.

In *Section 2.1.1 – Human-computer Interaction versus User Interface* it shows that there are suggestions that consider context of usage and user tasks are the two key aspects of HCI design. However, it is less clear of how to include these aspects into the HCI design process. We understand that, in general, context of usage and user tasks encompass the user's work, but how these two aspects can be described, or which aspect(s) are particularly important in what situations, remains unclear. Context Analysis (Section 2.2.2) and Task Analysis (Section 2.2.3) provide guidelines and tools to examine system environment and low-level tasks in work-place. GOMS Model provides a basic direction to analyze user tasks, and GTA supplements additional techniques for analyzing complex tasks amongst a group of users. However, applications of these techniques to analyze heterogeneous system environment have yet to be discovered.

Cognitive psychological framework provides a fundamental framework to explain the rationale of HCI and to derive the human performance within the interaction. Distributed cognition further describes group cognition in order

to understand how collaborative works is coordinated to achieve common goals. These two cognitive theories facilitate the understanding of human behavior and performance in HCI, therefore application of these theories to analyze HCI requirements will definitely beneficial to the design of the HCI. However, how to make use of these two cognitive theories to analyze heterogeneous HCI requirements and usability evaluation is still unclear.

The concept of HCI modeling has several perspectives and levels in describing a system, and it is a common technique used for communication between system designers and end users. But for a heterogeneous complex system, such as the heterogeneous safety-critical CST system, the virtual machine model proposed by HCI modeling becomes unable to depict the system representation, because multiple operators (with different classes of operators) will prohibit a unified view of system representation, therefore it will become more difficult to analyze the HCI requirements from a unified point of view. Furthermore, there will have possibility that the operators will have different mental models (the third level of HCI modeling) due to heterogeneity of domain specific systems within a safety-critical CST system; in other words, operators may have inconsistent understanding of system representation and this is extremely undesirable in the design of HCI. How could we apply the concept of HCI modeling without creating inconsistent system representation becomes a challenge to any HCI development methodology.

2.3.3 **Requirements and Suggestions**

With the paradigm mentioned in the above *Section 2.3.1 – Underlying Paradigm* as a guiding principle, and the open issues from *Section 2.3.2 – Open Issues* as the potential areas to be addressed when describing a new approach to HCI requirements analysis and usability evaluation, this section

lists a number of requirements for such an approach. Thus, it sets the stage for *Chapter 4 – Methodology for Developing the Usability Evaluation Approach*, where an approach based on these requirements will be described.

If there is one thing that all analysis approaches have in common, it must be the use of objects and functions to describe the design. While there is no guarantee that this is the best basis, it does provide strong support for it. By using objects and functions, as abstractions of the artifacts and activities in the real world situation, we can derive a better picture of context of usage and user's tasks, and therefore the user's work. Furthermore, we can apply the notion of scenario (Section 2.2.4) to describe artifacts and activities associated to a specific environment, for example, a safety-critical CTS system environment.

Context Analysis described in Section 2.2.2 provides an excellent tool to analyze the technical, environmental and social settings where the CST systems will be used. Task analysis (Section 2.2.3) continues to demonstrate its powerful capability to analyze the details of work to be performed by system operators. The hierarchy of objectives and goals that shapes the work is a very useful and well understood way of describing work; however, such hierarchical approach of analysis may not be able to address non-deterministic situations, which are very common in CST systems environment, therefore we need to develop new methods to integrate the contextual information and details of work / task structures identified by these two tools to formulate a high-level concept of abstraction, so that unified requirements can be described by scenarios, which is a better descriptive tool to address non-deterministic situations.

Chapter 3

Operational Perspective of Heterogeneous Safety-critical CST Systems

Like the advancement of computing technology in recent years, people's social needs are also progressed in a rapid pace. The ever-increasing complexity of people's tasks requires them to perform open-ended intellectual tasks and discretionary decision-making. This is particularly prevalent for human operators in large-scale, complex socio-technical (CST) systems that require real-time responses. A heterogeneous safety-critical CST system involves a variety of domain specific systems that contain technical and operational processes with safety aspects. Furthermore, future CST systems must fulfill new requirements compared with today's systems. The rapid development of technology, higher expectation from general public, tighter demand for optimization in performance; and more importantly, increasing stringent statutory requirements, all make it necessary to revisit the current approaches of designing heterogeneous safety-critical CST systems.

One of the most important aspects for the success of a heterogeneous safety-critical CST system is the Human-computer Interaction (HCI) provided for the system. From the operability perspective the HCI must be efficient in both normal and disturbed work situations; and must support operational

goals of various natures. However, experience of previous projects shows that it is a difficult task to design the HCI for a heterogeneous safety-critical CST system with optimized functionality and usability. The main problem is that the design of the HCI must be based on detailed analysis of the operational tasks and associated real-time situations that the operators will face. This analysis is difficult to perform, partly because of the unavailability of appropriate analysis tools, partly because of the operators' skill is tacit and based on long time practice, and mostly because of the heterogeneous domain specific systems of a CST system do not have a coherent approach of requirement analysis. Lack of methodologies for HCI requirement analysis in heterogeneous safety-critical CST system becomes a critical issue, consequently the design of HCI fails to address all the operational requirements, thus resulting severe problems in safety and usability of the heterogeneous safety-critical CST system. There are a number of issues being studied in the HCI design for heterogeneous safety-critical CST systems, for example, multi-modal interactive devices, augmented reality and HCI mobility etc., are some of the key research areas in this field; however, in this thesis, we take a different stance to explore the HCI development process within a complex environment. The objective is to explore how the system usability can be evaluated through the HCI requirements analysis, so that the evaluation result can be used to support the design of HCI in the system development lifecycle.

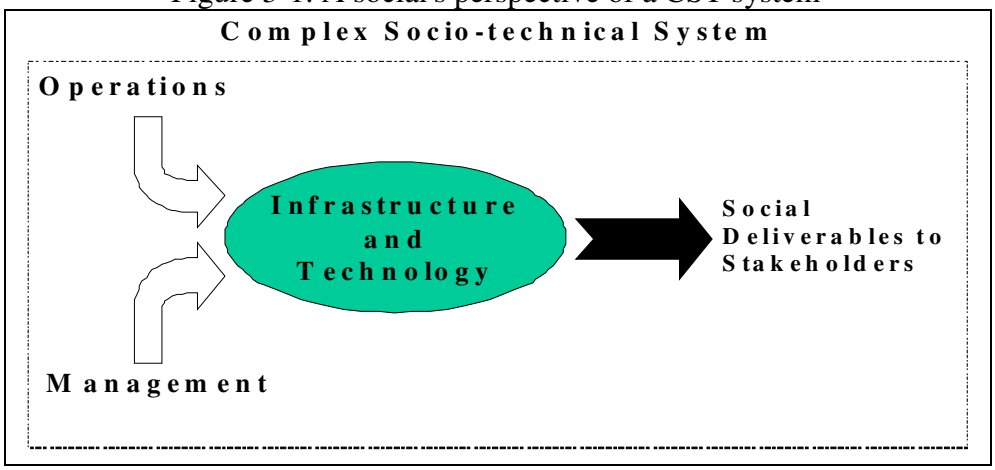
Before we offer our approach to tackle the problem, as we defined in *Chapter 1, Section 1.4 – Research Statement of Problem*, this Chapter provides an insight into the heterogeneous safety-critical CST system, from the operational perspective; and makes use of a mass-transit railway system as an example to illustrate the concept of a heterogeneous safety-critical CST system and its complexity and issues. Following the introduction of CST systems we then describe the environment of a mass-transit railway system to illustrate the heterogeneity of a safety-critical CST system. This

chapter also serves as a facilitator to acquire the foundation domain knowledge that this thesis is laid upon. Despite the fact that a mass-transit railway system comprises of various heterogeneous domain specific systems to operate, certain key elements are common to all systems' operations. These elements, which are typical characteristics in CST systems, are directly related to how the railway operators safely make use of the systems to accomplish the operational tasks; they are co-operation, collaboration, communication, co-ordination and operational safety. The following sections review in details how these fundamental elements are applied in the operations of a railway system and are linked to the analysis of HCI requirements.

3.1 Complex Socio-technical System

From the social point of view, a CST system consists of four main elements: the infrastructure and technology, the management of the system, the operations of the system and the ultimate social deliverables to stakeholders. Figure 3-1 shows the relationship of the elements within a CST system from the social's perspective.

Figure 3-1: A social's perspective of a CST system



CST systems typically have infrastructures across a number of physical sites; for example, a mass-transit railway network usually has multiple stations, tunnels and other fixed structures. Within the infrastructure there are technologies deployed for domain specific systems and applications. These applications provide the fundamental functions to comply the social obligations of the system. For example, in a mass-transit railway network, a number of technologies are equipped to provide and support various functions, such as train services, as social deliverables to the stakeholders. Computing and communication devices are equipped for the control of signaling and train movement, which subsequently provide safe and comfortable rides to the patronage. The management of a CST system provides necessary business and logistic support to the entity. The infrastructure and technology need people to operate. Since operations are carried out by human operators, how they interact with the system becomes one of the most important issues to be considered.

Much of the early HCI works were focused on the user-interface of the desktop-computing model, which included only single user and his/her associated tasks. In recent years, the user-interface research work expand the scope to field studies of workplaces, computer-supported cooperative work (CSCW), homes and other real-world and virtual-world settings. One of the key research areas in the field is the human-computer collaboration, where the operational pattern of heterogeneous safety-critical CST systems fits into the scope. Collaboration is defined as a process in which two or more agents work together to achieve common goals [Terveen, 1995]. The agents can either be system or human and this can mean either system emulating or complementing human [Fischer, 2001]. Emulation uses metaphors to present system's behavior as human-like while complement accepts that computers are not humans and uses human-center design that incorporates the human-computer asymmetry. This shifts the focus to the allocation of operators' tasks and system functionality within the system.

This is basically related to a strategy of automating parts of human contribution in complex work settings [Rognin, Salembier & Zouinar, 2000]; hence the major focus of this thesis is on the development of HCI requirements analysis that contribute to the collaboration of human and system in a heterogeneous safety-critical CST system.

From the operational perspective, to effectively operate a heterogeneous safety-critical CST system, there are four key elements that operators need to execute carefully: cooperation, collaboration, communication, and coordination. As a result, we need to examine issues on how HCI is designed to facilitate the execution of these four elements. The terms of cooperation, collaboration, communication, and coordination are ill-defined and used in a confusingly range of ways in the literature [Oravec, 1996]. In order to better understand the distinctions between these elements in a heterogeneous safety-critical CST system environment, they are defined below:

Cooperation – A form of activity that involves individuals (i.e. operators) working together, and using each other as resources for learning, sharing cognitive tasks, and as memory aids. To achieve cooperation in work, individuals must somehow coordinate their behaviors, by sharing their goals, plans and motivations with each other, together with the shared knowledge as described in *Chapter 2, Section 2.1.3 – Distributed Cognition*. When engaged in joint activities, actions must be negotiated to synchronize and co-ordinate individual activities, so as to avoid conflict. This exchange of information is managed through interaction and communication between the participants. When multiple operators are involved, coordination of activities moves outside the individual's cognitive domain into a social one, involving communication to coordinate the division of work. Group activities, as well as being made up of individual cognitive problems, also

involve building a problem space collaboratively – discovering what the collective problems are, as well as solving them collectively.

Collaboration – The work that is carried out by people who are acting together; it is a subset of cooperative work; the different is that individuals share a single goal that is larger than their individual goals [Branki, 1993]. Collaborative work is more than an individual effort: it involves the aggregation of many plans and goals held by individuals which are subsumed into a greater task. It involves agreements on the shared goals, planning the allocation of responsibility and coordination, and keeping track of goal solving progress [Terveen, 1995].

Communication – Defined as the exchange of information [Connors, Harrison and Summit, 1994]. Communication is the process by which individuals make known their wants, needs, expectations and future behaviors to others. This may be achieved through verbal and non-verbal forms. Communication is the cement that binds the organization together; the greater the need for coordination and cooperation, the greater the necessity for communication [Brehmer, 1991]. However, communication requires resources (both mental and physical) that are additional to the task being performed.

Coordination – The process that allows individuals to work together, which involves communication between the participants. [Malone and Crowston, 1993] define coordination as the act of managing interdependencies between activities to achieve a goal. Through organizing themselves into a unit, individuals can perform complex work distributed over time and space. Coordination is the means by which the distribution of labor is achieved, and may arise through the actions of an 'executive' (management role), or through emergent properties of the work that allow 'naturally arising' coordination. In the heterogeneous safety-critical CST system operation,

coordination is most likely aided by cognitive artifacts. Cognitive artifacts are tools that aid thought, and are defined as artificial devices designed to maintain, display, or operate upon information in order to serve a representational function [Norman, 1991]. It is important that cognitive artifacts flow through the system smoothly and require as little cognitive processing as possible to be interpreted or used.

Defining the relationship between these elements clarifies the nature of the operational characteristics of a heterogeneous safety-critical CST system. Communication is the mechanism used to coordinate cooperative and collaborative behavior within participants. Communication, by itself, does not cause collaboration, and simply increasing communication will not necessarily cause better collaboration. Coordination involves bringing together individuals so that they can work in a purposeful way, both dividing activities into parts that can be performed by individuals, and combining these parts back together to achieve a collective goal. This must involve communication at some stage. Collaboration appears to be mediated through socially encoded protocols [Hutchins, 1995], and it is these channels of communication that bring the actions of agents into coordination with one another to perform productive work.

If we are to propose a means of supporting the HCI design of a heterogeneous safety-critical CST system, it is essential that we understand the operation of these complex activities in order to guide the appropriate use of technological tools.

3.2 Operational Processes of Heterogeneous Safety-critical CST System

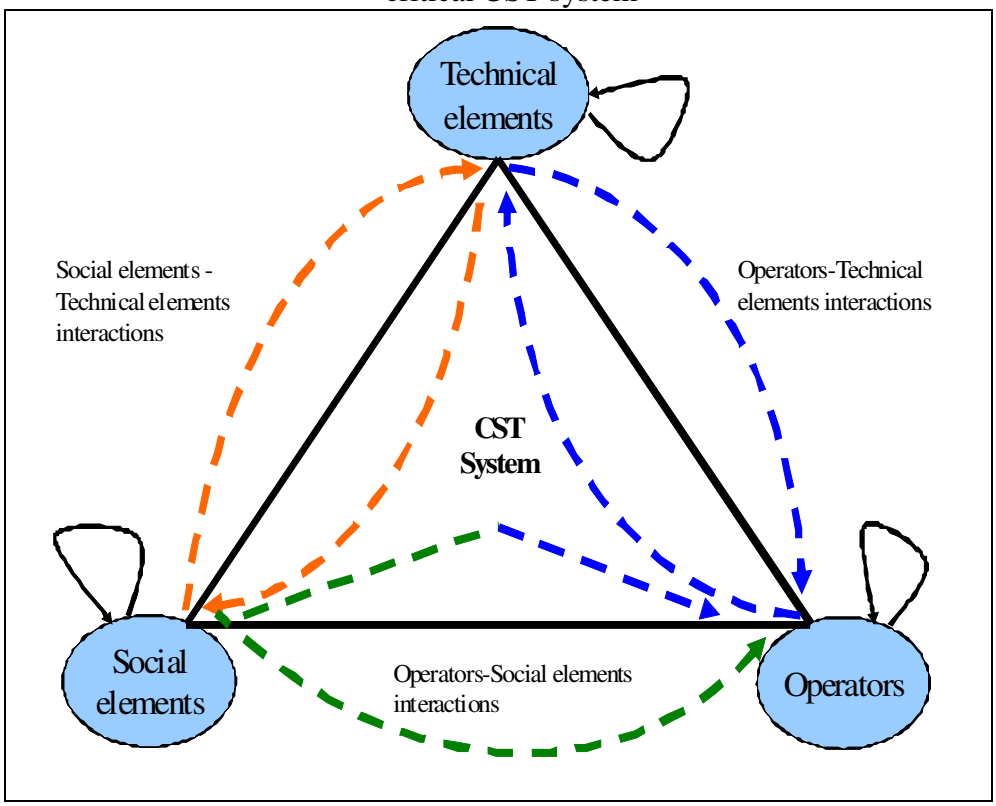
Processes within a heterogeneous safety-critical CST system include interdependencies between operators, especially the mutually dependent activities of multiple operators. These interdependencies include communication, collaboration, coordination and cooperation, formal organizational hierarchies, personal expectations, interests and qualifications [Herrmann & Loser, 1999]. There are three central operator-involved elements in a typical heterogeneous safety-critical CST system: automation of the control loop, supervisory role of operators and the dynamic nature of system-operator interaction [Cacciabue, 1997]. Firstly, automation allows machinery to carry out repetitive processes and operational tasks without (or with minimal) operator intervention. Computerized automation is now widespread but still requires collaboration with operators, for whom it is a resource among many. This creates a new spectrum of HCI and usability issues that do not exist in traditional electro-mechanical automation systems as, notwithstanding the automation of so much work, operators retain the ultimate responsibility for the entire system operations. Secondly, the primary role of operators in a heterogeneous safety-critical CST system is to supervise and monitor the overall real-time execution of the system automation in accordance with established operating procedures. The operators must know the procedures, the means and goals of control, and the system's topographical layout, physical characteristics and behavior, and ultimately the operational environment. During normal operations, operators are simply observers but during abnormal or disturbance conditions, operators must make decisions and take actions to ensure smooth running of the processes [Riera, 2001]. If the situation requires the intervention of operators, for example in implementing new procedures or

alternating the status of a process, the system's HCI provides the media for interaction. Thirdly, the interaction of a heterogeneous safety-critical CST system is dynamic and involves operators, technical systems and social elements. For example, in a mass-transit railway system, there are numerous events with regular changing status, such as a train's position and the traffic modes between peak-hour and non peak-hour. This dynamism is reflected on the interaction between operators, technical systems (e.g. train's position), and social elements (e.g. patronage in peak hour). Figure 3-2 depicts the interaction relationship between these elements within a heterogeneous safety-critical CST system. For example, in the case of the mass-transit railway system, operators in the control room may be required to interact with the system for changing the trains' running profile (operators – technical elements interaction), while at the same time communicating with other train operators (operators – operators interaction) to ensure the instructions are properly executed, which subsequently affect the punctuality of train services (technical elements – social elements interaction). The operators in the stations may also be required to communicate with passengers regarding the re-scheduling of train services (operators – social elements).

These interactions frequently have safety-critical components, which have operational processes that occur concurrently and require real-time responses from the operators. One of the major issues that HCI designers of heterogeneous safety-critical system must address is how to facilitate operators performing these complex operational tasks simultaneously. It should be noted that in a complex system the analysis is not only limited to individual operators and their tasks but also the structural relationships between organizational units [Sutcliffe, 2000]. Different stakeholders within a heterogeneous safety-critical CST system may have different criteria for design success. Hardware designers may consider the design of a technological artifact to be successful when it complies with the design

specification. Operators may consider the design is successful only when it satisfies the usability criteria. Conventional design methodologies for heterogeneous safety-critical CST systems focus on technology-driven criteria. Despite safety management is normally included in the design of heterogeneous safety-critical CST systems, but such design mainly focuses on hardware related issues. Even though human factors and safety assessment are commonly engaged in the design process, there is still lack of unified consideration amongst the heterogeneity of domain specific systems' HCI, and therefore fails to adequately take into account the safety and usability requirements of unified HCI in such a heterogeneous environment. Therefore, further research efforts are required.

Figure 3-2: The interaction relationship within a heterogeneous safety-critical CST system



The operations of heterogeneous safety-critical CST system become more challenging with the increasing number of complex operational processes.

Frequently, these processes are non-deterministic in nature and do not always produce the same result when presented with the same input criteria, as the systems' behavior is partially depended on the performance of human operators. Consequently human factors become a critical issue that needs to be addressed in the design and operations of heterogeneous safety-critical CST systems. Previous research in human factors mainly focused on ergonomic aspects of human-machine work relationship, although cognitive issues of interface design for heterogeneous safety-critical CST systems have been conducted sparsely. Ergonomic research provides detailed knowledge and guidelines for designing optimal human-machine work environment for heterogeneous safety-critical CST system, however, it cannot substitute the importance of HCI, in particular for today's heterogeneous safety-critical CST systems, because the nature of today's system operations involves a large number of abstract processes with high complexity and extensive application of virtual information representation. Process representations have become more abstract, partly contributed by computing technology now make it possible to represent processes in ways impossible on discrete instruments, and partly because increase in automation means that the operators does not interact with discrete components anymore, but rather with processes. This naturally required different types of visualization of the process. A secondary result of the use of computing technology is that the HCI is much more flexible in terms of representational and interaction modalities. This operational evolution triggers new type of research in human-machine work relationship. Therefore, we consider the HCI is the key issue in this aspect and therefore we argue that much research effort is required.

3.3 Human Operators, System Operability and HCI in Heterogeneous Safety-critical CST Systems

There are a number of operational issues in heterogeneous safety-critical systems, which are notoriously challenging. Typically, a heterogeneous safety-critical CST system has the following characteristics [Vicente, 2000]:

- Large problem space;
- Social;
- Heterogeneous perspectives;
- Distributed;
- Dynamic;
- Potentially high hazards;
- Many coupled subsystems;
- Significant use of automation;
- Uncertain data;
- Mediated interaction via computers; and
- Disturbances.

These characteristics make a heterogeneous safety-critical CST system difficult to manage. Operations of a heterogeneous safety-critical CST system are characterized by chronic conditions of information deficit; operators are frequently required to perform control tasks in which insufficient (or overloading) information and/or inadequate interface tools encumber decision and performance [Ntuen & Park et al., 1996]. In addition, working with smart machines can also suffer from negative consequences of automation, such as the out-of-the-loop performance problem, loss of situation awareness, complacency or over-trust and

automation surprises [Inagaki, 2006]. On the other hand, the operators must quickly respond to all sorts of open-ended intellectual tasks and make discretionary decision in disturbed situations that may arise from time to time. In particular when incidents occur, various sources of information for situation analysis and decision-making are coming from the user-interfaces of heterogeneous domain specific systems. Comprehension of information from heterogeneous user-interfaces becomes the bottleneck in the incident handling process. This creates a new category of probable operative errors. As summarized by [Begg, Gnocato & Moore, 1993], typical difficulties faced by operators of such systems include:

- Time pressure;
- Inconsistent and excessive amounts of information;
- Viewing information at an appropriate level of detail and in the context of operational needs;
- Navigation problems, such as the "lost of space" problem;
- Evolving operator's mental model;
- Changes in system configuration;
- Level of training; and
- Complex operational procedures.

Despite advances in computing and automation technologies in recent years, human operators are still an integral component within a heterogeneous safety-critical CST system and continue to play a specific, sometime vital, role in the operational loop. Without viable substitution, this is likely to remain to be the case in the foreseeable future. Operators may play a monitor role within the complex processes; they may also play a backup role to the automation processes. Other possible option is to make the complex processes a group of partners to operators.

Regardless the roles of operators, almost all heterogeneous safety-critical CST systems are provided with a number of system-operator interaction

facilities to enable operators to control and monitor complex processes. These facilities ranged from conventional mimic tile panels to typical personnel computers with windows, icons, menus and pointers (WIMP) input/output devices and large display boards. For example, the direct manipulation interface, commonly used in conventional computers, presents a visual representation of physical or conceptual objects and allows operators to execute actions on them to change their state, which is reflected in the interface [Shneiderman, 1998]. This one-to-one relationship between the action explicitly invoked by the operator and its feedback status introduces other kind of operational problems. The increasing use of computer-based tools and supervisory control automation has expanded the capacity of operations but has drawbacks. Many spectacular system failures were caused by human and user-interface design errors as well as failure in software functioning [Galliers, Sutcliffe, & Minocha, 1999]. For example, the much-publicized London Ambulance Service [Beynon-Davies, 1999; Finkelstein & Dowell, 1996] and Therac-25 accidents [Leveson, 1995; Leveson & Turner, 1993] were attributable to poor user-interface design as well as unreliable control software. In the London Ambulance Service's Computer-Aided Dispatch System case, the result of system failure had consequently caused the lost of 20 to 30 people lives. [Beynon-Davies, 1999] concludes that to make computing systems safer, we not only need to address the technical aspects, but also the cognitive and organizational aspects of the real-world applications. A recent study also reveals that 60% of software defects arise from usability errors, while only 15% of software defects are related to functionality [Vinter, Poulsen, & Lauesen, 1996].

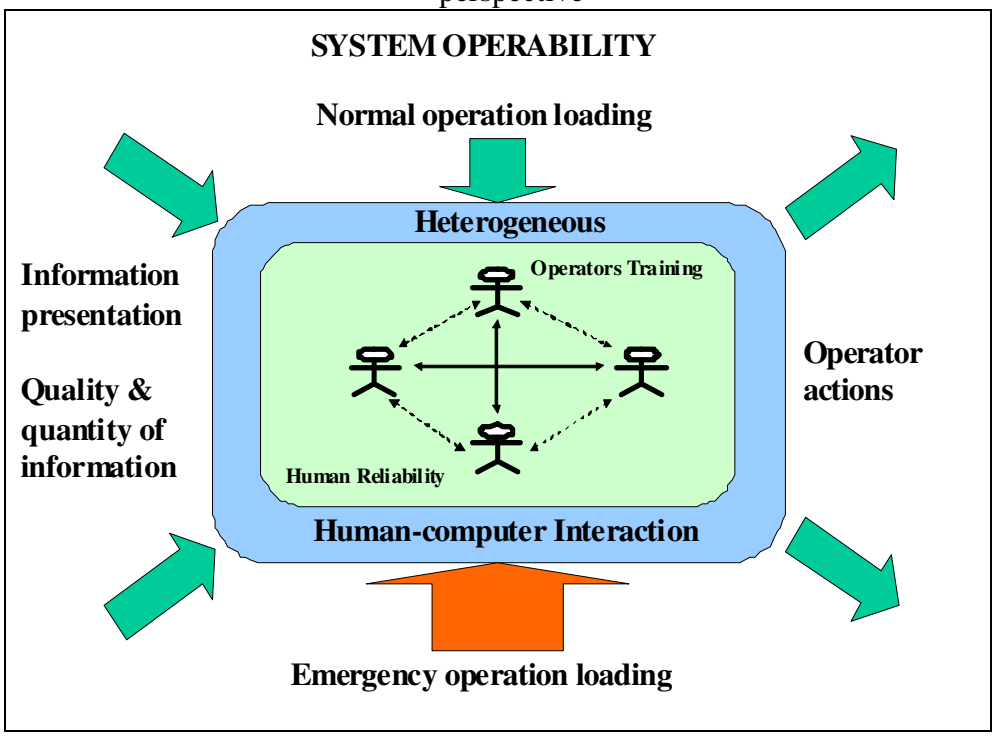
The quality of the system-operator interaction with the system is a critical success factor. In many places where heterogeneous safety-critical CST systems are part of general public's daily activities, the statutory authorities are particularly concern about the operability of these systems. From statutory authorities' perspective, the system operability of a heterogeneous

safety-critical CST system including the following issues related to how operators work with the system [Bourne & Carey, 2001]:

- The operators' ability to cope with normal, abnormal and emergency workloads;
- The operators' capability to absorb, understand and act on the information presented to them;
- Human reliability issues have been addressed in the system design process;
- Adequate training is provided; and
- System reliability is adequately catered by the design.

Figure 3-3 illustrates the concept of system operability from the statutory authorities' perspective. However, many of these issues are still open for debate and further research efforts are required.

Figure 3-3: The concept of system operability from the statutory authorities' perspective



One of the critical design aspects in the context of system operability is the HCI provided to operators, which embraces the operators' activities and is their means of communication with the outside world. The study of HCI can be traced back to the research of human factors in the operations of machinery at the beginning of last century, when there were mass deployments of various kinds of mechanical machinery. At the early stage of the emergence of interactive computer systems, the knowledge established from the study of how people operating machinery became the source of reference for investigating how people interacting with computers. This is mainly because many of the principles and guidelines for interacting with mechanical machines can also be applied to interaction with computers. HCI is a discipline concerned with the design, evaluation and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them [ACM, 1997]. Human factors, psychology and computer science become three key inter-disciplines that contribute to the development of HCI [Monk & Gilbert, 1995]. A brief history of HCI technologies can be found in [Myers, 1998]. In the past, HCI researchers and professionals helped to develop and investigate concepts and the foundation model of goals, operators, methods and selection (GOMS Model), which analyzes human performance in operating the computers [Card, Moran & Newell, 1983]. The now-pervasive graphical user interface paradigm of windows, icons, menus and pointing devices (WIMP) is one of the results of such research efforts. More details are given in [Shneiderman, 1998] and [Dix et al., 2004].

3.4 Mass-transit Railway System

Heterogeneous safety-critical CST systems exist in a variety of forms in our daily life. We encounter these systems everyday, from small-scale systems (such as the building automation system in our apartments) to large-scale systems (such as the power generation and distribution system). One of the

most critical infrastructure components in most countries across the globe is the railway network [Wilson & Norris, 2006]. Today's heterogeneous safety-critical CST system in the form of mass-transit railway system becomes a social necessity. For example, in 2010, the Hong Kong's mass-transit railway system operated by MTRC carried a total patronage to 1,608.5 million, with average weekday patronage of 3.8 million [MTRC, 2010]. People's daily life heavily relies on services provided by the mass-transit railway system. Failure in the mass-transit railway system can cause the city at a complete standstill. The heavy dependence on the mass-transit railway system imposes a significant responsibility to the service providers, which include railway companies, the government agencies that oversee public transportation and the vendors who design and built the systems for the railway companies. Due to the criticality of human performance in the delivery of railway services to the general public, a number of rail human factor research projects were carried out in 1960s and 1970s largely through the British Rail Research Center [Wilson & Norris, 2006]. However, the research issues were mainly related to the ergonomics of operating the electro-mechanical trackside devices and train-borne devices, as the computer-based systems were not available at that time. For the past three decades, computer-based systems were pervasively deployed in the rail industry. In recent years, advance computing technology are developed for the rail industry, it includes all kinds of work – from train control, to monitoring, planning and physical work with electronic tools. The settings are varied in different forms; from train driving cabs, to station control rooms and regional control centers. The environment of settings can be indoors or outdoors, to large buildings and space. The operations of the mass-transit railway system also cover a wide range of workers: signalers, electrical controllers, train controllers, drivers, station controllers, planners and maintainers of all set of different disciplines within the mass-transit railway system. The focus of this thesis is concentrated on the operational aspects of the mass-transit railway system, in particular, the HCI issues for

the operators' roles in the control room environment, therefore, other activities such as system maintenance and planning will not be discussed in the thesis.

Like other typical heterogeneous safety-critical CST systems, a mass-transit railway system operates in an environment that is unique to itself. The term "environment", as depicted by [Calvary, Coutaz & Thevenin, 2001], covers the set of objects, persons and events that are pertaining to, directly or indirectly, to current task(s) and it may have impact on the system's states and/or the user's behavior, either now or in the future. For the context of this research, the idea of "environment" is further expanded to incorporate the architectural and physical space, where the domain operations are situated in, it is because in certain operational situations physical space may determine the roles of the operators. An environment does have it own boundary, either operational or physical, which limits it coverage via operators' practice, technical constraints or operating procedures. Typically, the environment of a mass-transit railway system consists of the following architectural and physical structures, which are closely tied together to form a complete network, as shown in Figure 3-4:

- Station public and paid area;
- Operational area (station control room and central control room);
- Plant room area;
- Tunnel;
- Viaduct; and
- Maintenance facility.

More importantly a mass-transit railway system commonly consists of a variety of heterogeneous domain specific systems integrated and operated in a distributed environment.

Figure 3-4: Environment of a mass-transit railway system

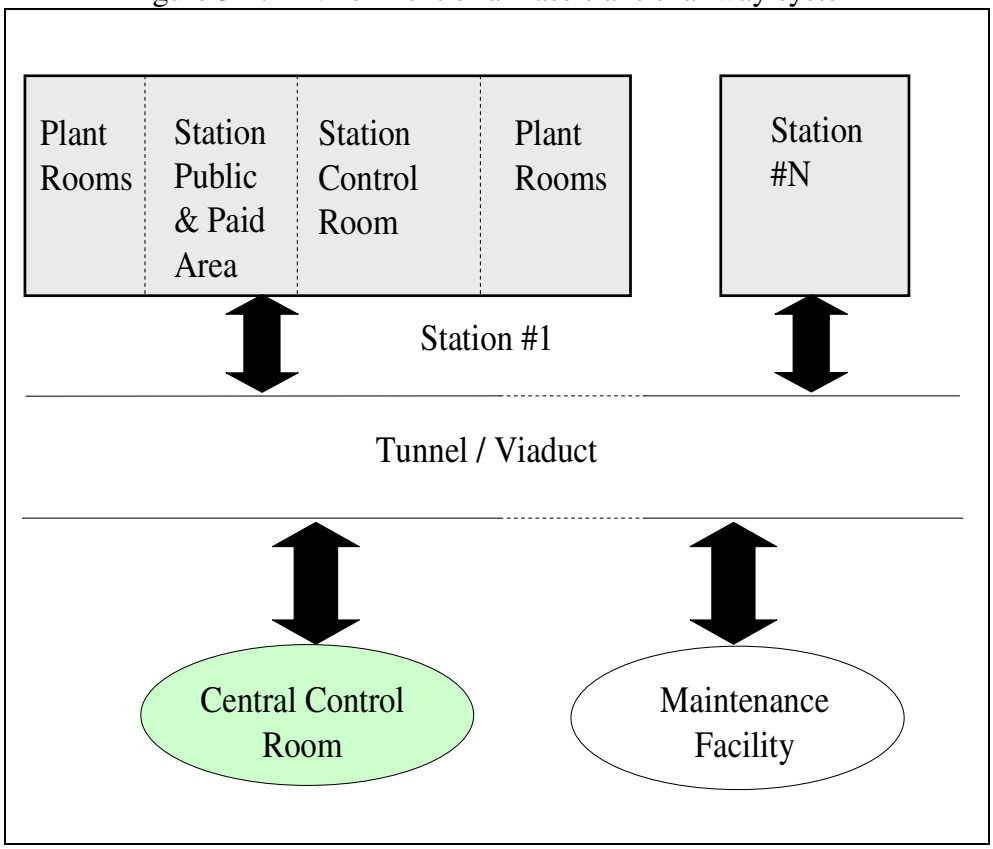
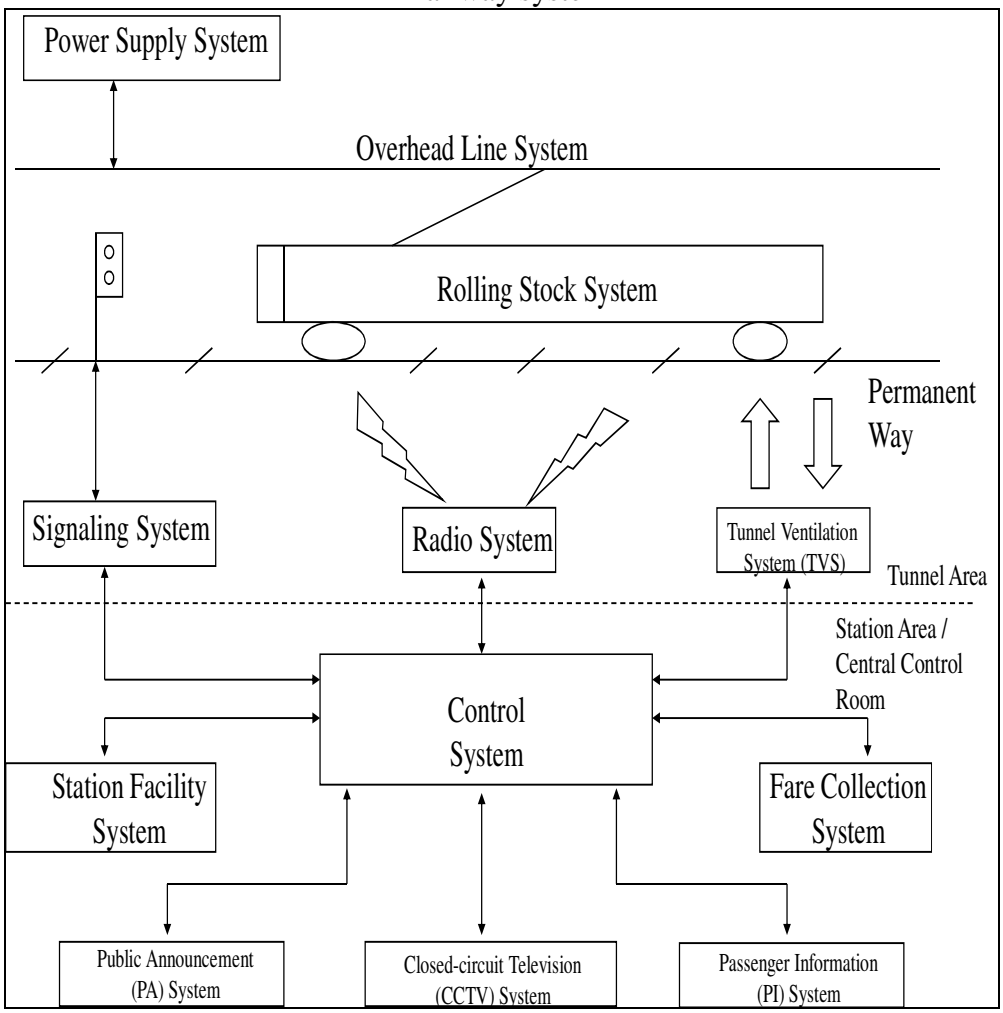


Figure 3-5 depicts a variety of heterogeneous domain specific systems in a typical mass-transit railway system. As the trains carry passengers around the railway network, the states of the majority of components within these systems are constantly changing. For example, the position of a running train and the status of proceed/stop signals for the route of this train are changing accordance with the train movement. The system characteristics and operational difficulties of a mass-transit railway system perfectly match those described in *Section 3.3 - Human Operators, System Operability and HCI in Heterogeneous Safety-critical CST Systems*. Therefore, in the thesis, we consider using a mass-transit railway system is a suitable example to illustrate the research contents of a heterogeneous safety-critical system.

Figure 3-5: Heterogeneous domain specific systems in a typical mass-transit railway system



Chapter 4

Methodology for Developing the Usability Evaluation Approach

A typical system development process commences with requirements engineering, which covers all of the activities involved in discovering, documenting, and maintaining a set of requirements for a system. The requirements engineering also include a set of processes that include requirements elicitation, requirements analysis and validation [Kotonya & Sommerville, 1998]. This is exceptionally vital to the development of heterogeneous safety-critical complex socio-technical (CST) systems; it is mainly due to the complexity and safety integrity imposed on the systems. If they fail to function as intended, the consequence could lead to human fatality, injury or damage to the environment. These system characteristics have triggered the emergence of system development standards, such as EN 50128 [CENELEC, 2001] and IEC 61508 [IEC, 1998], which are internationally accepted industrial standards for safety-related systems with electro-technical in nature. For instance, IEC 61508 applies to safety-related systems when one or more of such systems incorporate electrical and/or electronic and/or programmable electronic devices [IEC, 2002]. These standards identify mandatory processes and outcomes for software design, implementation and testing for various situations defined under a Safety Integrity Level (SIL) scheme. Despite compliance to international standards for large-scale socio-technical system development is widely mandated, the software requirements have been repeatedly recognized to be the most problematic area within the software development lifecycle

[Lamsweerde, 2000]. These problems are primarily due to the fact that in developing highly interactive software with significant Human-computer Interaction (HCI) elements, such as a heterogeneous safety-critical CST system, most software engineering methodologies do not propose any mechanisms for explicitly and empirically identifying and specifying user needs and usability requirements. They also lack the testing and validating requirements with end-users before, during and after the development. As a result, the developed systems generally meet all functional requirements, and yet are difficult to use with effectiveness, efficiency and satisfaction. Insufficient methodologies explain a large portion of the frequently observed phenomenon whereby large numbers of change requests to modify are made after the systems are deployed [Seffah & Gulliksen, 2005].

Human-centered design (HCD) and usability engineering are the notions advocated to resolve the usability issues for highly interactive systems. These notions intend to tackle the software development from the users' perspective, i.e. user-driven, rather than the traditional technology-driven philosophy. In fact, usability engineering and software engineering share some common goals and techniques, but their primary focuses are not aligned in the same direction [Seffah & Metzker, 2004]. The software development is driven by specification of functional requirements and the requirements are tied to the system that corresponds to the application itself. The focus is on the software application and the user interface is only one of the many components that have to meet the requirements. On the other hand, the HCD is more concerned about the quality of use. Its main theme and ultimate requirements are to ensure that users can perform the tasks with the application. These two perspectives can have major impact to the software development process, in particular the requirements management and quality control activities [Seffah, Desmarais & Metzker, 2005]. To bridge the gap between software development and usability, there is a specific need to establish a usability evaluation that can be incorporated as

part of the software engineering development process; this is main theme of this thesis to propose an approach to satisfy this requirement.

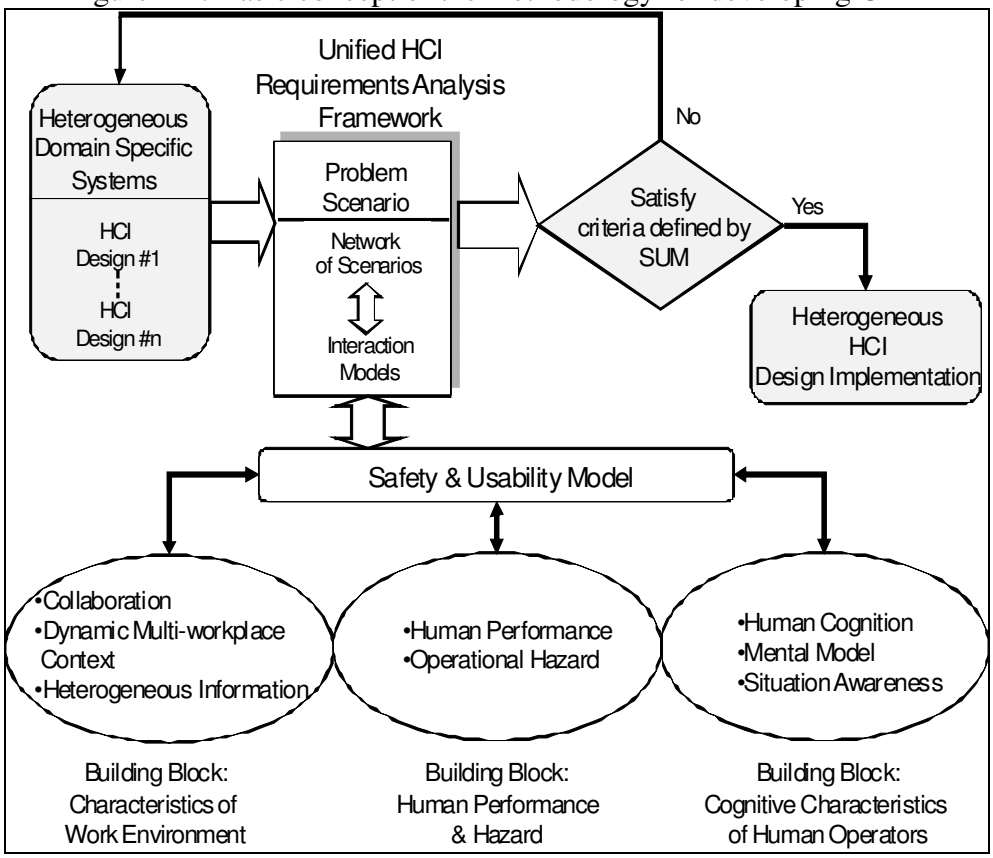
4.1 Overview

This chapter provides a detailed description of the methodology applied to develop the Usability Evaluation Approach (UEA) for evaluating the HCI of a heterogeneous safety-critical CST system. It also describes the processes that need to be executed to implement UEA. As described in *Chapter 1, Section 1.4 – Research Statement of Problem*, in the development of a heterogeneous safety-critical CST system it is a common practice that major system development and software designs of domain specific systems are completed independently before the HCI issues are collectively addressed and evaluated. This discordant between system development and HCI issues can lead to failure of compliance to system operability and make the system unsafe and less usable. To resolve these issues, the HCI requirements for a heterogeneous safety-critical CST system must be fully analyzed and understood by system stakeholders before the system design is finalized. This thesis provides UEA as a methodological approach to resolve these issues. UEA offers a Unified HCI Requirements Analysis Framework (UHRAF) for requirements analysis and also a Safety and Usability Model (SUM) to define the criteria for safety and usability, and to evaluate the safety and usability of HCI designed by heterogeneous domain specific systems, in accordance to the interaction requirements analyzed by UHRAF, with the aim of optimizing the operability of a heterogeneous safety-critical CTS system in a control room environment. UHRAF aims to address the research question 1 and research question 2 as stipulated in *Chapter One, Section 1.4 – Research Statement of Problem*, i.e. (1) how can we formulate the requirements analysis activities to facilitate the design of HCI from a number of domain specific systems in a heterogeneous safety-critical CST system; and (2) how can the heterogeneous HCI requirements

be represented explicitly from the operator's perspective of a unified system operation? SUM is proposed to answer the research question 3, i.e. how to validate the HCI analysis result and its representation can provide a solution towards the achievement of safety and usability for a heterogeneous safety-critical CST system? Both UHRAF and SUM have associated processes, which are designed to facilitate the actual implementation of the methodology.

The basic concept of the methodology used to develop UEA is shown in Figure 4-1. In the figure, the blocks with gray color are outside the scope of this thesis. Details are described in following sections.

Figure 4-1: Basic concept of the methodology for developing UEA



To evaluate usability in a complex environment, such as the operational environment of a heterogeneous safety-critical CST system, we concur with

the notion of Usability Engineering suggested by [Rosson & Carroll, 2002], which describes three perspectives contributing to the general concept of usability: (i) human performance, time and errors; (ii) human cognition and mental models of plans and actions; and (iii) collaboration, group dynamic, and workplace context. It is because the Usability Engineering's notion has precisely pointed out all fundamental issues of usability that cover a wide spectrum of HCI problems in a complex environment. However, we believe that the inclusion of safety will enrich the Usability Engineering concept to address the operability requirements of a heterogeneous safety-critical CST system. Therefore, our methodology is to extend the general concept of Usability Engineering to formulate UEA, which consists of two major components; namely UHRAF and SUM.

UHRAF creates Problem Scenario, Network of Scenarios and Interaction Models to analyze and describe the interaction that needs to be taken to achieve an operational goal. SUM will define the criteria for safety and usability, and to evaluate the safety and usability of HCI designed by heterogeneous domain specific systems, in accordance to the interaction requirements analyzed by UHRAF, for achieving the operational goal. SUM consists of three Building Blocks: (i) Characteristics of Work Environment; (ii) Human Performance and Hazard; and (iii) Cognitive Characteristics of Human Operators. UEA demonstrates explicit safety views, namely Heterogeneous Information, Operational Hazard and Situation Awareness, which are not apparent in the Usability Engineering. Details of the Building Blocks are described in the following sections.

4.2 Unified HCI Requirements Analysis Framework

The Usability Engineering suggested by [Rosson & Carroll, 2002] applies the scenario-based methodology to capture the interaction and usability requirements. It is founded on the use of scenarios as a central representation for the analysis and design of use. The basic idea is that a scenario can be used to describe an existing or envisioned system from the perspective of one or more users. Scenarios include sequences of actions and events. These actions and events may aid, obstruct, or be irrelevant to goal achievement. By using a set of user interaction scenarios, the system can be explicitly represented and therefore the analysts and designers can have a broader view of the system's usage. We concur with the fact that scenario-based methodology has advantages of describing complex processes, events and operator actions in the form of representations that are easy for communication between analysts, designers and end-users. However, the Usability Engineering emphasizes the system's interaction usability, but not apparent on the safety aspects of the HCI, despite human performance is considered in its perspective of usability. Based on the core concept of the Usability Engineering, we extend its scenario-based approach to discover scenarios in heterogeneous safety-critical CST system in order to understand the HCI requirements across a range of domain specific systems. This approach is not only able to identify HCI requirements but also detects the safety issues that are raised due to mismatch or inconsistent of interaction design between domain specific systems, for which conventional system safety engineering will not be able to discover. It is because generic system safety engineering focuses on the identification of hazards associated with a system or product and subsequent control of the residual safety risk. Operational hazards are one of the notorious hurdles

and should be avoided and mitigated by appropriate design. However, in heterogeneous safety-critical CST system, operational hazards are identified in the basis of individual domain specific systems, without a holistic view on the heterogeneity of the CST system, in particular with the HCI design. UHRAF adopts an integrated approach such that scenarios discovered will address heterogeneous HCI requirements in a unified view.

4.2.1 Scenario-based Approach of UHRAF

UHRAF extends the scenario concept of the Usability Engineering advocated by [Rosson & Carroll, 2002]; in particular it adopts the usage of scenarios to depict the control room operations of a heterogeneous safety-critical CST system.

Since the late 1980s, researchers in HCI have used scenarios as representation of system requirements to improve communication between developers and users. Software engineers look at scenarios as an effective means to discover user needs, to better embed the use of systems in work processes, and to systematically explore system behavior – under both normal and exceptional situations. The effectiveness of the use of scenarios in several disciplines is fundamentally due to their capability of stimulating thinking; scenario provides a situated task vision together with an effective way of communication among the actors involved in the subject of study [Leite et al., 2000], but without the burden to consider low-level procedures of task execution. In a heterogeneous safety-critical CST system environment it is particularly useful for scenarios to describe a set of operations and system behaviors, from a holistic view, without the need to understand the details of individual domain specific systems' concept. Scenarios can also be used in helping system stakeholders to understand the current system [Carroll, 2000], and facilitating a walkthrough of an envisaged system's behavior to discover requirements [Rolland, Souveyet,

& Achour, 1998]. However, the great variety of scenario usage in many different disciplines is probably the reason for the lack of a unified research framework in the field of scenario management [Jarke et al., 1998]; problematic issue with scenario-based methodology is that scenarios can be represented by a number of ways, and interpreted with different level of abstraction, from narrative description to detailed system behavior. [Anton & Potts, 1998] conducted a survey of different representational schemes used to represent different scenarios in HCI, object-oriented software engineering and requirements engineering. The survey result shows that different representational schemes have a wide range of forms: from informal narrative to formatted texts and more formal models. They also compared scenarios as models using concrete scenarios or instances that represent a single example of an event sequence [Anton & Potts, 1998b].

Regardless of usages and forms of representation, scenarios in heterogeneous safety-critical CST systems can be viewed as snapshots of operational events and states. From the system development's perspective, these operational events can be used to depict the target system's contextual sequence of behaviors and states can be used to set targeted results that operational tasks need to accomplish. From the HCI perspective scenario-based methods have become an accepted approach for requirements discovery and design exploration [Sutcliffe, 2003]. A number of scenario-based methodologies have been proposed by researchers, for example the SCRAM [Sutcliffe, 2002], [Sutcliffe & Ryan, 1998] and CREWS-SAVRE [Maiden et al., 1998], [Mavin & Maiden, 2003]. These methodologies have been used to elicit and analyze requirements for complex systems; their main focus is on one's system behavior and functionality. [Rosson & Carroll, 2002] have developed the Scenario-based Design (SBD) methodology for the HCI, and the scenario-based requirements analysis is the starting-point activity of the design. Analysts prepare a root concept, which consists of documents used to describe the vision, rationale,

assumptions, and stakeholders of the target system, prior carrying out the field study. The root concept is a set of documents, which is derived from various sources. For example, the vision may come from open-ended discussions among various people related to the target project. Identifying those people — the stakeholders — is also part of the root concept. The rationale may come from discussions about the current technology and problems in the target domain. Finally, listing assumptions about the project and their impacts on it can provide helpful ideas for the analysts. After preparing the root concept and questions about it, the analysts conduct field studies. They use several tools and techniques of task observation and recording to identify the problem scenarios, which illustrate and put into context the tasks and themes discovered in the field studies. [Go & Carroll, 2004] expand the definition of a scenario to cover actors, the background information about them, and the assumptions about their environment, their goals or objectives, and sequences of actions and events to accomplish tasks assigned for them. In addition, associated with a scenario is a claim, which is a description of trade-offs related to specific usability concerns with a given artifact. Claim analysis becomes an analytical evaluation method to investigate the scenario features that have significant positive or negative usability consequences.

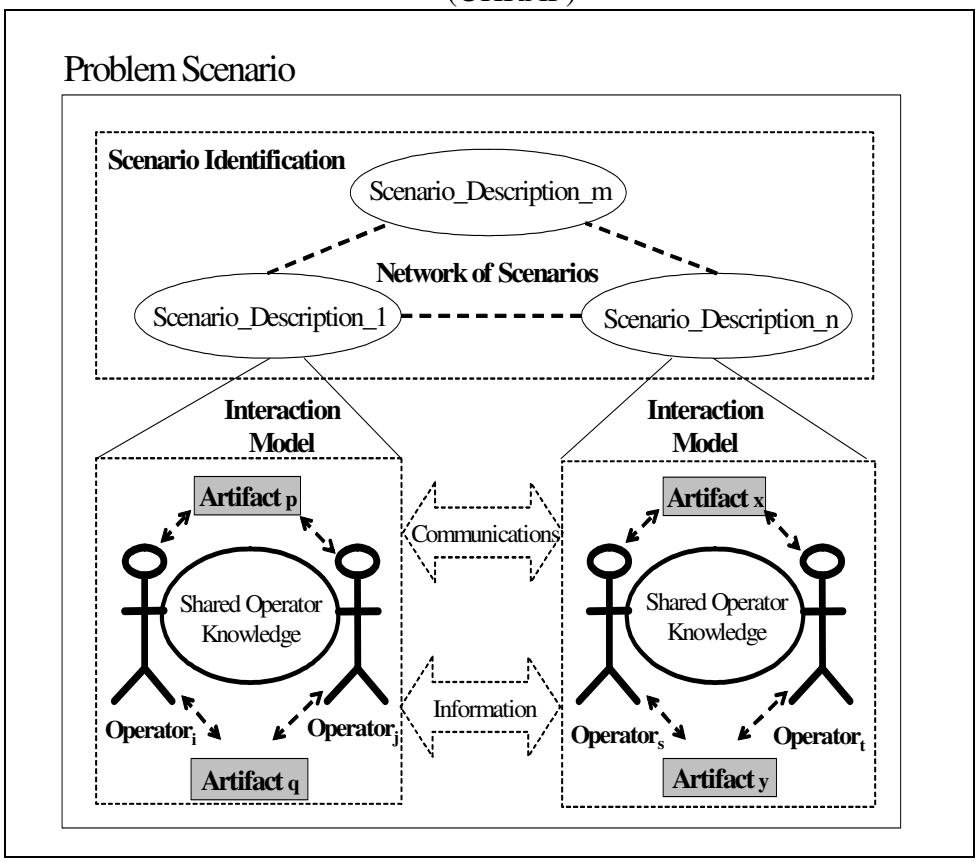
One major problem with scenario usage is how to collect a set of scenarios for requirements elicitation and analysis. More importantly, in a heterogeneous safety-critical CST system even individual domain-specific system's scenarios and context of use are available; scenarios that require collaboration of heterogeneous domain-specific systems are not trivial to be identified. For example, in a mass-transit railway system (a typical heterogeneous safety-critical CST system) there is a Traction Power Control and Monitoring System (TPC&MS) that supervises the traction power supply to the railway network, and there is also a Train Control System (TCS) that regulates and monitors all train movement. Both TPC&MS and

TCS requirements can be analyzed thoroughly with requirements analysis processes; however, during an incident of power interruption to particular track section(s), the requirement of holding train(s) and avoiding train(s) from entering an outage section(s) is not a trivial requirement that can be identified in either TPC&MS or TCS. In fact there are abundant heterogeneous functions that involve collaboration of domain specific systems for the operations of a heterogeneous safety-critical CST system. Consequently, it is a common phenomenon in a heterogeneous safety-critical CST system project that all requirements for individual domain specific systems are well analyzed, but the final system ends up with a wide heterogeneous functional gap, which is difficult and costly to fix. Under this situation, user requirements are always sacrificed. It is even worse if such heterogeneous functional gap jeopardizes the integrity of the HCI and consequently impacts the operability of the final system. To discover the heterogeneous functional gap that may impact the HCI design is one of the main purposes of our UEA.

As discussed in the above section, we concur with the benefit of adopting scenarios as a tool to analyze complex problems; because of its capability to describe complex processes, events and operator actions in form of representations that are easy for communication between analysts, designers and end-users. However, UHRAF proposed in this thesis takes a different approach to supplement the SBD by Rosson & Carroll in the analysis of interaction requirements. The main reason is that the problem domain is related to the operations of a CST system that commonly integrates a number of heterogeneous domain specific systems within a unique environment. The attention focuses on collaborative workers working in distributed multi-operational units; therefore the analysis should cover not only the stakeholder requirements but more importantly the interactions between scenarios. From the interactions between scenarios, the proposed framework also aims to identify safety and human hazard issues, which are

not apparent in the SBD. Figure 4-2 demonstrates the skeleton of UHRAF and details are explained in the following sections.

Figure 4-2: Skeleton of the Unified HCI Requirements Analysis Framework (UHRAF)

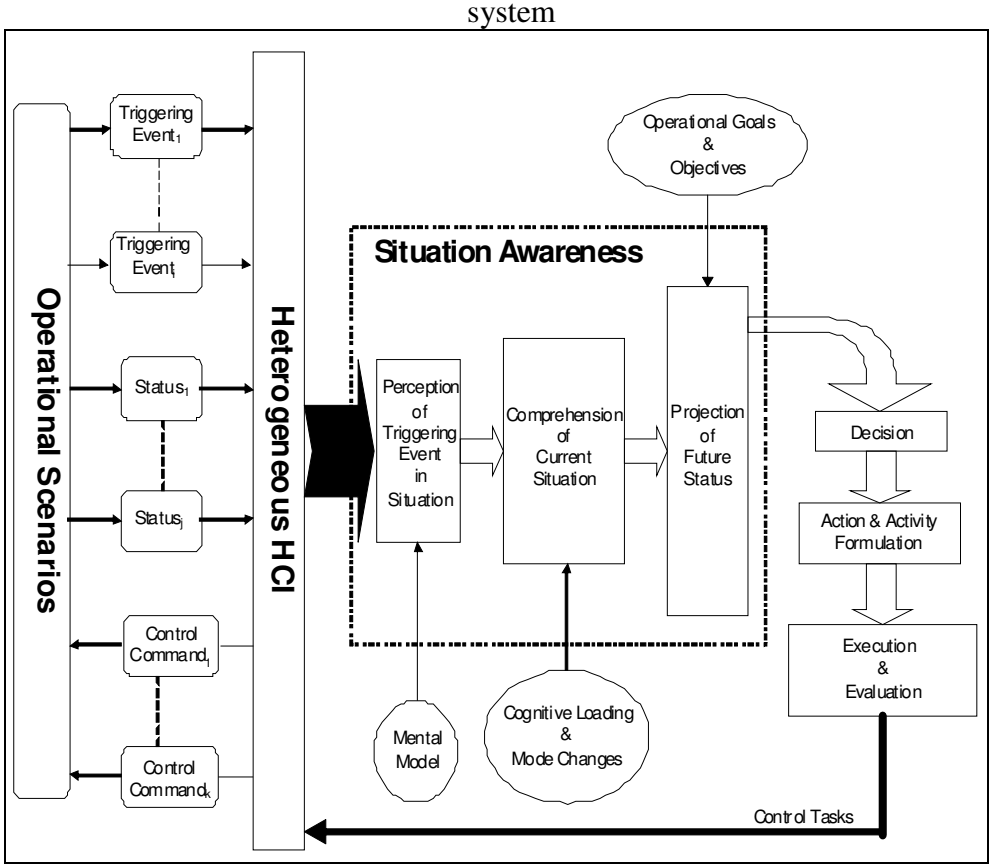


4.2.2 Typical HCI Model of Heterogeneous Safety-critical CST System

As discussed in *Chapter 2 – Background and Related Work*, situation awareness is a critical property of a heterogeneous safety-critical CST system for achieving the operability requirements; for example, operators in a mass-transit railway control room must possess situation awareness to ensure the transformation process from information perception to action is

well performed in a responsive manner. Based on this requirement, we propose a typical HCI model for a control room of a heterogeneous safety-critical CST system, as illustrated in Figure 4-3.

Figure 4-3: A typical HCI model for a heterogeneous safety-critical CST system

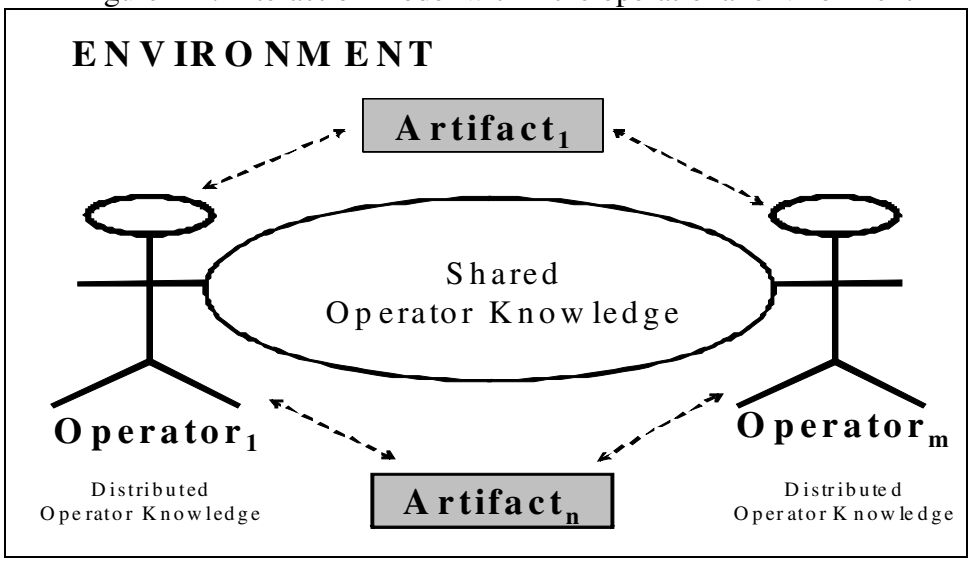


If we compare this HCI model with the system operability requirements as shown in Figure 3-3, the components "information presentation" and "quality and quantity of information" in the operability requirements are implemented by the linkage between operational scenarios and heterogeneous HCI. Operational scenarios generate system status and triggering events to operators, and also receive control commands from operators. The heterogeneous HCI are responsible for presenting this information, which then enables operators' situation awareness for subsequent decisions and actions, through a series of control tasks. This corresponds to the transformation of information received by operators to

actions performed by operators in the operability requirements. All these are related to operators' interactions, and this is the reason why in UHRAF Interaction Modeling process is needed to analysis the HCI requirements.

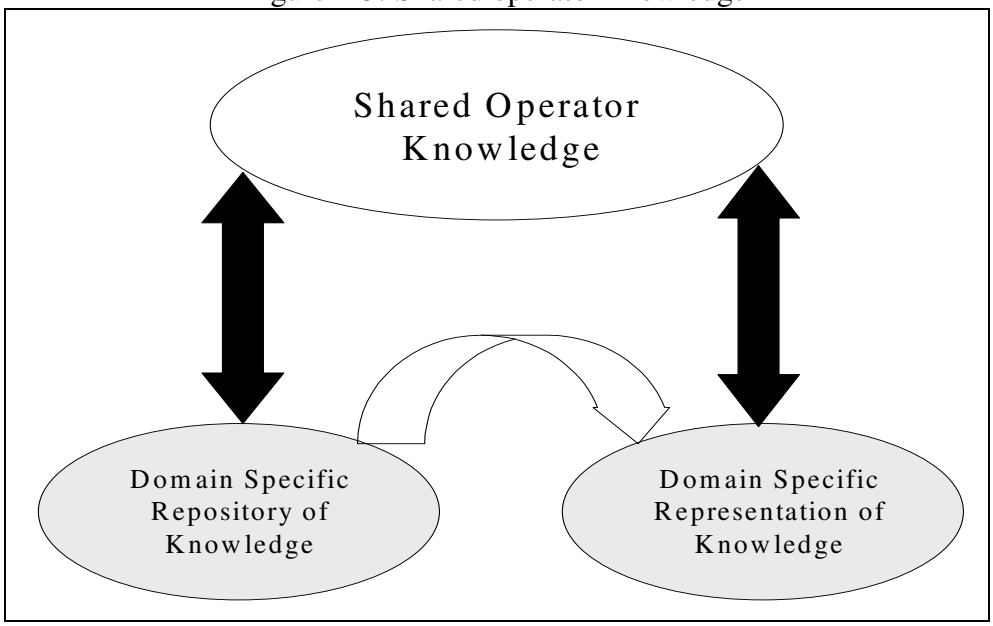
Furthermore, in a heterogeneous safe-critical CST environment, three types of interaction need to be addressed: social distribution, i.e. the interaction among people; technological distribution, i.e. interaction among people and artifacts; and the interaction among people, artifacts and work environment [Sharp, Rogers & Preece, 2007]. Figure 4-4 shows an Interaction Model within an operational environment of a heterogeneous safety-critical CST system, which consists of multi-artifact interactions. The interaction takes place between [operator$_1$ to operator$_m$] interacting with [artifact$_1$ to artifact$_n$] – a typical collaboration pattern with dynamic multi-workplace context. This Interaction Model also includes interactions between operators and agents, where agents can be intelligent devices or domain artifacts. As the interactions involve various domain artifacts, the information flowing across the Interaction Model is heterogeneous in nature, this complicates the HCI design and therefore the requirements must be carefully analyzed.

Figure 4-4: Interaction model within the operational environment



In addition, operators' knowledge can be divided into two different types; the first type is the distributed knowledge – each individual has specific knowledge, which represents a part of the complete knowledge that need to accomplish the tasks. The second type is the shared knowledge – all individuals involved in the activities share a part of the knowledge necessary to complete the tasks [Rogers & Ellis, 1994]. For example, in a mass-transit railway system, operators in the control room and the train drivers in train-cabins possess shared knowledge of how to perform certain train regulation tasks, however, they do own distributed knowledge on their respective roles in control room and train-cabins. Regardless of knowledge types, the knowledge representations amongst various domains must be understood consistently. The relationship and dependency of heterogeneous representations that derived from the shared operator knowledge, as shown in Figure 4-5, must be studied before the design of HCI can proceed. This issue will be addressed in our proposed Approach.

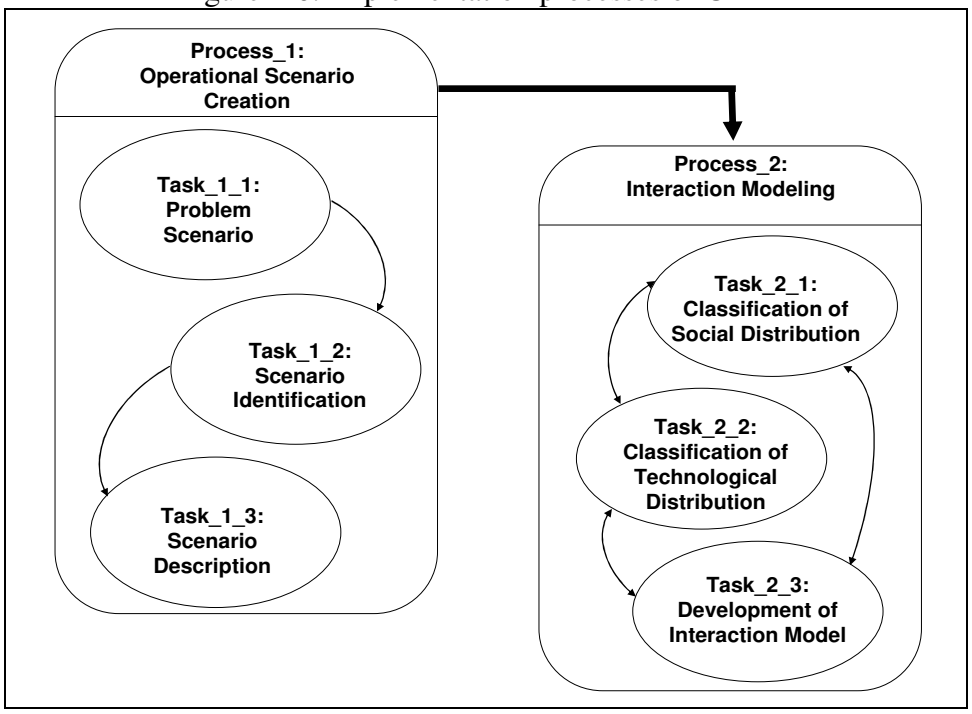
Figure 4-5: Shared operator knowledge



4.2.3 **Processes of UHRAF**

UHRAF is implemented through two simple processes executed sequentially, namely: (1) Operational Scenario Creation process; and (2) Interaction Modeling process. Each process consists of separate tasks, which may or may not be carried out sequentially. These two processes are used to generate the scenarios and all associated Interaction Models. These two processes however do not responsible for assessing the design of the heterogeneous HCI, but merely for developing the requirements criteria. Figure 4-6 illustrates the processes of implementation. The followings describe the details of each process and task.

Figure 4-6: Implementation processes of UHRAF



(1) Operational Scenario Creation Process

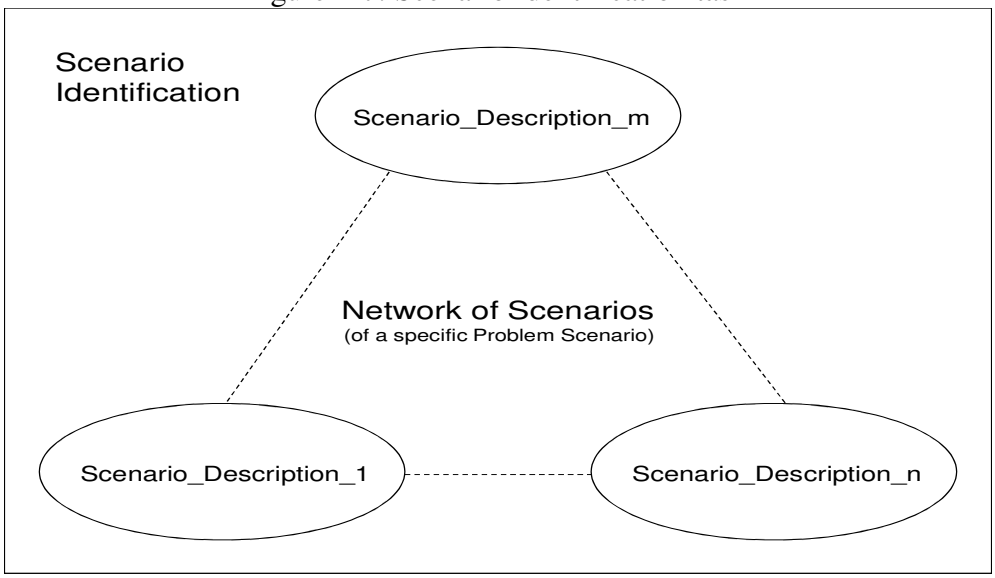
The implementation of UHRAF commences with an Operational Scenario Creation process. This process consists of three tasks: (1) Problem Scenario

task; (2) Scenario Identification task; and (3) Scenario Description task. It is the uniqueness of these three tasks, to be described below, which makes the scenarios created in UHRAF distinguish from scenarios created by other methodologies. Firstly, the Problem Scenario task is performed to create a Problem Scenario corresponding to a specific operational goal in a heterogeneous safety-critical CST system. In a typical heterogeneous safety-critical CST system, there will be numerous operational goals, which are derived from and driven by high-level social goals. For example, one of the probable social goals for a mass-transit railway system is to maintain a committed punctuality level for train services. To achieve this social goal, a number of operational goals need to be satisfied, for example, the operational goals of "train-regulation", "train-recovery from delay", or "train-dispatching from depot" etc. are the potential Problem Scenarios that need to be integrated to satisfy the high-level social goal. Consequently, each of these operational goals becomes a Problem Scenario for further analysis. Due to the complexity of the system, we develop the notion of the Network of Scenarios for a specific Problem Scenario to maintain the granularity of details for analysis. Solving a Problem Scenario is equivalent to accomplish an operational goal.

Secondly, the Scenario Identification task is followed to identify and form a Network of Scenarios, and describe each low-level scenario, for a specific Problem Scenario (see Figure 4-7). We consider the formation of a Network of Scenarios (low-level and inter-related) as being more appropriate to interaction relationship than the generic description of individual scenarios because, from the requirements analysis point of view, each Problem Scenario can be directly associated to an operational goal, which are derived and driven by high-level social goals. Furthermore, compared with the schema proposed in ScenIC [Potts, 1999], which maps the scenario-related knowledge composed of goals, objectives, tasks, and obstacles and actors, the Scenario Identification process emphasizes the

inter-relationships (information and communication means) between scenarios within the Problem Scenario, rather than the low-level details of tasks; although in the Interaction Model, to be described below, we still need to identify the actors and associated tasks for each scenario. This makes the discussions and communications between parties to be involved in the analysis share the common focus on operational goals. Tools applicable to Scenario Identification include documentation review, such as standard operating procedures, organizational structure documents, interview and observation [Dix et al., 2004].

Figure 4-7: Scenario Identification task



Thirdly, the Scenario Description task is used to provide detailed information for each scenario identified in the Network of Scenarios. A Scenario Description is defined as "a story or example of events taken from real world experience"; these stories may include details of the system context (scenes) [Sutcliffe, 2002]. The basic concept is that any operational goals, for example in a mass-transit railway system "signaling equipment failure" or "train-fire", can be used to develop Problem Scenarios and associated Network of Scenarios, which represent an existing or envisioned system operation from the perspective of the operators.

The Scenario Description contains a set of scenario elements, which includes a narration of operators' goals, plans, and actions and other relevant information. In simple terms, a Scenario Description is a story about actors, information about them and their activities, and the situation of the workplace environment. Figure 4-8 illustrates the schema of a Scenario Description and Table 4-1 provides a set of Scenario Elements defined for the Scenario Description. Ultimately, at the completion of the Operational Scenario Creation process, a Problem Scenario is defined and represented by a Network of Scenarios with associated Scenario Descriptions. Each Scenario Description does not only include all relevant actors and artifacts that must take part in the operations but also identifies the interaction requirements within the operations. Within a Scenario Description, a number of Scenario Elements are used to depict the associated interactions between operators and artifacts, as illustrated in the Interaction Model inside each Scenario Description.

Figure 4-8: Schema of Scenario Description

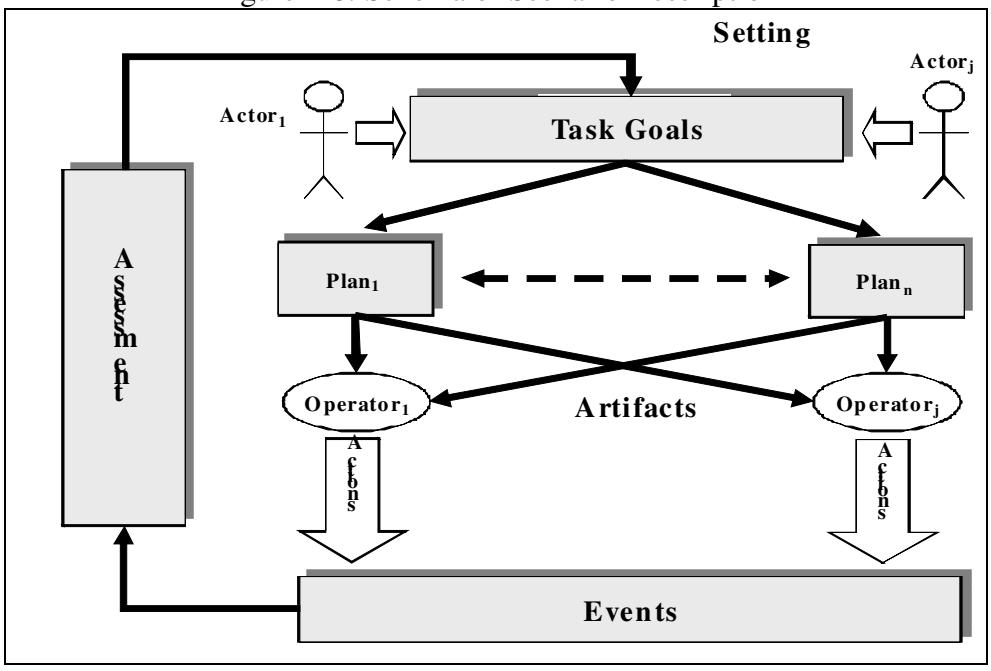


Table 4-1: Definition of Scenario Elements

Scenario Elements	**Definition**
Setting	Situational details that motivate or explain goals, actions, and reactions of the actor(s).
Actors	Operator(s) interacting with the system or other setting elements; personal characteristics relevant to scenario.
Task goals	Effects on the situation that motivate actions to be carried out by actor(s).
Plans	Mental activities directed at converting a goal into a behavior.
Artifacts	External functional entities to operators for which the interaction takes place.
Actions	Observable behavior.
Events	External actions or reactions produced by the system or other features of the setting; some of these may be hidden to the actor(s) but important to the scenario.
Assessment	Mental activities directed at interpreting features of the situation.

Furthermore, scenarios can be used to address both the size and complexity issue of the problem domain, it can reduce complexity by providing a pathway between the specific artifacts, actions or events and the abstract concept, and by suggesting a mechanism for decomposing and linking related scenarios through the Network of Scenario. It can also help to maintain a connection between domain stakeholders and system designers throughout the system development lifecycle. Tools applicable to Scenario Description include document review (e.g. SOP), interview with operators, observation, and protocol analysis, etc.

(2) Interaction Modeling Process

There are two main purposes of the Interaction Modeling process: (i) to discover the details of interactions and knowledge shared between operators and artifacts in a scenario; and (ii) to identify the details of interaction between scenarios within the Network of Scenarios, which will be captured as "communication" and "information".

After the Operational Scenario Creation process is completed, a Network of Scenario is formed and associated Scenario Descriptions are defined; however, the details of interaction between these scenarios are still needed to be defined, and inputs / outputs to these scenarios (triggering events, statuses, and control commands etc. – refer to Figure 4-3) are yet to be identified. The purpose of the Interaction Modeling process is to reveal the details of interaction amongst these scenarios, so as to understand their inputs / outputs requirements. In a heterogeneous safety-critical CST system environment, the HCI involve various domain artifacts, the information flowing across the Interaction Model is heterogeneous. Operators' knowledge is either distributed or shared; to address the issue, UEA tackles three types of interaction: social distribution; technological distribution; and the interaction among operators, artifacts, and work environment. Based on this approach, the Interaction Modeling process consists of three tasks: (1) Classification of Social Distribution; (2) Classification of Technological Distribution and (3) Development of Interaction Model.

The task: Classification of Social Distribution is to clearly identify, within a Network of Scenarios, who are the operators and what types of distributed knowledge and shared knowledge that they must acquire in order to play the roles that they are allocated in the Problem Scenario. The task: Classification of Technological Distribution, on the other hand, concerns

about the interaction between operators, artifacts and events. In UEA, artifacts are primarily the HCI within a heterogeneous safety-critical CST system; this is particular important in an environment with heterogeneous domain specific systems, for which artifacts may have different interaction characteristics. Events are generated either through the system or external parties; and both may require the attention from operators. Once we have obtained basic information from the Classification of Social Distribution task and the Classification of Technological Distribution task, then we can develop the Interaction Model. The task: Development of Interaction Model is aimed to identify the communication and information required to be exchanged within the scenarios of a Network of Scenarios. The Interaction Model consists of two levels of interaction: Level-1 Interaction (see Table 4-2) and Level-2 Interaction (see Table 4-3). Level-1 Interaction is defined as interaction that occurs within an individual scenario, and Level-2 Interaction is defined as interaction that exists between scenarios. The purpose of Level-1 Interaction is to identify the artifacts and events required or occurred for the interaction to be accomplished. Together with the information obtained from the previous two tasks, the Level-1 Interaction can be completed.

Table 4-2: Definition of Level-1 Interaction of the Interaction Model

Level-1 Interaction Elements	**Definition**
Events	Events that will be generated by the scenario, which may or may not have external impact; or external events that will trigger a course of action within the scenario.
Artifacts	Artifacts (including HCI of domain specific systems) at the disposal for operators who are involved in the scenario.
Actors	Operators who are involved in the scenarios.
Shared operator knowledge	Common knowledge that all actors involved must be able to understand and utilize (e.g. dialogue

Level-1 Interaction Elements	Definition
	protocol between operators, standard operating procedures etc).
Distributed operator knowledge	Knowledge that is only applied to individual operators who play the same function role with a scenario.

Table 4-3: Definition of Level-2 Interaction of the Interaction Model

Level-2 Interaction Elements	Definition
Communication	Patterns, formats and procedures etc. for which the information needs to be exchanged with other scenarios within the Network of Scenarios.
Information	Information that needs to be exchanged with other scenarios within the Network of Scenarios. This information will facilitate the successful completion of the course of actions in other scenarios.

The main purpose of Level-2 Interaction, which occurs between different scenarios, is to define the communication pattern and the information required for the interaction to be accomplished. The communication pattern and the information will be used to derive the input / output requirements between scenarios and therefore the entire interaction associated to a specific Problem Scenario can be discovered. It should be noted that the tasks in the Interaction Modeling process are performed iteratively and each task's outputs can be used as input to other tasks in order to refine the outcomes of the process.

4.3 Safety and Usability Model (SUM)

As described in *Section 4.1 - Overview*, our methodology is to extend the general concept of Usability Engineering to formulate the Safety and

Usability Model (SUM), which consists of three Building Blocks: (i) Characteristics of Work Environment; (ii) Human Performance and Hazard; and (iii) Cognitive Characteristics of Human Operators.

Furthermore, as described above, we put forward the notion of Problem Scenario, which consists of a Network of Scenarios and associated Interaction Models, to describe the interaction that needs to be taken to achieve an operational goal. SUM defines criteria applicable to the Problem Scenario; these criteria will then be used for evaluating against the HCI design, from a unified perspective of operability, of a heterogeneous safety-critical CST system. As described in the following sections SUM demonstrates explicit safety views, namely heterogeneous information, operational hazard and situation awareness, which are not apparent in the Usability Engineering. Details of the Building Blocks are described in the following sections.

4.3.1 Characteristics of Work Environment

In this section we describe the first Building Block of SUM, namely the Characteristics of Work Environment, and explain the rational of its significance in SUM.

In a heterogeneous safety-critical CST system, operational tasks are accomplished by utilization of information and automation systems. The system provides a variety of tasks for different operator roles under different situations. Work activities in a heterogeneous safety-critical CST system include cooperation, collaboration, communication and coordination between operators in various locations, with shared artifacts and workplaces, under the same work environment. For example, a train incident in a mass-transit railway system involves operators from different locations and different roles; operators in the affected station(s) at the vicinity of the

incident will be responsible for handling the passenger evacuation procedure, while operators at the control room will be responsible for regulating other train routings to minimize the impact of disruption caused by the incident train. As a result, we identify three main aspects in the characteristics of work environment: the collaboration of operators; the dynamic multi-workplace context and the heterogeneous information encompasses the work environment.

Research in collaboration of operators and dynamic multi-workplace context are abundance. For example, Groupware Task Analysis (GTA) and Distribution Cognition (DC) [Rogers & Ellis, 1994], to name but a few, are useful frameworks that can be used to analyze collaboration in complex environment. GTA is a task analysis conceptual framework, which is based on an integration of a variety of approaches mainly from HCI and Computer Supported Cooperative Work (CSCW). GTA focuses on agents, roles, work and situations. In order to overcome the problems of complex task models, GTA describes a task world ontology that specifies the relationships between the concepts on which the task world modeled, then based on this ontology a supporting tool to model the task knowledge is developed. DC, on the other hand, adopts different perspectives on describing and explaining how collaborative work is coordinated through group cognition. It assumes that a complex system is consisted of multiple individuals as well as the artifacts they work with, and the cognition that distributed between them; and is aimed to investigate the shared construction of knowledge. However, there is little study on heterogeneous information, which is inherited from the deployment of heterogeneous domain specific systems, and how it impacts the Characteristics of Work Environment in complex system, such as heterogeneous safety-critical CST systems.

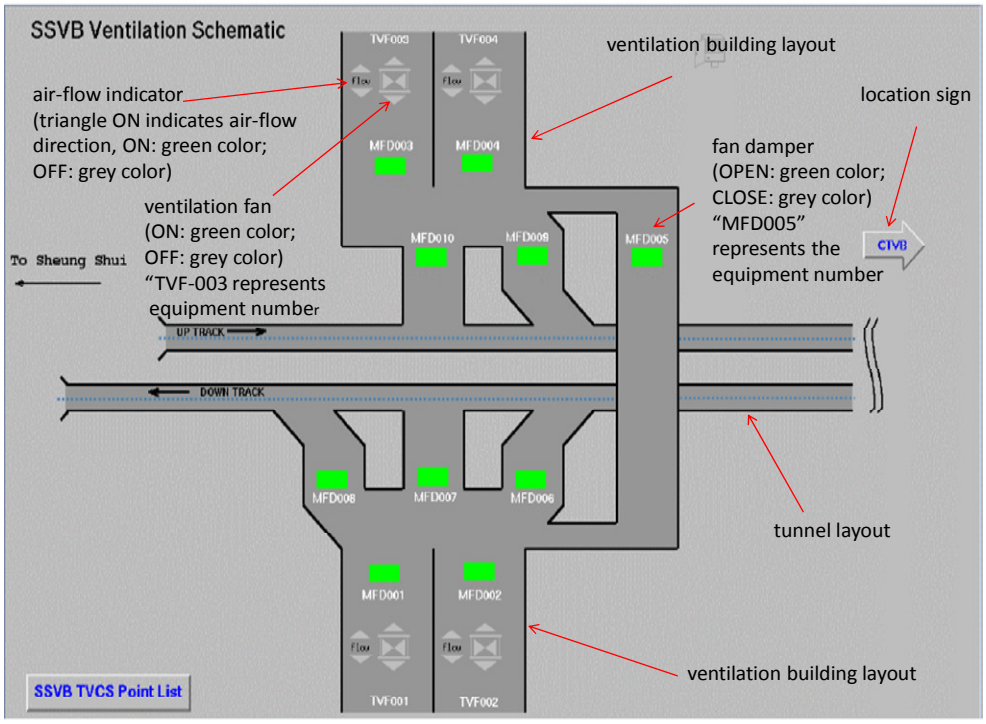
Information of a heterogeneous safety-critical CST system exists in various forms; one of the most significant forms is sign. The study of signs and

their meaning, formally called semiotics [Chandler, 2007], is particularly relevant to electronic space, for example the control room of a heterogeneous safety-critical CST system, because it is so rich in different appearances of information presentation [Hugo, 2005]. To analyze the information presented to operators in the control room of a heterogeneous safety-critical CST system, we need to determine the syntactic, semantic and pragmatic properties of the sign systems. Syntactic refers to the rules governing the structure of the signicata (the form of the sign) within a sign system. Signicata may seem relatively easy to analyze objectively, but there is no meaning in identifying signicata as part of a sign system without looking at the semantics as well. Semantic is the relation between signicata and denotata (what the sign stands for) within a sign system. Pragmatic refers to the relation between sign and sign user, in other words, in what condition the user uses a sign, and what will be the interpretation when a user uses that sign. Figure 4-9 shows an example of HCI display with domain specific signs that represent a tunnel ventilation plant in a mass-transit railway system. In this example, we have domain specific signs for tunnel ventilation fans, fan dampers, air-flow directions (air in-take and air exhaust), and railway generic signs, such as locations, track orientation and their relative geographical direction.

The control room of a heterogeneous safety-critical CST system is a complex system with a large number visual signs. These visual signs allow operators to have a basic orientation in physical as well as information space. In a mass-transit railway system, for example, the control room is commonly provided with a signaling system for traffic management, which also provides a physical orientation by reporting the trains' locations and their traveling direction. The control room is also provided with a control system for real-time stations and critical plants management. Information generated by visual signs is presented through individual systems' HCI, which is then mapped to operators' mental models to become the domain

specific knowledge. Regardless of knowledge types, heterogeneous information presented to operators amongst various domain specific systems must be understood consistently. Therefore, the relationship and dependency of heterogeneous information, including semiotics, must be evaluated to ensure the safety and usability comply with the operability requirements. Failure to do so will create information gap between heterogeneous domain specific systems, consequently operators' mental models will become unable to functioning, and thus human errors could occur.

Figure 4-9: An example of signs in the HCI display of a mass-transit railway system



4.3.2 Human Performance and Hazard

In this section we describe the second Building Block of SUM, namely the Human Performance and Hazard. One of the main purposes of deploying computing equipment in a heterogeneous safety-critical CST system is the

needs to deal with complex operational tasks. HCI within a heterogeneous safety-critical CST system is entirely different with other types of machine interaction, in the sense that it interacts in the intellectual level of performed operational tasks with abundant use of abstract concepts. Consequently new issues in human performance are raised, which go beyond the conventional human performance issues of errors. Similarly typical hazards analysis methods mainly focus on system-level components but without touch upon on human-system interaction issues.

In order to design a heterogeneous safety-critical CST system for reliable human performance, it is critical to establish a proper set of HCI, which not only serves as a tool for displaying information and acts as the interaction media between the system and the operators, but also adheres to the operational tasks to be carried out by the operators. Therefore, the HCI for reliable human performance must possess the following attributes:

- The HCI must feed operators' mental model with adequate data, to guarantee that operators are kept aware of system status.
- Operational tasks should be triggered whenever necessary by unambiguous data presentation. The HCI should provide all necessary data required to accomplish these tasks.
- The HCI should possess adequate action resources, so that the operators can control the system processes and intervene with the system's automatic behavior, through the manipulation of HCI artifacts.
- The HCI should require proper amount of operator attention, and capable of indicating clearly an erroneous operator action.

There are various techniques to predict human performance in a given mission. One of them is Human Reliability Analysis (HRA) technique, which is aimed to produce human performance reliability as a function of operator tasks and context variables. The Technique for Human Error Rate

Prediction (THERP) [Swain & Guttman, 1983], a widely used technique, is based on task decomposition and probability compounding techniques. It models human errors using probability trees and models of dependence as well as considering the performance-shaping factors affecting the operator's actions. THERP is linked to a database, which is implicitly classified into two basic error types: (i) errors of omission, by which a step or an entire task is omitted; and (ii) errors of commission, which entail selection errors (such as issuing the wrong command, or selecting the wrong control), sequence errors (such as executing a step too early in an operating procedure), and qualitative errors (such as performing too many repetitions of a particular tasks). Although HRA techniques have gained a fair degree of accuracy and experience on data treatment, only limited precious has been obtained in the modeling of human behavior and in the consideration of the cognitive components of the root causes of human error. Furthermore, the dynamic aspects of HCI are almost completely neglected in the analysis, mainly due to the intrinsic difficulty and complexity of the problem domain; and the inadequacy in the systematic approaches to safety studies.

As described in *Chapter 2, Section 2.1.7 – Safety Aspects of HCI in CST Systems*, many areas in HCI design can lead to hazards. The essential difficulty is in providing the HCI with accurate assessment of present and future system states to control the safety-critical system to achieve the desired states. Therefore, before we can evaluate whether the design of the HCI complies with the safety and usability requirements, we must first understand what will be the potential hazards and how these potential hazards will be materialized by the HCI; operational hazard becomes an area that needs to be included. Unfortunately, despite hazard analysis techniques are common they are mostly applied in system-level; and they neither are lack of focus on HCI nor integrated with general usability evaluation methods.

The Building Block of Human Performance and Hazard in SUM is to supplement the limitation of dynamic aspects of HCI in HRA techniques and lack of operational hazard perspective. Through the creation of scenarios, the dynamic nature of the system can be reflected in the HCI. The main analysis concepts of HRA and operational hazard analysis techniques will be included in this Building Block, which then work in conjunction with other Building Blocks to tackle the dynamic nature and hazard issues of heterogeneous safety-critical CST system.

In SUM, the human performance is measured by using the scenarios identified in UHRAF Network of Scenarios and their corresponding time requirements and constraints for tasks completion within the scenario. For a given scenario, operators are required to make use of the heterogeneous HCI from relevant domain specific systems to complete all actions that are necessary to accomplish all tasks in the scenario. Independent checkers will be appointed to record the time taken to complete all actions by each operator. All operator actions will be captured either in the system event logs, or other means such as video recording, for further analysis.

Operational hazard techniques will be applied to perform the analysis of all operator actions for scenarios tested. In the situation that there are operational errors and mistakes, analysts will create hazard log to capture these errors and mistakes, in particular the heterogeneous HCI artifacts of the involved domain specific systems will also be recorded. Hazard analysis will be performed to obtain a clear understanding of the hazards identified. Risk assessment technique will be used to assess the chance of occurrence of the hazards and the consequence of severity if such hazards do occur.

However, Human Performance and Hazard is only one of the Building Blocks of SUM, it should be emphasized that operational analysis

techniques will also be applied to review all assessment outputs from SUM in order to obtain an overall safety and usability perspective of the heterogeneous HCI design.

4.3.3 Cognitive Characteristics of Human Operators

The last Building Block of SUM deals with the Cognitive Characteristics of Human Operators. Cognitive characteristic of human is a major subject in psychology and there are rich research literatures in this subject. However, studies of cognitive characteristics of human operators in control room operations of heterogeneous safety-critical CST systems are relatively rare and do not particularly focus on HCI issues. Cognitive Characteristic of Human Operators is an important aspect of HCI design; in particular we consider situation awareness and mental model need to be taken into consideration when conducting usability evaluation. The following explains our rationale in this regard.

As discussed in *Chapter 2, Section 2.1.2 – Cognitive Psychological Framework and Mental Model* and *Section 2.1.6 – Situation Awareness*, mental model and situation awareness are critical properties of a heterogeneous safety-critical CST system for achieving the operability requirements, thus we consider situation awareness an element in the Building Block – Cognitive Characteristics of Human Operators. For example, operators in the control room of a mass-transit railway system must possess situation awareness to ensure the transformation process from information perception to action is well performed in a responsive manner. In the control room of a heterogeneous safety-critical CST system operators are required to execute the four key elements, i.e. cooperation, collaboration, communication and coordination, as discussed in *Chapter 3, Section 3.1 –*

Complex Socio-technical System, to ensure the system functions are performed according to the operational requirements. In such an operational environment, large quantity of real-time operational status and alarms data are collected by the system and continuously reported to the control room for operators to monitor the condition and performance of the system operations. These dynamic data coming from all over the heterogeneous domain specific systems and are presented to operators through the system's heterogeneous HCI. The operators are required to mentally integrate the heterogeneous information to form a unified picture. This unified picture becomes an internalized mental model of operator and is used to form the central organizing feature from which all decision-making processes and actions are taken place. Situation awareness can be considered as an internalized mental model of the current state of the operators in such an environment [Endsley, 2001] and thus becomes a critical property for a heterogeneous safety-critical CST system to achieve the operability requirements.

The issue becomes increasingly serious as the gap between the data generation / dissemination and the operators' ability to digest and convert the data to useful information becomes larger. It is becoming widely recognized that more data does not equivalent to more information. Automation and intelligent systems have frequently exacerbated the problem rather than resolving it. One of the explanations for this adverse drawback is the limitation of the operators' mental model. With their experience in mind, the operators develop mental models of the system they operate and the environment in which they operate. These models serve to filter out the irrelevant data and directly limit the attention in an efficient way, which provides a mean of integrating information without loading to the working memory and suggests a mechanism for generating projection of the future system's states [Endsley, 2000]. The application of mental models in achieving situation awareness is considered to be dependent on

the ability of individuals to pattern match between critical cues in the environment and elements in the mental models. However, situation awareness cannot be based on the operators' perception of all the elements that exist in the real world situation. If operators had to control complex systems and monitor individually thousands of elements, they would simply be overwhelmed by the complexity of the system [Baxter & Bass, 1998]. Alternatively, a "situation model", the current state of the mental model, i.e. an instance of the mental model, is used. For example, in the control room of a mass-transit railway system the operator can have a mental model of a passenger train, but the situation model is the current state of the train, such as the current location, train run number, direction of travel and destination etc. This situation model describes not only the operator's representation of various parameters of the system, but also a representation of how they are related in term of system forms and functions in order to create a meaningful synthesis and a comprehension of the system state. In this example, the situation model of the operator also includes an understanding of the punctuation of the train and whether remedial actions need to be taken, such as making public announcement to passengers for the delayed train. However, the use of mental model is not all positive to the situation awareness. One of the critical issues is that the mental model can lead to significant problems of biasing in selection and interpretation of information that may create errors in situation awareness. Furthermore, the quantity and format of heterogeneous information generated by the system can easily go beyond the capacity of the operators' mental model.

When emergency condition happens the operators must react quickly, effectively and accurately; the situation awareness of the operators is critical to their ability to make decisions, revise plans and act promptly to correct the abnormal situation. The HCI is the front agent for providing situation data to the operators; therefore the HCI can have a profound effect on the operational integrity of the system. This argument emphasizes the

importance of designing HCI to support the situation awareness explicitly in a heterogeneous safety-critical CST system. Furthermore, any suggestions for design trade-off between usability and safety may also affect the reliability of the cognitive processes involved with acquiring and maintaining a safe level of awareness of a situation. If the design intent is to develop a transparent HCI in the name of usability, the resulting automatic interactions may have an adverse effect on the awareness of the operators. This may also affect the safety of the system [Sandom, 1999].

Evaluating the HCI design for a heterogeneous safety-critical CST system from the perspective of operators' situation awareness with dynamic operational constraints becomes a challenging issue to system designers; this Building Block can facilitate the evaluation of HCI to ensure the Cognitive Characteristics of Human Operators is fully considered in the design.

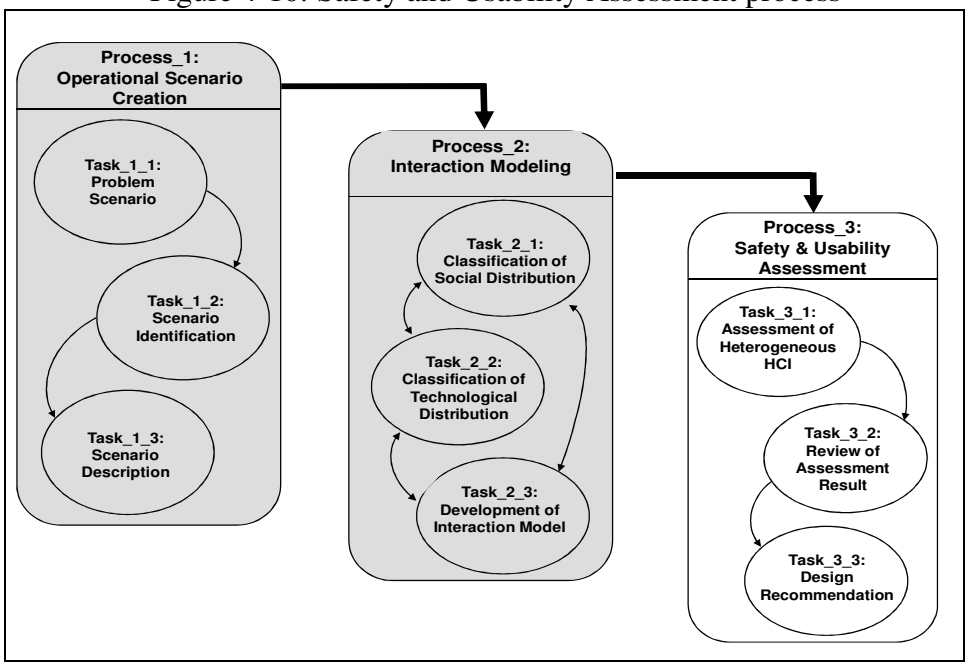
The methods will be used are (i) think-aloud; and (ii) field measurement. Similar to the methods for the Building Block: Human Performance and Hazard, the Network of Scenarios identified in UHRAF is given to the operators for performing all necessary tasks. In this Building Block, the cognitive characteristics, mental model and situation awareness are assessed, instead of the time requirements and constraints of the human performance. Think-aloud technique enables operators to express their actions' rational (originated from their mental models) of using heterogeneous HCI for accomplishing the operational tasks. Records of operators' rational are assessed in accordance to the shared operator knowledge and distributed operator knowledge identified in UHRAF. Field measurement is used to assess the response time, from the perception of situation to the projection of future status, of operators' situation awareness, through the manipulation of heterogeneous HCI. By collecting the result generated by these methods, the aspects of the Building Block: Cognitive Characteristics of Human

Operators with respect to the heterogeneous HCI design can be thoroughly evaluated.

4.3.4 Safety and Usability Assessment Process

The Safety and Usability Assessment process is the process of applying SUM to assess the results generated by the previous two UHRAF processes used to create the Network of Scenarios and all associated Interaction Models. The Safety and Usability Assessment process is responsible for assessing the heterogeneous HCI with the criteria established by SUM, and eventually proposing design recommendation. The process, as illustrated in Figure 4-10, consists of three tasks: (1) Assessment of the Heterogeneous HCI; (2) Review of the Assessment Result; and (3) Design Recommendation.

Figure 4-10: Safety and Usability Assessment process



The first task to be performed is the task: Assessment of the Heterogeneous HCI. This is to assess the heterogeneous HCI initially designed for the

specified operational goal. A set of HCI design from all domain specific systems that need to be involved to satisfy the operational goal is collected; then compare it with the Interaction Elements established by the Interaction Modeling process. The result is filled-in to the Safety and Usability Matrix (Table 4-4).

Table 4-4: Safety and Usability Matrix

Interaction Model of Scenario: Scenario_Description under the Assessment			
Building Block	Aspects		
Characteristics of Work Environment	Collaboration	Dynamic Multi-workplace Context	Heterogeneous Information
Human Performance & Hazard	Human Performance	Operational Hazard	
Cognitive Characteristics of Human Operators	Human Cognition	Mental Model	Situation Awareness

In Table 4-4, the header will be the Scenario_Description under the assessment to be performed. Each Building Block and its associated aspects are listed in the matrix; and therefore the Interaction Elements identified in the Interaction Modeling process can be assessed with respect to the aspects of the Safety and Usability Matrix. This task is repeated until assessment for all scenarios within the Network of Scenarios are completed. The assessment is conducted by operator's representatives, safety specialists, system integrators and HCI designers of respective domain specific systems. Following the assessment of the heterogeneous HCI is the task: Review of the Assessment Result. This review is focused on the overall result on the Problem Scenario, and to ensure that the assessment is completed without any missing or erroneous steps. Similar to the above task, this task also

requires the participation of operator's representatives, safety specialists, system integrators and HCI designers of respective domain specific systems. Finally, the task: Design Recommendation concludes the entire assessment for the specific Problem Scenario and suggests design recommendation that will fix any heterogeneous HCI design problems identified in the Safety and Usability Assessment process.

4.4 Summary Remark

This chapter describes in detail the methodology of the Usability Evaluation Approach (UEA) and the rational and supporting factors of developing such a methodology. UEA consists of two major components: UHRAF and SUM. UHRAF is a framework that extends the general concept of the Usability Engineering and proposes the notion of Problem Scenario and its associated Network of Scenarios and Interaction Models, as the main tool to analyze and describe the interaction requirements and activities within a heterogeneous safety-critical environment of CST system. UHRAF however does not assess the merit of usability and safety associated to the identified HCI requirements and activities. The assessment falls within the scope of SUM, a model that consists of three Building Blocks, namely (i) Characteristic of Work Environment; (ii) Human Performance and Hazard; and (iii) Cognitive Characteristics of Human Operators. These three Building Block cover issues that conventional safety analysis tools and usability techniques do not addressed, and the aim is to evaluate the usability and safety of a heterogeneous safety-critical CST system, from a unified operational perspective, instead of individual domain specific system's perspective for which most other scenario-based methodologies is based on.

Implementation of the UEA is realized by the execution of processes developed for UHRAF and SUM. These processes are simple in term of

execution and without the needs of specific tools, other than common requirements analysis tools. The result generated by these processes is to discover usability and safety issues, which can be used to provide important design feedback to HCI design. In particular, UEA demonstrates explicit safety views, namely heterogeneous information, operational hazards and situation awareness, which are not apparent in the Usability Engineering and other scenario-based methodologies.

Chapter 5

Application of the Usability Evaluation Approach

In Chapter 4, we have described the methodology of developing the Usability Evaluation Approach (UEA) and the processes that facilitate its implementation. In this chapter we demonstrate the application of UEA to an operational environment of a mass-transit railway system, which is a typical heterogeneous safety-critical complex socio-technical (CST) system, to test the Human-computer Interaction (HCI) designed by heterogeneous domain specific systems; and aiming for resolving an operational issue – handling a railway tunnel train-fire incident scenario.

A mass-transit railway system operates in a unique environment; this environment possesses all elements defined by [Calvary, Coutaz & Thevenin, 2001], which covers the set of objects, persons and events that pertain, directly or indirectly, to current task(s) and which may impact the system's states and/or the user's behavior, either now or in the future. In addition, it has boundaries, operational or physical, which define the scope of operators' roles and technical constraints. Typically, modern mass-transit railway systems can be divided into 3 levels of operations: track-related (including trains), station-based and control room level. This research mainly focuses on the heterogeneous HCI issues of control room operations and therefore other levels of operations will not be discussed. The operational environment of the scenario under tested is related to the design of heterogeneous HCI for the tunnel train-fire incident. The railway under

study is the LMC Spur Line, a 7.4km extension of the MTR East Rail Line in the Hong Kong Special Administrative Region (HKSAR).

5.1 Overview of the Operational Environment

The LMC Spur Line, approximately 7.4km, is an extension of the MTR Corporation's (MTRC) East Rail Line (ERL) in the HKSAR of the People's Republic of China (PRC). The LMC Spur Line was commissioned and opened for revenue services in August 2007. The tunnel portion of the LMC Spur Line, approximately 4.5km with separate up and down lines, is equipped with heterogeneous computer control & communication systems for various domain specific applications; this is considered as a typical heterogeneous safety-critical CST system. It is a statutory requirement for the railway systems' design to incorporate the tunnel train-fire incident as a probable operational scenario. To address this requirement a mechanism must be provided in the tunnel for smoke proliferation control, so that during the tunnel train-fire incident a smoke-free path can be established for passenger evacuation. One of the most challenging design issues is how to identify the HCI requirements and develop the interaction model to handle this operational scenario. The following sections describe in details how UEA was used to analyze and evaluate the HCI problem and how the findings were used to guide the HCI design.

To address the above-mentioned statutory requirement of providing a smoke-free path for passenger evacuation during a tunnel train-fire incident, there are three critical domain specific systems involved in the handling of a tunnel train-fire incident: the Train Control System (TCS); the Tunnel Ventilation System (TVS) and the Integrated Control & Communications System (ICCS). TCS provides a fixed-block signaling system with Automatic Train Protection (ATP) and Automatic Train Operations (ATO) for train movement according to the required operational headway and time-

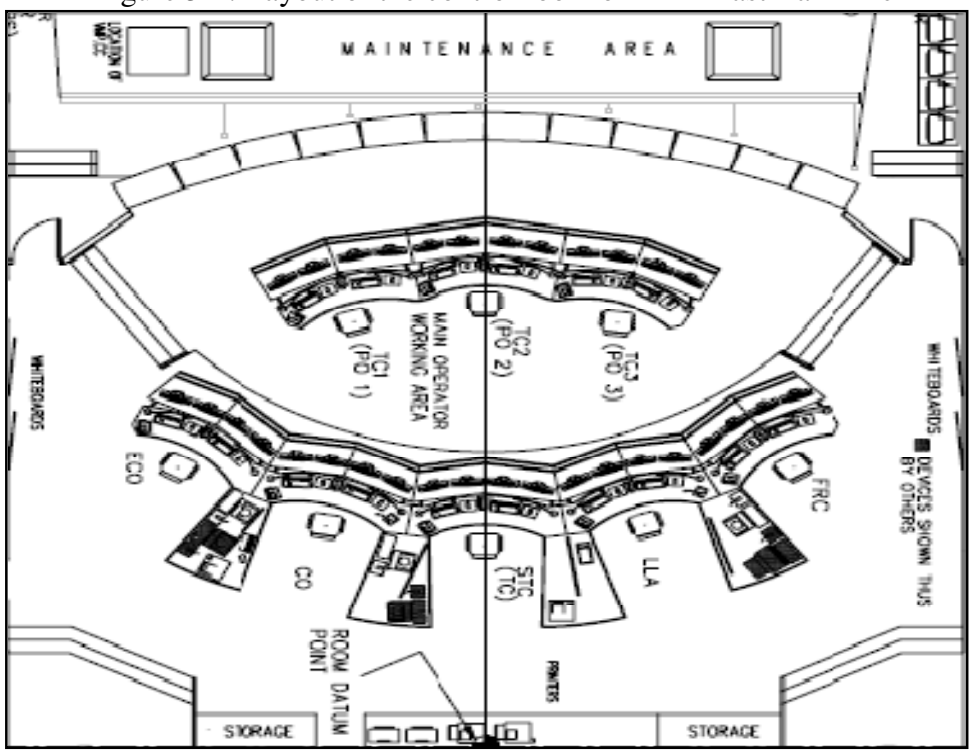
table schedules. TVS consists of electro-mechanical equipment such as ventilation fans, air dampers and associated Programmable Logic Controllers (PLC); it ventilates the tunnels to control smoke spread during tunnel train-fire incidents through the execution of emergency mode (an emergency mode is defined as a pattern of ventilation fans' operations with their associated dampers' settings specifically for different tunnel train-fire scenarios). ICCS interfaces with both TVS and TCS to provide the integrated control and monitoring functions for operators in the control room.

The control room is the nerve center for operators to perform railway traffic control and monitoring functions. Figure 5-1 illustrates the control room of MTR East Rail Line.

Operators in the control room are structurally organized into different roles. The Train Controllers (TC1, TC2 & TC3) are responsible for managing the train movement within their region of authority. Depending on the length of the railway, the region of authority can cover the whole railway line, or just a portion of the railway line. Their main duties include train dispatching, route setting and communicating with train drivers for train service regulation. The Senior Train Controller (STC) is the person-in-charge of the control room. He/she is responsible for overseeing the entire railway operations within his/her jurisdiction. The Control Officer (CO) is the assistant to STC for general coordination with external parties. There are other operators in the control room to carry out essential functions for railway operations. The Electrical Control Officer (ECO) is responsible for supervising the electrical traction power supply to the railway system. If the railway alignment has tunnels, he/she is also responsible for control and monitoring of TVS operations. When there is specific traffic rescheduling the Long Line Announcer (LLA) is responsible for communicating with passengers through public announcement. The duty supervisor of the Fault

Report Center (FRC) is responsible for monitoring the performance and conditions of equipment and devices installed along the railway.

Figure 5-1: Layout of the control room of MTR East Rail Line



One of the problems faced by the mass-transit railway system is the concurrent development of heterogeneous domain specific systems. For example, in MTR East Rail Line TCS is provided for train scheduling, traffic monitoring, route setting and related control functions; the Radio System is provided for voice communication between operators in the control room and train drivers; and ICCS is provided for supervisory control and data acquisition (SCADA) of power supply equipment, tunnel ventilation equipment and other critical field equipment. Common HCI design practice and usability guidelines for individual domain specific systems are followed by respective system designers; however, unified approach to system operability is not guaranteed. This situation is exactly the same as what we have defined in the research statement of problem. The discordant of system development and HCI issues between

heterogeneous domain specific systems can lead to failure of compliance to system operability and can make the system unsafe and less usable. The following sections reveal the problem in more details and illustrate how UEA was applied to test the tunnel train-fire scenario.

5.2 Heterogeneous HCI Design Problem

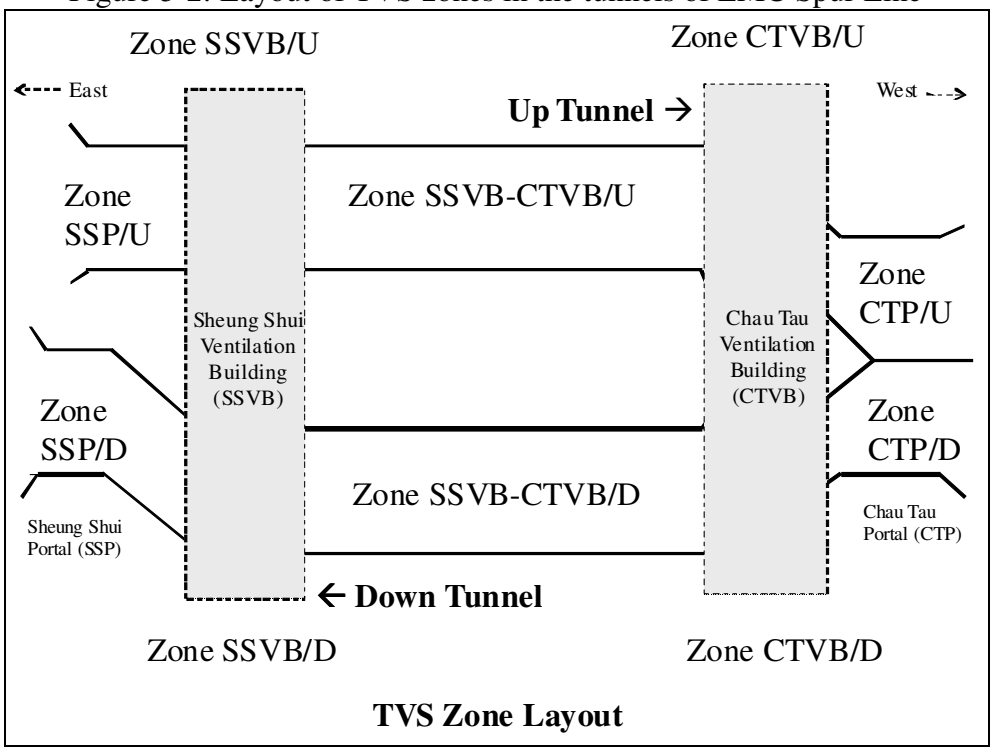
Before we apply UEA to test the tunnel train-fire scenario, we need to understand the heterogeneous HCI design problem of the mass-transit railway system. In the following sections, we explain a few domain specific concepts for which the railway operation is based on.

5.2.1 Tunnel Ventilation and Its Design Concept

The first domain specific system within the mass-transit railway system that needs to be involved in the operation of the tunnel train-fire scenario is the Tunnel Ventilation System (TVS). Tunnel train-fire is a scenario that all railway operators will try their best effort to avoid it from happening; however, as a safety precaution, preventive provision must be in place so that if train-fire incident does happen inside the tunnel, the impact to passenger safety can be reduced to minimum. Therefore, tunnel ventilation equipment is commonly installed along the tunnels as a statutory requirement; this includes mechanical ventilation equipment and computer control and communication equipment, collectively called a TVS. The purpose of TVS is to control the proliferation of smoke during tunnel train-fire scenario, so that a clear pathway can be established for the passengers to evacuate. In order to reduce the construction and equipment costs, and spatial requirements for equipment, tunnel ventilation is usually designed and implemented in a special way, such that maximum ventilation efficiency can be achieved with minimum requirements of ventilation equipment. Based on these design constraints to TVS, a “zone” concept is

used to achieve such design target. A TVS zone is defined as a section within the tunnel for which specific coverage of TVS emergency mode is designed. A tunnel is normally divided into a number of zones. Each zone will be handled by a set of emergency modes, and each set of emergency mode can handle a number of zones. Figure 5-2 shows the layout of TVS zones of the tunnels for the LMC Spur Line.

Figure 5-2: Layout of TVS zones in the tunnels of LMC Spur Line



The LMC Spur Line consists of an up line tunnel and a down line tunnel, with two ventilation buildings (SSVB and CTVB) in between; and each tunnel is divided into 5 TVS zones. Each zone is identified by a zone name, for example, Zone "SSP/U" and Zone "SSVB/U" etc ("U" stands for up; "D" stands for down). Totally there are 10 different zones, 5 for the up tunnel and 5 for the down tunnel. Table 5-1 lists all the zones defined for the LMC tunnels (both up and down). The allocation of each zone will normally depend on the location of the ventilation buildings and other ventilation

facilities, but does not directly related to the length of the tunnel sections, so there are zones with various physical lengths.

Table 5-1: TVS Zone description for the LMC tunnels (both up tunnel and down tunnel)

TVS Zone Description	**Up Track Zone Name**	**Down Track Zone Name**
Chau Tau Portal. The area to the west of CTVB.	CTP/U	CTP/D
The area around CTVB.	CTVB/U	CTVB/D
The area between SSVB and CTVB.	SSVB-CTVB/U	SSVB-CTVB/D
The area around SSVB.	SSVB/U	SSVB/D
Shueng Shui Portal. The area to the east of SSVB.	SSP/U	SSP/D

5.2.2 TVS Emergency Modes

To establish a smoke-free pathway during the tunnel train-fire incident for passengers to evacuate from the tunnel's incident point, the ventilation equipment (ventilation fans and dampers etc.) must be operated in an organized manner. In general, one end of the ventilation must be operated in "supply" mode, i.e. supplying fresh air to the tunnel, and the opposite end must be operated in "exhaust" mode, i.e. exhausting smoke out of the tunnel. Passengers will need to evacuate toward the direction where fresh air is supplied from. Based on this simple ventilation principle, a set of emergency mode are created. An emergency mode is defined as a pattern of ventilation fans' operations with their associated damper settings specifically for different tunnel train-fire scenarios. Each emergency mode is designed to serve a number of tunnel train-fire scenarios; each tunnel train-fire scenario is defined with attributes of specific TVS zone(s)

occupied by the incident train and passenger evacuation direction. Due to the varying physical lengths of the TVS zones for the LMC Spur Line tunnels, an incident train (of fixed length) may occupy up to three TVS zones. Table 5-2 shows a list of 13 emergency modes for the tunnels of LMC Spur Line. Emergency modes F1 to F6 are designed for the up tunnel and F7 to F12 are designed for the down tunnel.

The "Mode Number" in Table 5-2 represents a unique number for identifying a specific TVS emergency mode. The "Mode Name" indicates the passenger evacuation direction and provides a brief description of the relative fire location (rear, middle and front) inside the train. The "Incident Train & Fire Location" describes the fire location and the occupancy of the incident train with respect to the TVS zone(s).

Table 5-2: Emergency modes for the tunnels of LMC Spur Line

Mode Number	Mode Name	Incident Train & Fire Location
F1	EVACUATION TOWARDS LMC Rear Train Fire at Sheung Shui Portal Tunnel (UP)	Up Track -Rear train fire at SSP/U only ; or SSVB/U & SSP/U only.
F2	EVACUATION TOWARDS SHS Front Train Fire at Sheung Shui Portal Tunnel or under SSVB (UP)	Up Track - Front train fire at SSP/U only; or SSVB/U & SSP/U only; or SSVB-CTVB/U & SSVB/U & SSP/U only.
F3	EVACUATION TOWARDS LMC Rear Train Fire at Central Tunnel or under SSVB (UP)	Up Track - Rear train fire at SSVB-CTVB/U & SSVB/U only; or SSVB-CTVB/U only; or CTVB/U & SSVB-CTVB/U only; or SSVB-CTVB/U & SSVB/U & SSP/U.

Mode Number	Mode Name	Incident Train & Fire Location
F4	EVACUATION TOWARDS SHS Front Train Fire at Central Tunnel or under CTVB (UP)	Up Track - Front train fire at SSVB-CTVB/U & SSVB/U only; or SSVB-CTVB/U only; or CTVB/U & SSVB-CTVB/U only; or SSVB-CTVB/U & CTVB/U & CTP/U only.
F5	EVACUATION TOWARDS LMC Rear Train Fire at Chau Tau Portal Tunnel or under CTVB (UP)	Up Track - Rear train fire at CTP/U only; or CTVB/U & CTP/U only; or SSVB-CTVB/U & CTVB/U & CTP/U only.
F6	EVACUATION TOWARDS SHS Front Train Fire at Chau Tau Portal Tunnel (UP)	Up Track - Front Train fire at CTP/U only; or CTVB/U & CTP/U only.
F7	EVACUATION TOWARDS LMC Front Train Fire at Sheung Shui Portal Tunnel (DN)	Down Track - Front Train fire at SSP/D only.
F7X	EVACUATION TOWARDS LMC Front Train Fire under SSVB (DN)	Down Track – Front Train fire at SSP/D & SSVB/D only; or SSP/D & SSVB/D & SSVB-CTVB/D only.
F8	EVACUATION TOWARDS SHS Rear Train Fire at Sheung Shui Portal Tunnel or under SSVB (DN)	Down Track - Rear Train fire at SSP/D only; or SSP/D & SSVB/D only; or SSP/D & SSVB/D & SSVB-CTVB/D only.
F9	EVACUATION TOWARDS LMC Front Train Fire at Central Tunnel (DN)	Down Track - Front Train fire at SSVB/D & SSVB-CTVB/D only; or SSVB-CTVB/D only; or CTVB/D & SSVB-CTVB/D

Mode Number	Mode Name	Incident Train & Fire Location
		only.
F10	EVACUATION TOWARDS SHS Rear Train Fire at Central Tunnel or under CTVB (DN)	Down Track - Rear Train fire at SSVB/D & SSVB-CTVB/D only; or SSVB-CTVB/D only; or CTVB/D & SSVB-CTVB/D; or SSVB-CTVB/D & CTVB/D & CTP/D.
F11	EVACUATION TOWARDS LMC Front Train Fire at Chau Tau Portal Tunnel or under CTVB (DN)	Down Track - Front Train fire at CTP/D only; or CTVB/D & CTP/D only; or SSVB-CTVB/D & CTVB/D & CTP/D only.
F12	EVACUATION TOWARDS SHS Rear Train Fire at Chau Tau Portal Tunnel (DN)	Down Track - Rear Train fire at CTP/D only; or CTVB/D & CTP/D only.

5.2.3 Train Control System and Monitoring of Train Position

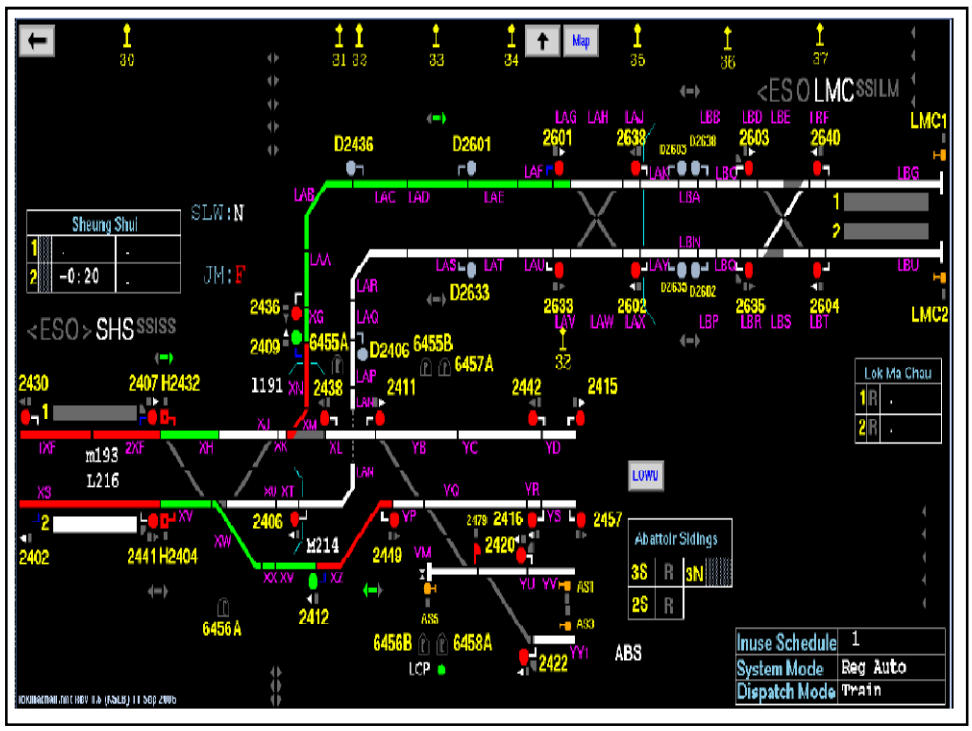
The second domain specific system within the mass-transit railway system that needs to be involved in the operation of the tunnel train-fire scenario is the Train Control System (TCS). TCS mainly provides automatic control of train movement (for example, setting a route from the departure station to a destination station) and tracking of train positions. It is a mission critical requirement that all trains on the running lines must be tracked and their updated positions reported back to the control room as they travel along the running lines, regardless of whether they are in-service or out-of-service.

The operators in the control room continuously monitor all train movement to ensure the train service is running properly as per the service schedule.

The train tracking mechanism is realized by the occupancy of a set of consecutive track circuit(s) by the relevant train. Each track circuit is given a logical name and represents a section of the physical railway track and is electrically connected to the detection equipment in the Signaling Equipment Room within the associated station. The position of a train is detected by the occupancy of a set of consecutive track circuit(s) when the train is located on the specific track(s). This will in turn send the occupancy signals to the computers in the control room for further processing. From the HCI perspective, TCS' HCI indicates in real-time the position of a train by displaying (i) the track circuit(s) being occupied; and (ii) the unique Train Run Number (TRN) associated to the train, and both are using domain specific semiotics to represent the displayed objects. In practice, the TCS HCI will show the tracking of trains in a form of occupy/un-occupy of track circuits and the stepping of TRN on the display. Figure 5-3 illustrates, as an example, the TCS HCI displays of the LMC Spur Line. In addition to the dynamic real time train information, TCH HCI displays also show specific static information, which is relevant operational information for the operators, such as the name of the track circuits, signage information for operators and other relevant geographical and signaling information for the operators to identify the track sections and equipment installed in these track sections. In Figure 5.3, the track layouts are presented by a pair thick lines (both horizontal and vertical), which stands for up line and down line. These lines contain dynamic information to represent the status of the track circuits (with names e.g. LAA, LAB, XH, XK etc. attached adjacently to the track circuits). Red color equivalent to the track circuit is occupied by the train; green color equivalent to the track circuit is set for a route (i.e. ready for a train to proceed); and white color stands for neither the track circuit is occupied nor a route is set. As the length of a track circuit varies, a train

may occupy a number of track circuits. To identify the position of a train, the track circuit(s) occupied status needs to associate a Train Run Number (TRN); for example, in Figure 5.3, "m193" and "L216" are TRN. When the train proceeds from one location to another, information will be dynamically updated and shown on the display, track circuit(s) status will be changed from occupied to clear (i.e. no train on it), and the associated TRN will be stepped to the next position.

Figure 5-3: TCS HCI display showing the real time signaling and train information



5.2.4 Integrated Control and Communications System

The third domain specific system within the mass-transit railway system that needs to be involved in the operation of the tunnel train-fire scenario is the Integrated Control and Communications System (ICCS). As the name

of this domain specific system implies, ICCS provides the control room operators an integrated control system, which covers the control and monitoring of electrical and mechanical (E&M) plant equipment (such as ventilation equipment, air-conditioning equipment, station lighting etc.) and power supply equipment for the railway operations. Also it integrates a number of communication systems, such as direct-line telephone systems, passenger information system etc. The main purpose is to provide an integrated control and communication facilities such that operators can utilize various functions from a single domain specific system.

One of the functions provided by ICCS is the control and monitoring of TVS equipment for the tunnels of LMC Spur Line. As described in *Section 5.2.2 - TVS Emergency Modes* above, the control and monitoring of TVS emergency modes are implemented as a function of ICCS; it is therefore required to provide TVS HCI for the operators to activate / stop any emergency mode if there is a tunnel train-fire incident happened. Figure 5-4, Figure 5-5 and Figure 5-6 are initially designed displays of ICCS TVS HCI that show the emergency modes for the up tunnel, and the tunnel schematic layouts for two ventilation buildings.

In Figure 5-4 the emergency modes are listed (F1 to F6) with associated mode names as static information, and mode state (on / off) and on time (represents the duration of how long this mode is activated) as real-time dynamic information. To activate or stop a particular emergency mode, the operator needs to click the respective mode state field of the emergency mode, it then pop-up a control menu for the operator to select the control on / control off. In general, this operation is an explicit interaction required by the operator to perform.

Figure 5-4: ICCS TVS HCI display showing a list of emergency modes for up tunnel

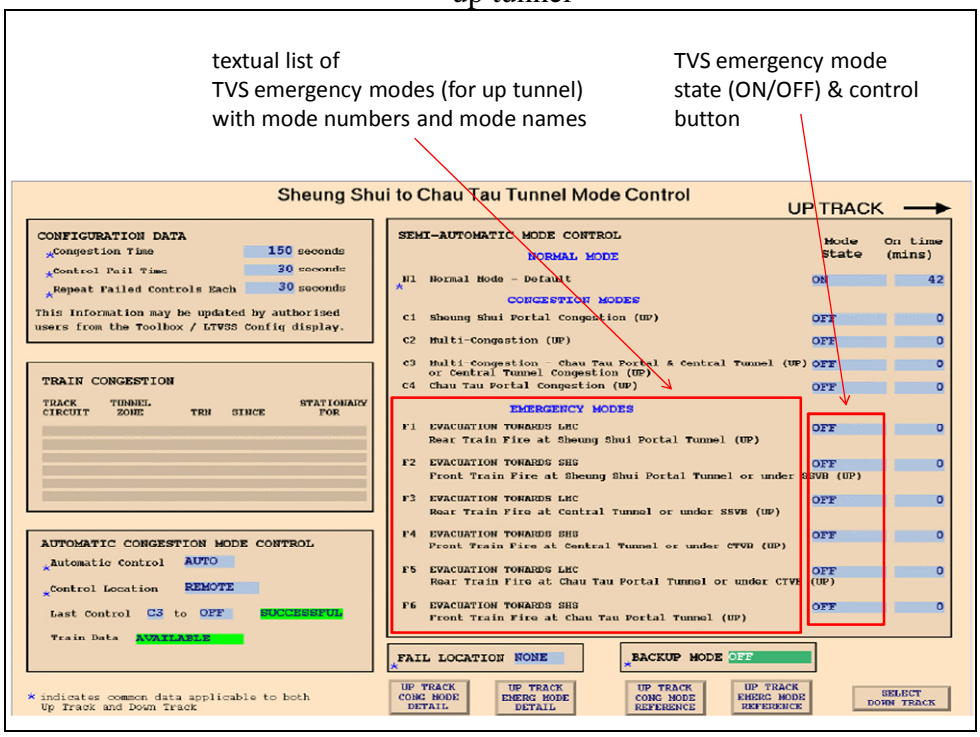


Figure 5-5: ICCS TVS HCI display showing the real time status of TVS equipment in SSVB

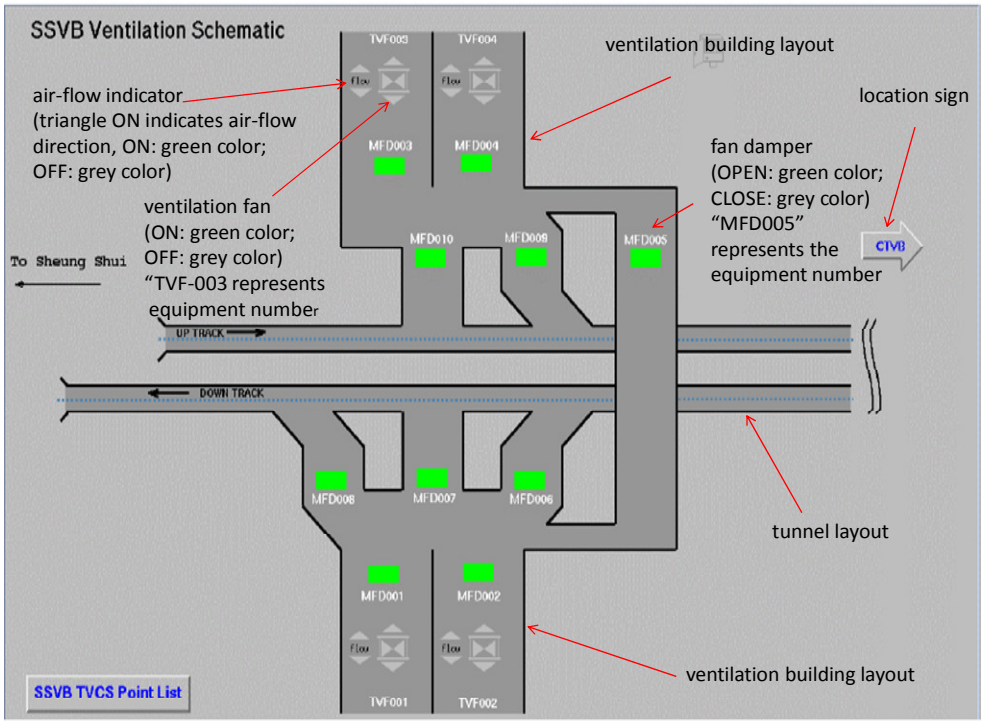
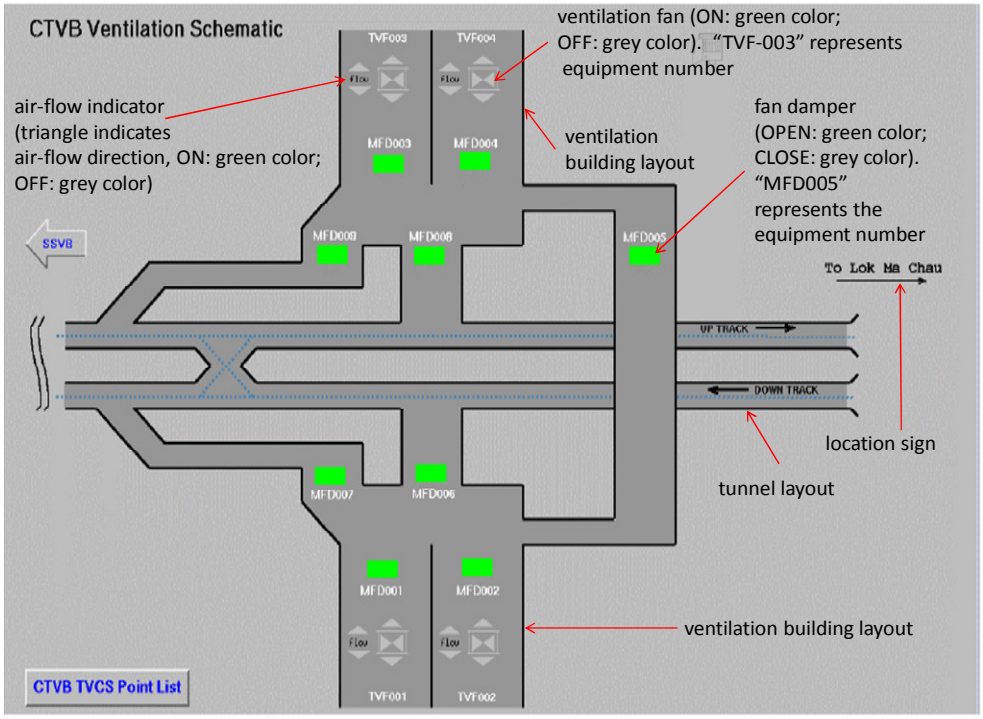


Figure 5-6: ICCS TVS HCI display showing the real time status of TVS equipment in CTVB



5.2.5 HCI Design Issues of Heterogeneous Domain Specific Systems

From the description of above sections, we clarify that a train-fire scenario needs to involve three domain specific systems to determine the situation and subsequent interactions of selecting which TVS emergency mode should be activated. This is a complex process that operators are required to execute carefully all four key elements: cooperation, collaboration, communication, and coordination in the operations of the heterogeneous safety-critical CST system as described in *Chapter 3 – Operational Perspective of Heterogeneous Safety-critical CST Systems*. Within the train-fire incident handling process, the operators in the control room are required to go through all interaction issues that we have reviewed and discussed in *Chapter 2 – Background and Related Work*. The model human

processor of the cognitive psychological framework provides the foundational theory to explain the operators' behavior of interpreting the symbolically code information, together with semiotic of different domain specific systems, to understand the situation; however this needs to be consistent with the operators' mental models, which depends on the situation awareness of the system environment. Furthermore the situation awareness relies on the heterogeneous HCI as the inputs for the operators to have perception of elements in current situation, comprehension of current situation and projection of future status. This is a series of processes that call for a complete understanding of operators' behavior and performance; and ultimately the design of the heterogeneous HCI plays a vital role for the success of such processes.

However, as we have pointed out in *Chapter 1, Section 1.2 – Issues of HCI of Heterogeneous Safety-critical Systems*, domain specific systems have their own functionality and their unique approach to HCI design; this makes the achievement of system operability for a heterogeneous safety-critical CST system a great challenge. From the above sections in explaining the design concept of tunnel ventilation, various HCI design from three different domain specific systems have been shown to illustrate the overall design concept of handling the tunnel train-fire scenario. In practice, each TVS zone is associated with a number of specific emergency modes, (see Table 5-1 for example). Each tunnel train-fire scenario is defined with attributes of specific TVS zone(s) occupied by the incident train and passenger evacuation direction. The physical lengths of the TVS zones can vary so an incident train (of fixed length) may occupy up to three TVS zones. There are a total of 13 emergency modes, which cover 36 tunnel train-fire scenarios (18 for the Up Line and 18 for the Down Line).

During a fire-drill exercise in the trial run operations of the LMC Spur Line, a hazard was raised when there were repetitive operator errors in the

identification of a correct train-fire scenario and the selection of a corresponding emergency mode during an emulated train-fire incident. As discussed in the above sections, the HCI design of respective domain specific systems generally followed their own design guideline and standards, but without a methodology of unifying the heterogeneity to achieve both safety and usability from the system operability perspective. Although each domain specific system satisfied its own design requirements individually, they failed to consider the impact of heterogeneity on system operability, and therefore could not comply with the overall safety and usability requirements. The operational hazard of failure to identify the correct train-fire scenario could impose serious consequence to passenger evacuation; it is because smoke extraction direction could be wrongly activated to run in the same direction of passenger evacuation, which means that passengers could not be able to receive fresh air supplied to the tunnel. This situation was un-acceptable to statutory authorities, therefore new design and evaluation methodologies must be developed to address this complex issue.

5.3 Application of the Usability Evaluation Approach

To resolve the problem as identified above in *Section 5.2.5 - HCI Design Issues of Heterogeneous Domain Specific Systems*, UEA was applied to test the tunnel train-fire scenario and aimed to propose design suggestion to resolve the safety and usability problem. As described in *Chapter 4 – Methodology for Developing the Usability Evaluation Approach*, UEA consists of a Unified HCI Requirements Analysis Framework (UHRAF) and a Safety and Usability Model (SUM). UHRAF is used to analyze the operational scenario and identify the interaction requirements; and SUM is aimed for evaluating the safety and usability of the heterogeneous HCI.

Three processes are required for UEA, Operational Scenario Creation process, Interaction Modeling process, and Safety & Usability Assessment process. This section provides in details how the processes were executed to test the tunnel train-fire incident scenario and the resultant information obtained after the processes were completed.

5.3.1 Operational Scenario Creation Process

The first process of UHRAF is the Operational Scenario Creation, which consists of three tasks: Problem Scenario, Scenario Identification & Scenario Description. The Problem Scenario task was executed to create a Problem Scenario corresponding to the development of a specific operational goal in a heterogeneous safety-critical CST system. It should be noticed that the Problem Scenario does not prescribe any domain specific systems, and therefore it is not intended to identify what functionality of each individual domain specific system must possess. Problem Scenario is viewed from the operational perspective and is aimed to provide a high-level requirement of how the system should behave as a whole. Table 5-3 shows the analysis techniques that were used for these tasks.

Table 5-3: Summary information of the Operational Scenario Creation process

Process: Operational Scenario Creation		
Task	**Main purpose**	**Analysis techniques used**
Task_1_1: Problem Scenario	Create a Problem Scenario	Review of statutory documents, operating agreement with authority etc.; Review of standard operating procedures (SOP).
Task_1_2: Scenario Identification	Identify the Network of Scenarios	Review of standard operating procedures; Review of guidelines; Peer-group discussion with operator representatives and safety experts;

Process: Operational Scenario Creation		
Task	**Main purpose**	**Analysis techniques used**
		Event-tree analysis.
Task_1_3: Scenario Description	Provide detailed information of each scenario within the Network of Scenarios	Review of standard operating procedures; Review of rules and guidelines; Interview with operators; Protocol analysis.

(1) Problem Scenario

The first task (Problem Scenario) corresponded to the development of a specific operational goal in the CST system for the LMC Spur Line. In this case, the operational goal was to manage the incident during tunnel train-fire incident. Therefore, the Problem Scenario of handling tunnel train-fire incident was created. It should be noted that in general it is relatively straightforward to identify a Problem Scenario if standard operating procedures (SOP) are in place. It would be more difficult to create if no well-established SOP is available.

(2) Scenario Identification

The second task (Scenario Identification) was to identify and form a Network of Scenarios, and to provide highlight of each low-level scenario, for the Problem Scenario: handling of tunnel train-fire incident. Figure 5-7 shows the Network of Scenarios that was formed after the task was completed, with individual low-level scenarios identified. The following highlights each low-level scenario:

- Identification of fire condition

  This scenario is to describe how a fire condition is identified, for example, fire alarm of the train is activated, passenger reports that a fire has happened, etc.

- Confirmation of fire condition

  This scenario is to describe the need to confirm the fire alarm whether it is a true alarm or a false alarm, either by verbal confirmation between passengers and train driver, or monitoring of closed circuit television (CCTV) inside the train compartment.

- Selection of evacuation direction

  This scenario is to describe the decision that needs to be taken to determine which evacuation direction for the passengers to follow. The decision made will depend on the fire location with respect to the train, the train position (e.g. close to the tunnel exit, etc.) and other situational conditions that may have impact to evacuation direction.

- Selection of TVS emergency mode

  This scenario is to describe the selection of TVS emergency mode, which is designed for the selected evacuation direction and the position of the incident train.

- Validation of selected TVS emergency mode

  This scenario is to validate the selection of TVS emergency mode, which is an outcome of the previous scenario.

- Execution of selected TVS emergency mode

  This scenario is to describe the actual control and activation of the selected TVS emergency mode.

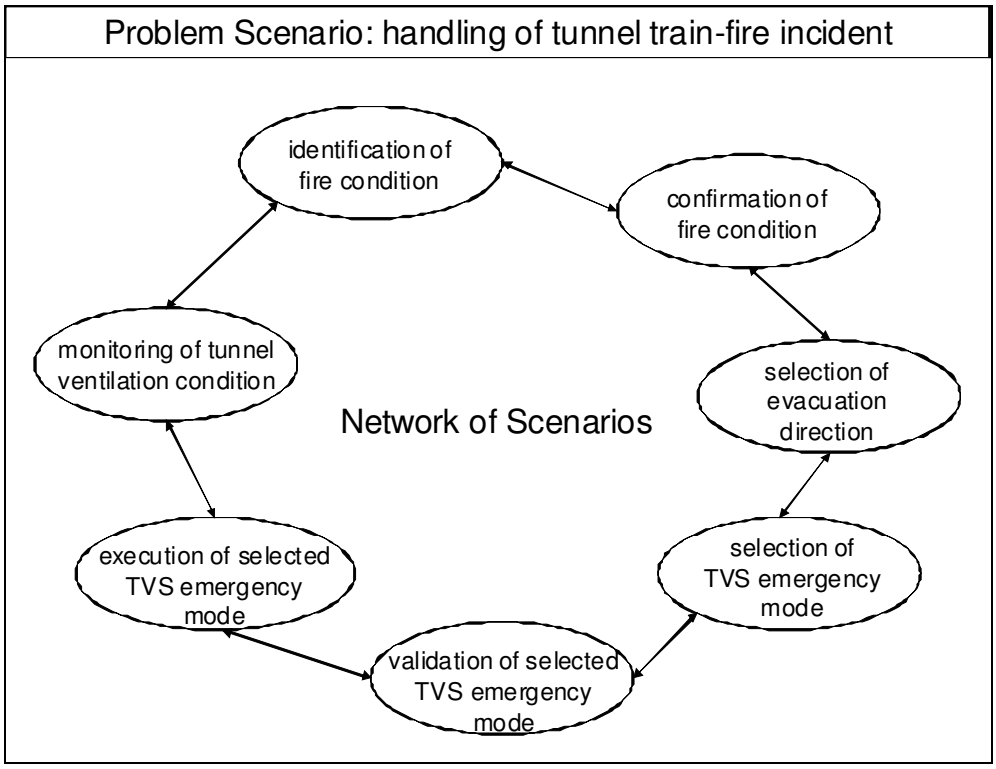
- Monitoring of tunnel ventilation condition

  This scenario is to monitor the effectiveness of the TVS emergency mode after being executed, for example, whether smoke-free path is

established for passenger evacuation; and to monitor the evacuation condition, such as whether the passengers orderly follow the evacuation path.

In this Problem Scenario, the Network of Scenarios was a ring-type network. However, there is no rule that prohibits the Network of Scenarios could be in other topological form.

Figure 5-7: Network of Scenarios for the Problem Scenario: handling of tunnel train-fire incident



(3) Scenario Description

The third task (Scenario Description) was conducted to provide detailed information of each scenario identified in the Network of Scenarios. Table 5-4 provides the details of the Scenario Description for the scenario: selection of TVS emergency mode, as an example.

After the details of each Scenario Element were identified, the Operational Scenario Creation process was completed. This will provide sufficient details to model the interaction requirements between each scenario in the Network of Scenarios, therefore the second process of UHRAF, interaction modeling, commenced.

Table 5-4: Scenario Description for the scenario: selection of TVS emergency mode

Scenario Description	**Scenario: Selection of TVS Emergency Mode**	
Scenario Element	**Definition**	
Setting	A tunnel train-fire incident is confirmed.	
Actors	ECO in control room.	STC in control room.
Task Goals	Decide the correct TVS emergency mode for the particular tunnel train-fire incident.	
Plans	ECO plans to operate the ICCS workstation to bring up the TVS emergency mode display.	STC plans to operate the TCS workstation to bring up the signaling and train information display.
Artifacts	ICCS and TVS.	TCS.
Actions	ECO operates the ICCS workstation to bring up the TVS emergency mode display. ECO receives information from STC the incident train position and evacuation direction. ECO receives instruction from STC to command the activation of selected TVS emergency mode.	STC operates the TCS workstation to bring up the signaling and train information display. STC informs ECO the incident train position and evacuation direction. STC decides the TVS emergency mode designed for this particular incident from the information presented in the display of ICCS workstation. STC gives instruction to ECO to command the activation of

Scenario Description	Scenario: Selection of TVS Emergency Mode	
Scenario Element	**Definition**	
		selected TVS emergency mode.
Events	The ICCS workstation responds to ECO's command with a correct display for the TVS emergency mode operation.	The TCS workstation responds to STC's command with a correct display for the signaling and train information.
Assessment	ECO assesses the correct display for the TVS emergency mode operation.	STC assesses the correct display for signaling and train information.

(Note: STC = Senior Train Controller; ECO = Electrical Control Officer; ICCS = Integrated Control & Communications System; TCS = Train Control System; TVS = Tunnel Ventilation System)

5.3.2 Interaction Modeling Process

The second process of UHRAF is the Interaction Modeling process. This process makes use of the information collected from the Scenario Description and further analyzes the interaction requirements for the scenario. It consists of three tasks: (1) Classification of Social Distribution; (2) Classification of Technological Distribution; and (3) Development of Interaction Model. Table 5-5 shows the tasks, main purpose and analysis techniques that were used for these tasks.

Based on the result obtained from the Operational Scenario Creation process, the Network of Scenarios and details of each scenario were available for further analysis and development of the Interaction Models. According to the Interaction Modeling process, each scenario would need to have the Interaction Modeling with its adjacent scenarios, therefore the following scenario pairs were required to go through the Interaction Modeling process.

- <identification of fire condition> : <confirmation of fire condition>
- <confirmation of fire condition> : <selection of evacuation direction>
- <selection of evacuation direction> : <selection of TVS emergency mode>
- <selection of TVS emergency mode> : <validation of selected TVS emergency mode>
- <validation of selected TVS emergency mode> : <execution of selected TVS emergency mode>
- <execution of selected TVS emergency mode> : <monitoring of tunnel ventilation condition>
- <monitoring of tunnel ventilation condition> : <identification of fire condition>

Table 5-5: Summary information of the Interaction Modeling process

Process: Interaction Modeling		
Task	**Main purpose**	**Analysis techniques used**
Task_2_1: Classification of Social Distribution	Identify operators, distributed knowledge, and shared knowledge	Review of standard operating procedures (SOP); Review of guidelines; Peer-group discussion with operator representatives; Interview with operators.
Task_2_2: Classification of Technological Distribution	Identify interaction between operators and artifacts	Review of standard operating procedures (SOP); Review of guidelines; Peer-group discussion with operator representatives; Interview with operators.
Task_2_3: Development of Interaction Model	Communication and information required to be exchanged between scenarios	Event-tree analysis; Protocol analysis.

The task: Classification of Social Distribution is to collect and classify information of interaction between operators, shared knowledge and communication dialogue and protocol between them. The task: Classification of Technological Distribution is mainly focused on the interaction between operators and artifacts, which includes the types of heterogeneous domain specific systems to be involved in the interaction, the operating procedures of these systems and how to interact with these systems. The information collected by these two tasks is then fed to the next task: Development of Interaction Model. Table 5-6 and Table 5-7 list the result generated by the task: Development of Interaction Model for Level-1 Interaction and Level-2 Interaction respectively for the scenario: selection of TVS emergency mode.

Table 5-6: Result generated from Level-1 Interaction Model

Scenario Description: Selection of TVS emergency mode	
Level-1 Interaction Element	**Definition**
Events	Train-fire alarm, fire location with respect to the train, train position, evacuation direction.
Artifacts	ICCS, TCS, TVS.
Actors	STC, ECO.
Shared operator knowledge	Communication dialogue and protocol; Train information (train position and train run number (TRN)); Operating procedure for fire incident; ICCS operations.
Distributed operator knowledge	STC – TCS operations; operating procedure for communicating with ECO. ECO – TVS operations; operating procedure for communicating with STC.

Table 5-7: Result generated from Level-2 Interaction Model

Scenario Description: Selection of TVS emergency mode		
Level-2 Interaction Element	**Definition**	
Scenario	Scenario Description: Selection of evacuation direction	Scenario Description: Validation of selected TVS emergency mode
Communications	The information of the incident train location is communicated through the TCS HCI display format, i.e. the occupancy of relevant track circuit(s) and the train's TRN.	The information of the incident train location is communicated through the TCS HCI display format, i.e. the occupancy of relevant track circuit(s) and the train's TRN.
Information	• Position of the incident train. • TRN. • Fire condition. • Relative location of fire with respect to the train compartment. • Evacuation direction. • Tunnel ventilation zone(s).	• Position of the incident train. • TRN. • Fire condition. • Relative location of fire with respect to the train compartment. • Evacuation direction. • Selected TVS emergency mode.

As we have described in the previous sections that the Operational Scenario Creation process does not require the identification of domain specific systems to be participated in the Network of Scenarios. In the Interaction Modeling process, however, all artifacts that will interact with the operators need to be discovered and we need to understand the basic functionality of the domain specific systems (artifact providers) so that we can identify the knowledge (both shared and distributed) that the operators should acquire. In the scenario: selection of TVS emergency mode, Table 5-6 and Table 5-7 identify the interaction details within the scenario itself and with it adjacent

scenarios respectively. In addition, detailed requirements of actors, artifacts and knowledge also need to be identified.

After all scenarios in the Network of Scenarios have gone through the Interaction Modeling process, all essential knowledge of the HCI requirements for the Problem Scenario was discovered. This formed the basis for the assessment to be conducted by SUM in order to assess whether safety and usability issues were complied with the criteria defined SUM.

5.3.3 Safety and Usability Assessment Process

This section describes how we used SUM to test the safety and usability of HCI designed by individual domain specific systems for the tunnel train-fire scenario. In this usability test we assessed all scenarios within the Network of Scenarios. For illustration purpose, we report in this thesis the assessment with respect to the Scenario_Description: selection of TVS emergency mode, created in the previous processes of UHRAF. As discussed in *Chapter 4, Section 4.3.4 – Safety and Usability Assessment Process*, assessment was carried out by operator representatives, safety experts, HCI designers of domain specific systems, and system integrator, and in accordance to the three different Building Blocks and associated eight aspects in SUM. A set of HCI artifacts, which were designed for the handling of tunnel train-fire incident was collected for assessment. Figure 5-3 to figure 5-6 in *Section 5.2 Heterogeneous HCI Design Problem* were used to illustrate the HCI displays provided by TCS and ICCS for the assessment.

Figure 5-3 shows the train and track related information, such as train position and associated Train Run Numbers (TRN), signaling status, direction of travel and track circuit occupancy, i.e. whether a track circuit is occupied by a train (red for occupied, green for unoccupied with route

setting, and white for unoccupied without route setting) in the tunnel section. The design of this HCI display conforms to standard TCS display design practices, which governs the semiotic within the domain of TCS. Figure 5-4, Figure 5-5 and Figure 5-6 show the list of available emergency modes for the up tunnel section in a tabular format, together with other control and monitoring functions. Similarly these HCI displays also conform to standard ICCS HCI design guideline. The following sections describe the assessment outcome.

(1) Assessment of Heterogeneous HCI

The first task of the Safety and Usability Assessment process is the Assessment of Heterogeneous HCI. This task is aimed to assess the HCI design in accordance to the Safety and Usability Matrix, as highlighted in *Chapter 4, Section 4.3.4 – Safety and Usability Assessment Process*. Details of the assessment are provided in the sections below.

(A) Assessment on Characteristics of Work Environment

As identified in the Interaction Modeling process (refer to Table 5-6 and Table 5-7), the Problem Scenario: handling the tunnel train-fire incident requires cooperation, collaboration, communication and coordination between operators in the control room. Specifically, STC was required to communicate with TC for the confirmation of train-fire incident. He/she was also required to make decision on the evacuation strategy, such as passenger evacuation direction according to the situational conditions, and then instructed ECO to perform emergency mode control function. In this Problem Scenario, the Collaboration was implemented through verbal face-to-face communication between operators within the control room, and radio communication between TC and the train driver of the incident train. In general the heterogeneous HCI design under assessment had no adverse

impact to the collaboration between operators responsible for handling the tunnel train-fire incident.

The Dynamic Multi-workplace Context was fully reflected in the Problem Scenario. It involved a number of workplaces, for example between the control room and the incident train, the control room and external parties such as Fire Services authority and other transportation authorities. It was a dynamic environment as the fire incident condition might change from time to time; but the heterogeneous HCI design did not impose any constraint on this situation.

However, in the assessment of Heterogeneous Information we identified repetitive operator errors in selecting correct TVS emergency modes for given scenarios. A deficiency of information presentation in the heterogeneous HCI design was logged. After further analysis on the operator errors, we discovered that the root cause was attributable to the HCI design of respective domain specific systems that needed to be involved in the handling of the train-fire incident, namely, TVS, TCS and ICCS. The analysis showed that the deficiency was caused by the difference between the design concepts of TVS and TCS. TVS is a zone-based design, for which a zone is represented by a tunnel section with geographical meaning, such as the tunnel section underneath the ventilation building. On the other hand, TCS is train position-based design with the train position represented by the track circuit occupancy and a unique train run number (TRN). Track circuits do not carry geographical information with them and they merely depend on the signaling system design. Consequently, these two domain specific systems created an incoherent information presentation on their respective HCI display design. This deficiency had knock-on effect on other safety and usability criteria, as discussed in the following sections.

(B) Assessment on Human Performance and Hazard

The assessment on Human Performance and Operational Hazard addressed operator errors due to unfamiliar software behavior, information retrieval, focusing problem and mode confusion. We had identified that operators were familiar with individual domain specific applications and software behavior, thus the possibility of wrong predictions causing error was minimal. The time required for data retrieval of the Problem Scenario of handling the tunnel train-fire incident was similar to the rest of other operational scenarios and system functions; therefore the issue of additional cognitive loading due to increasing availability of data was unlikely to happen in this Problem Scenario. Since there were frequent communication between operators within the control room, and between the control room operators and train drivers, decrease in attention/focus to the system status and important events was unlikely in this scenario because communication between operators required refresh of system status.

Mode confusion was identified as a deficiency in the heterogeneous HCI design for the Problem Scenario in this usability test. The main cause was due to a number of mode indications spread over multiple HCI displays and each HCI display containing just a portion of the potential mode status data but not the overall system. In this usability test, TCS HCI display only showed the incident train position; on the other hand, ICCS HCI display only showed a table of possible TVS emergency modes. It relied on operators to bridge the information gap between the two domain specific systems, and that required extra cognitive loading, which was likely to cause hazard on selecting the wrong emergency mode for the incident.

(C) Assessment on Cognitive Characteristics of Human Operators

The problem on Heterogeneous Information had raised specific impact to the Cognitive Characteristics of Human Operators, as identified below.

Since the correlation of train position and the corresponding TVS zone was not a trivial exercise, it required extra cognitive loading to interpret the track circuit occupancy data and train run number (i.e. position of train) with the appropriate TVS emergency mode. The extra cognitive loading was consumed by frequent navigation of multiple displays for unifying information from different sources, which consequently required switching of operators' mental models. The handling of tunnel train-fire incident also required a new mental model and there were cognitive constraints on forming a new mental model, such as past experience and limitation of short-term memory. The mapping between the train position in association with the corresponding TVS zone was a critical operator's decision for the selection of the correct emergency mode under a given tunnel train-fire scenario. From the perspective of HCI, this incoherent information of "position" imposed a major gap between the operator's goal and the system's state, i.e. mode confusion. Although the perception of triggering event (i.e. occurrence of train-fire) was convinced to be effective, the comprehension of current situation was impacted by the exhaustive cognitive loading and mode confusion. The operator would find it difficult to establish the goal. The subsequent tasks of forming plan and specifying action sequence could not be accomplished in a timely manner. In addition, there might well be interaction mistakes such as being unable to formulate the right goal. Without a right goal the operators would fail to translate the goal into a plan of performing appropriate actions, or an action sequence which, when performed, would lead to the achievement of the goal; as a result situation awareness would be degraded because of the failure to project the future status. Table 5-8 summarizes the assessment result for the scenario: selection of TVS emergency mode.

Table 5-8: Summary of assessment (***Italic Bold*** represents deficiency conditions)

SUMMARY OF ASSESSMENT			
Scenario: Selection of TVS Emergency Mode			
Characteristics of Work Environment	**Collaboration**	**Dynamic Multi-workplace Context**	**Heterogeneous Information**
	Addressed in the Interaction Modeling.	Addressed in the Interaction Modeling.	***Incoherent interpretation of heterogeneous information.***
Human Performance and Hazard	**Human Performance**	**Operational Hazard**	
	Extra cognition loading required due to interpretation of heterogeneous information.	***Potential operator error in selecting the TVS emergency mode for tunnel train-fire incident.***	
Cognitive Characteristics of Human Operators	**Human Cognition**	**Mental Model**	**Situation Awareness**
	Extra cognition loading required due to interpretation of heterogeneous information.	***Frequent switching of mental models triggered by heterogeneous information.***	***Degraded projection of future status caused by the difficulty of mode confusion and goal formation.***

(2) Review of Assessment Result

Each of the scenarios within the Network of Scenarios was assessed, with result filled-in to the Safety and Usability Matrix. After the Network of Scenarios was assessed, the assessment for a Problem Scenario was then completed. A set of Safety and Usability Matrices was generated for review, for example, Table 5-8 for the scenario: selection of TVS emergency mode. Review sessions were organized for assessors to go through all outcomes for

validity, correctness, ambiguity and omissions. If abnormality of result was raised, consultation for re-assessment would be required, if necessary.

(3) Design Recommendation

This section describes the design recommendation to the heterogeneous HCI design for the Problem Scenario: handling of tunnel train-fire incident. The design recommendation was based on the assessment result generated from the previous tasks. It provided remedial measures to remove or mitigate the impact caused by the adverse conditions identified in the Safety and Usability Assessment process. However, it did not prescribe the exact design details to solve the problem and it was up to the respective domain specific systems' HCI designers to propose design solution.

To address the deficient conditions identified in the evaluation, the root cause of incoherent heterogeneous information must be reconciled. In this usability test, TCS HCI display, as shown in Figure 5-3, focused on train position represented by track circuit occupancy and TRN. There was no representational concept of TVS zoning in its HCI displays. On the other hand, ICCS HCI display focused on TVS emergency mode status, and TVS equipment monitoring and control functions, as shown in Figure 5-4, Figure 5-5 and Figure 5-6; therefore no train position concept was provided. A simple tabular representation that listed the TVS emergency modes did not satisfy the criteria defined by the three Building Blocks of UEA. Therefore a special method needed to be designed to bridge the gap created by the heterogeneous information of domain specific systems.

The design recommendation to rectify the problem was suggested as: the primary requirement of the heterogeneous HCI identified in the usability test was to link together information from heterogeneous domain specific systems so that it could do the following:

- Bridge heterogeneous information gap to enable the coherence of information from multiple sources;
- Avoid information overloading by presenting information from the context of operational needs;
- Minimize navigation requirement to reduce operators' cognitive loading and eliminate mode confusion;
- Avoid frequent switching of operators' mental models; and
- Facilitate operators' goal formation to exercise operational procedures.

Design recommendation was given to respective domain specific systems' HCI designers after the usability test was completed. A series of design workshop were conducted to identify solution. Eventually, to implement the recommendation highlighted above, a Tunnel Ventilation Overview display was created in ICCS to provide a summary of TVS information (such as TVS fan and damper status, air flow directions etc.), and track circuit and TRN information, as shown in Figure 5-8. In addition, a TVS Emergency Mode Reference Overview display was also created in ICCS to facilitate the operators in the control room to handle the tunnel train-fire incident, as shown in Figure 5-9.

Figure 5-8: TVS overview display

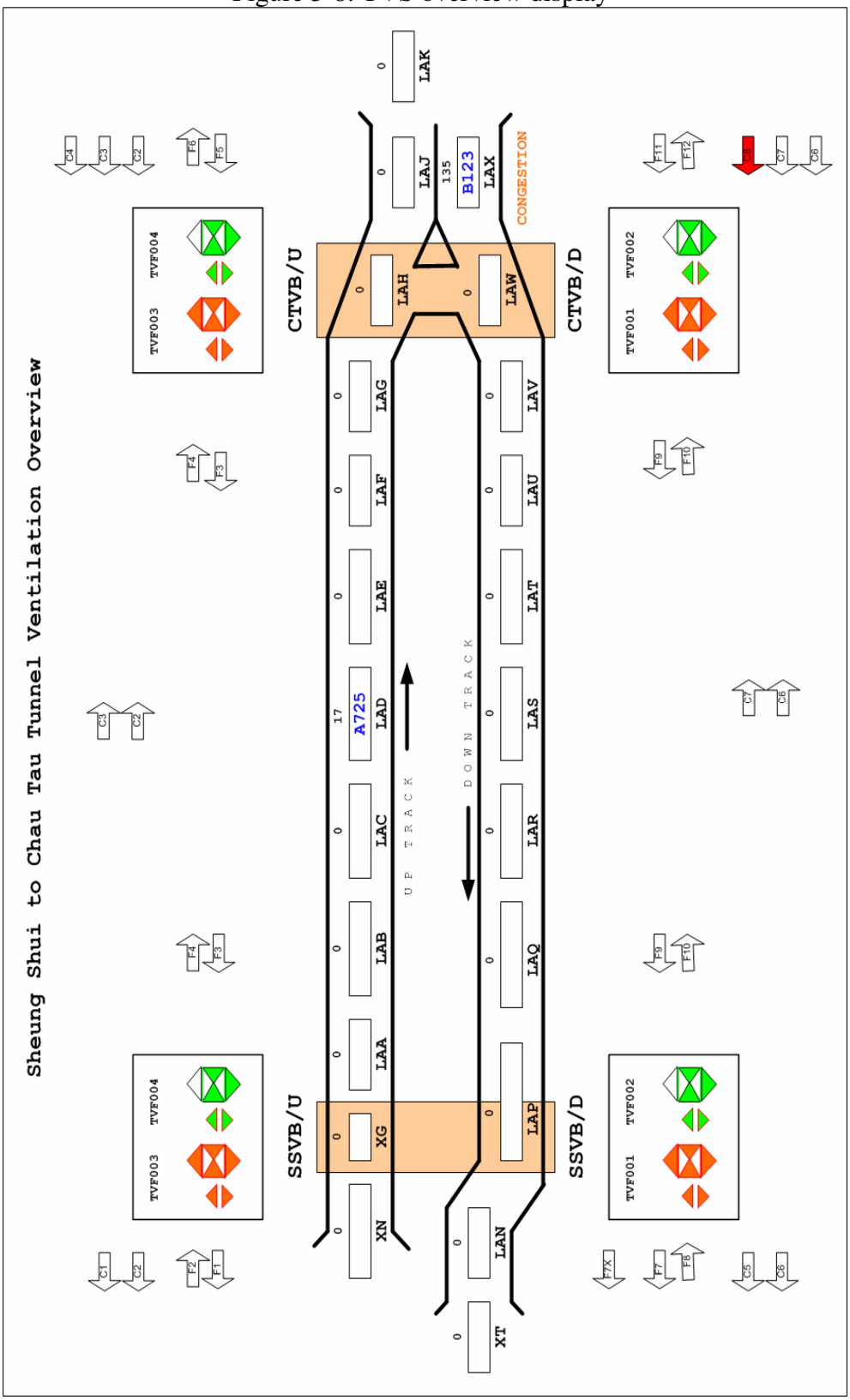
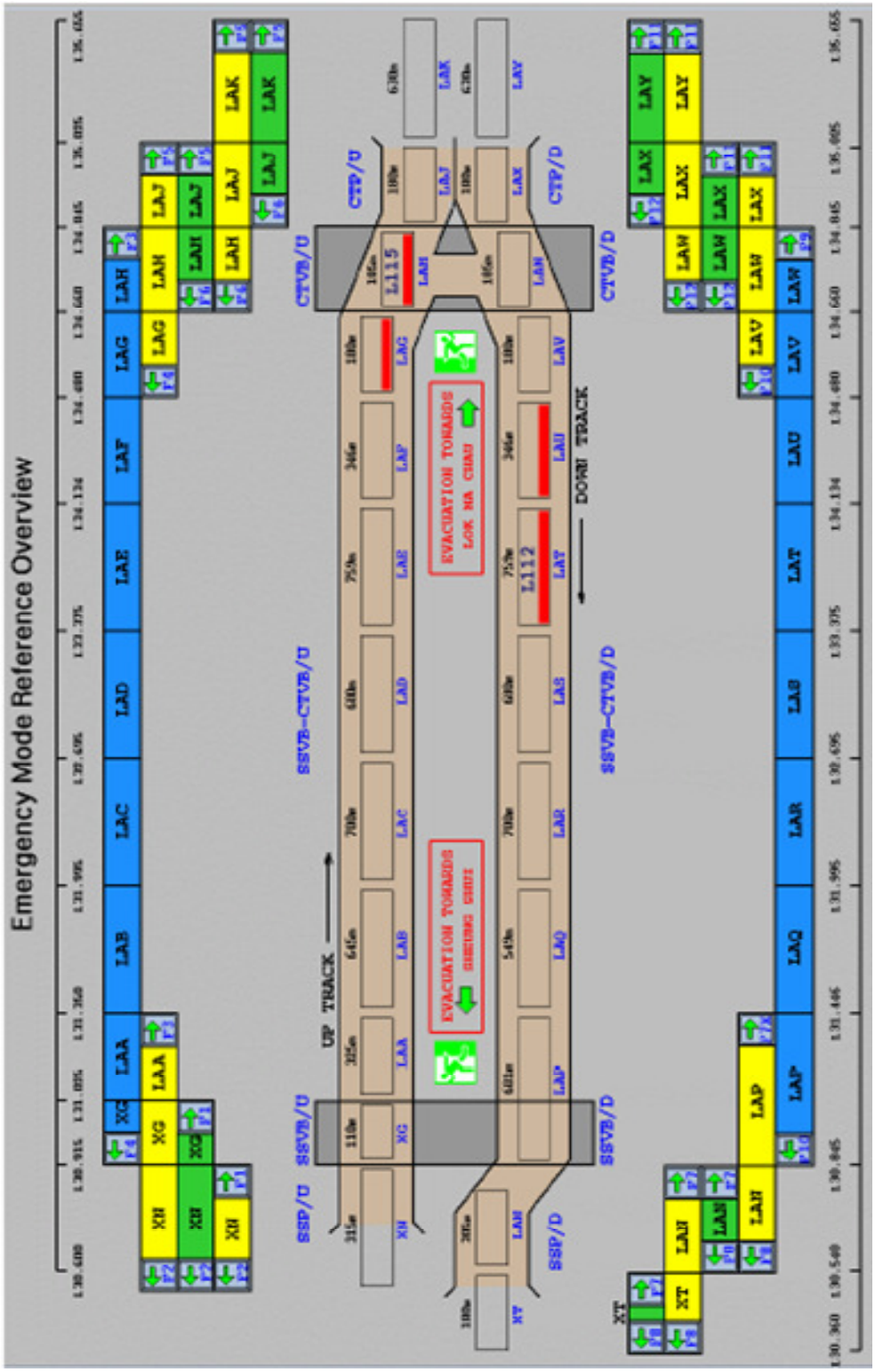
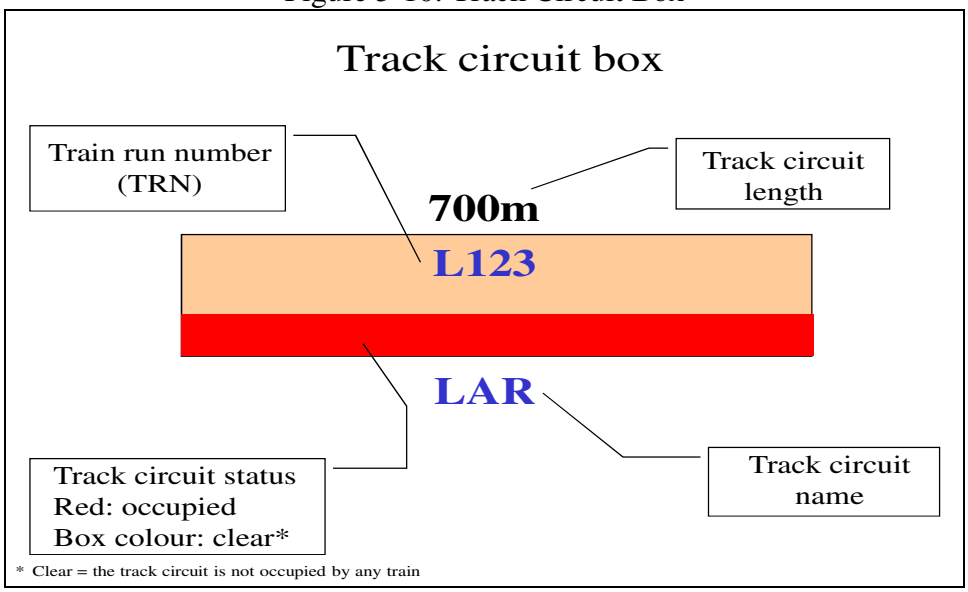


Figure 5-9: TVS emergency mode reference overview display



The Emergency Mode Reference Overview display addressed the heterogeneous information gap by presenting both the train information and the TVS zoning concept into a unified display. The train position was represented by TRN stepping in the rectangular track circuit boxes, while track circuit occupancy was represented by a red line inside the track circuit boxes, as illustrated in Figure 5-10.

Figure 5-10: Track Circuit Box



TVS zones were shown by the color bars above and below the tunnel layout; and the TVS zone bars were layered and colored to distinguish them from each other to identify the coverage of respective TVS zones with associated track circuits. This could reduce the operators' cognitive loading when mapping the train position and TVS zone coverage. As an example, Figure 5-11 shows an incident train (TRN = L123) stalled in the position that occupied 3 consecutive track circuits LAG, LAH & LAJ. In this scenario, the TVS zone bar (yellow color) will correspond to either TVS Emergency Mode F4 (evacuate toward SHS direction), or TVS Emergency Mode F5 (evacuate toward LMC). Once the operator (STC) confirmed the passenger evacuation direction, the operator's (ECO) goal formation of selecting the corresponding TVS emergency mode could be easily established. The TVS

emergency modes were also designed as a "button" so that when the operators click these buttons, the corresponding details of this TVS emergency mode were displayed; this gave sufficient information regarding the concerned TVS emergency mode and therefore switching of operators' mental models could be avoided. Figure 5-12 illustrates, as an example, the details of TVS emergency mode F3 is pop-up when the button "F3" is pressed.

The unified Emergency Mode Reference Overview Display integrated heterogeneous information so that the chance of mode confusion could be reduced, which implied the projection of future status would be more accurate.

Figure 5-11: Example showing an incident train stalled in the tunnel

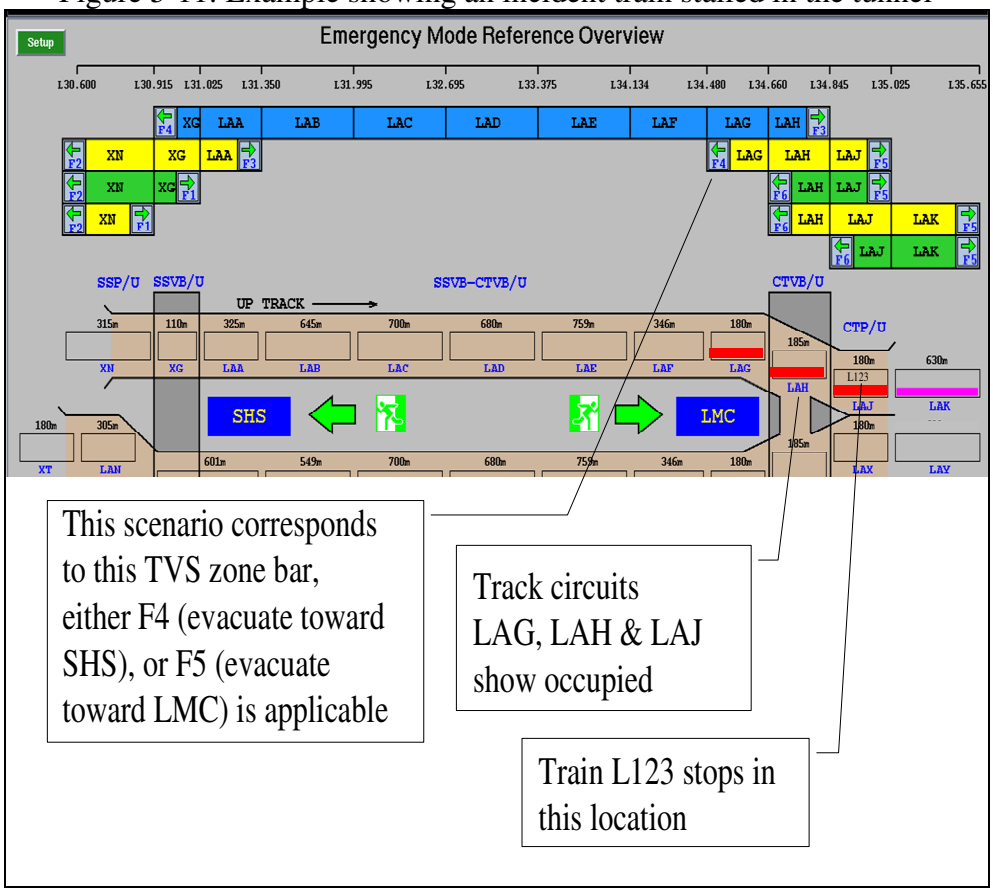
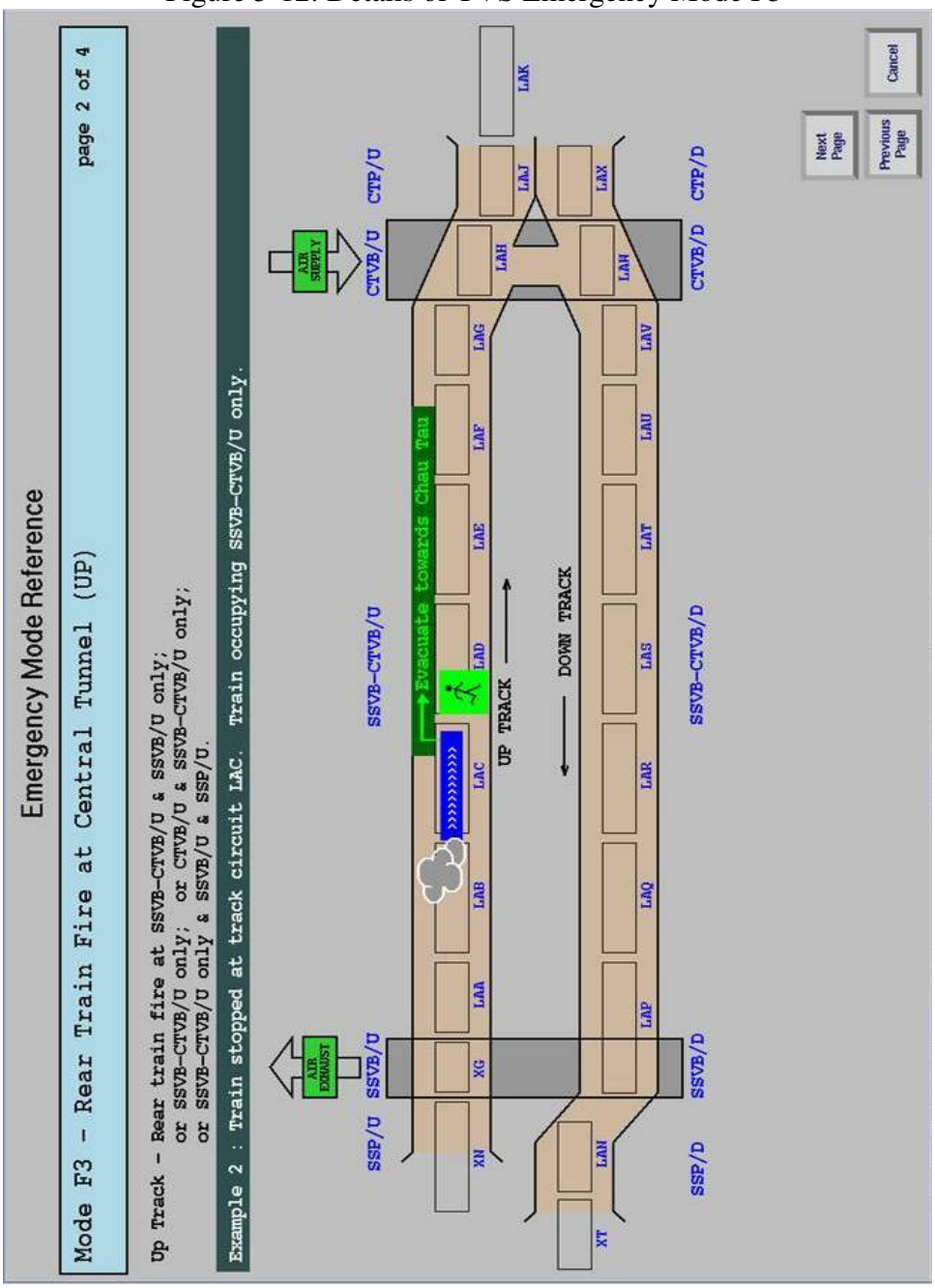


Figure 5-12: Details of TVS Emergency Mode F3



5.4 Summary Remark

This chapter has presented the application of UEA proposed in this thesis to test a scenario of handling the tunnel train-fire in a mass-transit railway

system. The aim of UEA is to make the large body of HCI and usability research reviewed in *Chapter 2 – Background and Related Work* available to specialists for dealing with HCI development of heterogeneous safety-critical CST systems. The scenario of tunnel train-fire has perfectly demonstrated the heterogeneity of the mass-transit railway system as a typical heterogeneous safety-critical CST system. To make this body of work useful to specialists who are responsible for developing heterogeneous safety-critical CST systems, two main components are developed: the Unified HCI Requirements Analysis Framework (UHRAF) and the Safety and Usability Model (SUM). Each of these two components has specific aims to analyze the heterogeneous HCI requirements and evaluate the outcome to ensure the system operability is achieved.

This chapter has explained the complexity of handling a tunnel train-fire scenario, and has provided the primary design concepts of those domain specific systems that need to be involved, namely, TVS, TCS and ICCS, in order to understand the operational processes of handling a tunnel train-fire incident; in particular those design concepts, which have profound effect on their respective HCI design, for example, the track circuit representation in TCS, and the TVS zone representation in ICCS. Although in the scenario under test, we mostly dealt with HCI artifacts for displays and without other HCI objects and devices for interaction and manipulation, they are the primary means for the operators to interact with the system, and therefore the HCI issues that we have reviewed in *Chapter 2 – Background and Related Work* continue to apply. More importantly, UEA focuses on requirements analysis and safety and usability assessment; it can facilitate the design of heterogeneous HCI, which would not be possible if developing individually by respective domain specific systems, as demonstrated in the usability test reported in the chapter. The value of UEA is fully demonstrated through the usability test on the scenario of handling tunnel train-fire incident by identifying the root cause of usability deficiency with

safety impact, which would not be discovered alone by individual domain specific systems.

The contribution of this chapter is the demonstration of UEA for heterogeneous HCI requirements analysis, evaluation and design recommendation to system designers at the early stage of the system development of a heterogeneous safety-critical CST system. UEA is grounded in a broad and varying body of literature from the discipline of HCI and usability. UEA is a lightweight approach that incorporates an appreciation of vulnerabilities to human error, which is not restricted to one particular theoretical standpoint. UEA also considers the efforts contributed by abundant research in requirements analysis, system development, HCI theories and usability testing practices are valuable assets; and this is the main reason UEA opts for a focus on developing new processes, rather than tools. The primary aim of developing UEA is to create a systematic means of applying scenario-based processes, with extended views in safety and usability, to holistically analyze a heterogeneous safety-critical CST system, which is commonly over-looked by domain specific systems' designers. In summary, by applying UEA we can facilitate the system designers and also system operators to appreciate the needs and ways of unifying heterogeneous HCI, and discover any safety and usability issues at the early stage of the system development lifecycle.

UEA was used to resolve a complex operational scenario in a mass-transit railway system – handling of tunnel train-fire scenario. The design recommendation of UEA was implemented in three domain specific systems: TCS, TVS and ICCS, to reconcile the heterogeneous HCI problem exists in these domain specific systems. UEA was considered to be a useful approach with implementable processes for analysts and designers to carry out without major drawbacks, other than extra time and cost incurred in the

implementation, this is further discussed in newly added S*ection 6.5.2 – Time and Cost Requirements of Using UEA*.

Chapter 6

Assessment of the Usability Evaluation Approach

In previous chapters, we have described the development of the Usability Evaluation Approach (UEA), an approach for evaluating the usability of heterogeneous safety-critical complex socio-technical (CST) system, with particular focus on HCI requirements from an overall system operability perspective, instead of individual domain specific systems' HCI design. In *Chapter 5 - Application of the Usability Evaluation Approach*, we have also reported the application of UEA to analyze the requirements and test the usability of the HCI designed for a scenario of handling the tunnel train-fire incident in a mass-transit railway system. In this chapter, we shift the focus from the development and application of UEA to how it is assessed for its own applicability, acceptability and effectiveness. More importantly, we revisit the research statement of problem defined for this thesis, and review the three research questions raised in *Chapter 1, Section 1.4 – Research Statement of Problem*, and see whether these questions have been answered and the research statement of problem has been fully addressed by UEA. Furthermore, we also review the accuracy, constraints and limitation of UEA identified during its implementation on the scenario of handling tunnel train-fire incident.

6.1 Approaches of Assessment

In considering the assessment of UEA, two main approaches have been adopted, each seeking (i) to support the development of UEA; and (ii) to gain understanding from its application to the scenario as reported in *Chapter 5 – Application of the Usability Evaluation Approach*. A formative assessment was initially used as part of the overall development of UEA. This was also supplemented by a more comprehensive summative assessment, which aimed to gain a broader understanding of the applicability, acceptability and effectiveness of UEA when applied in practice. This sought to uncover both how effective the processes are, and how easy the processes are, if used by other HCI specialists and system developers.

Information on the use of UEA plays a major part in its refinement. Basically, the design of UEA is informed by the results of formative evaluation of components of the method as they are being developed. This formative evaluation of UEA is complemented by a much more summative approach to assessment. The summative assessment will also be used to judge qualitatively how well the research questions have been answered and whether the overall research satisfies the research statement of problem. This takes the form of using UEA in the actual application to a scenario in a mass-transit railway system. These two complementary approaches of the assessment structure provide the presentation in the remaining part of this chapter.

6.2 Achievement of the Research Statement of Problem

To assess whether UEA meets its design target, we revisit the research statement of problem stipulated in *Chapter 1, Section 1.4 – Research Statement of Problem*, as follow:

A heterogeneous safety-critical CST system is built by integrating a set of domain specific systems, which are constituted structurally by objects, human operators, artifacts, physical surroundings, data, processes and operating rules and procedures. The heterogeneity of HCI in a heterogeneous safety-critical CST system environment involves a variety of complex human activities with safety contexts. However, the concurrent development of domain specific systems in a heterogeneous safety-critical CST system does not address the coherency and compatibility issues of HCI requirements from a unified operational perspective and it does not describe the overall users' activities and associated system-operator interaction. Consequently the safety and usability of the system will be jeopardized. Therefore new analysis and evaluation approach needs to be explored to address the challenges faced by the development of HCI in such environment.

The key issue of the research statement of problem concerns with the ignorance of HCI coherency and compatibility issues in the heterogeneous safety-critical CST system, despite the fact that HCI guidelines for individual domain specific systems are generally complied. In the application of UEA, we successfully utilized the Unified HCI Requirements Analysis Framework (UHRAF) to analyze a complex scenario of handling the tunnel train-fire incident in a mass-transit railway system. This has

demonstrated that UHRAF does possess the capability to analyze requirements, especially from a number of domain specific systems that needed to be interfaced in order to orchestrate a unified solution for the system operators in the control room of the mass-transit railway system. The notion of "unified solution" is a vital factor to the success of the operations; this has been validated by the Safety and Usability Model (SUM) through the safety and usability assessment. Although UHRAF is inspired by the Usability Engineering (UE) proposed by [Rosson & Carroll, 2002], its ability to analyze and collect important heterogeneous information from interactions between scenarios makes it becomes a more appropriate requirements analysis method compared with UE, for which claim analysis is its strongest feature for usability reasoning.

Another feature of UHRAF is its capability in discovering user involvement that needs to be participated in a Problem Scenario. The advantage of UHRAF's user discovery feature and user requirements analysis capability is that it does not require low-level details of user tasks, like those demanded by task analysis methodology [Diaper, 2004]. Task analysis is useful in defining detailed work-flows; however, its focus is mainly on the task structure and related task information, but lack of exploration on task-to-task interface. Furthermore, in real world practice, most CST projects are time constrained and lack sufficient resources to perform a complete task analysis. UHRAF, on the other hand, emphasizes the interactions between scenarios and therefore more suitable for heterogeneous environment. More importantly, UHRAF does not require low-level task details, because this is the scope of individual domain specific systems, therefore implementing UHRAF processes is more time economical, compared with the task analysis methodology.

Judging from the results of the application of UEA to the scenario as described in *Chapter 5 – Application of the Usability Evaluation Approach*,

we consider that our proposed UEA has achieved a resolution to the research statement of problem.

6.3 Applicability, Acceptability and Effectiveness

After reviewing the achievement of the research statement of problem in the above section, we are now assessing whether the three research questions have been answered by the proposed UEA. These research questions can be represented by applicability, acceptability and effectiveness, as described in the following sections.

6.3.1 Applicability

The first research question is re-iterated below, which also implies the applicability of the solution to the real world practice needs to be validated.

Research Question 1 – How can we formulate the requirements analysis activities to facilitate the design of HCI from a number of domain specific systems in a heterogeneous safety-critical CST system?

To answer this research question, we need to show our proposed UEA has demonstrated its ability in formulating requirements analysis activities to facilitate the design of HCI for heterogeneous safety-critical CST system. In assessing the achievement for answering this research question, we have summarized our views based on the results obtained from the application of UEA to the real world scenario as reported in this thesis. The followings list our views in this regard:

- We develop UHRAF, which is a scenario-based methodology, to organize the analysis activities. In particular, UHARF adopts a flexible approach, in the sense that from an operational goal level (to determine the Problem Scenario) it will allow maximum flexibility of determining the Problem Scenario; but once a Problem Scenario is determined it will adopt a more structured approach, from forming the Network of Scenarios to Interaction Modeling, which is used to discover scenario-to-scenario information exchange and to determine interactions between scenarios. Due to this flexible approach, activities can be formulated in a way that suites the practical constraints of performing work-place analysis activities. For example, in the process of identifying Problem Scenarios, we need high-level management personnel to participate the analysis process; it is because Problem Scenarios are related to high-level operational goals (originated from social goals expected from the general public that use the CST system). Problem Scenarios do not require low-level details and therefore working-level personnel needs not be participated in this stage.

  Once a Problem Scenario is identified, Scenario Identification task and Scenario Description task can be performed with input from working-level personnel. This will become a more structural approach and will reduce the overall resources required to carry out the analysis activities.

- As discussed in *Chapter 2, Section 2.3.3 – Requirements and Suggestions*, objects and functions are common concepts frequently used by analysis approaches. In UHRAF, the Interaction Modeling also embraces the concept of objects and functions (e.g. object of Train Run Number (TRN) and function of indicating the track circuit occupancy). However, Interaction Modeling employs a 2-level

interaction to categorize the objects and functions, so that there are clear demarcation to separate the owners of these objects and functions, and therefore the characteristics (e.g. spatial and temporal attributes) and applications of objects and functions will become straight forward for analysts and operators to understand their importance; consequently the analysis will benefit from such understanding.

- Also discussed in *Chapter 2, Section 2.3.3 – Requirements and Suggestions*, non-deterministic situation is common for CST systems. However, UHRAF can facilitate the discovery of non-deterministic scenarios and make them become deterministic scenarios. During the development of the Network of Scenarios, opportunity for exploration of un-foreseen scenarios exists. This had been validated in our application of UEA to the scenario of handling tunnel train-fire incidents; for example, the scenario "validation of selected TVS emergency mode" was not apparent in the first place, but became a deterministic scenario that needed to be involved for the Problem Scenario under study.

6.3.2 **Acceptability**

The next research question that we need to review is re-iterated below:

Research question 2 – How can the heterogeneous HCI requirements be represented explicitly from the operator's perspective of a unified system operation?

This research question requires an answer that can explain the representation of heterogeneous HCI requirements from the operator's perspective of a unified system operation. We interpret that if such representation is

accepted it implies that the acceptability of UEA is confirmed. As reported in *Chapter 5 – Application of the Usability Evaluation Approach*, two main work-products were produced, namely, the Network of Scenarios and the Interaction Model. The Network of Scenarios, as shown in Figure 5-7, represented a description of how scenarios interact with each other, within the Problem Scenario of handling the tunnel train-fire incident. This also provided an insight of how interaction would be followed. However, the Network of Scenarios would not be possible to represent an explicit view on HCI requirements without the supplementary information generated by the Interaction Modeling. It is important to point out that this research question emphasizes the operator's perspective of a unified system operation, rather then a system's perspective for which most analysis methodologies assume. We argue that both the Network of Scenarios and Interaction Model fulfilled the requirement imposed by this research question. In the tunnel train-fire scenario, the Network of Scenarios addressed the "scenario flow", instead of specifying what technical functionalities need to be provided by individual domain specific systems. This made an important difference between UHRAF and other analysis methods, such as functional allocation. Furthermore, the Interaction Modeling discovered the types of knowledge that operators must possess in order to complete the interactions and the types of information needed to be exchanged between scenarios; this unfolded the hidden interaction problems that would not be easy to identify by conventional methodologies such as the Task Analysis and Context Analysis.

UEA is a scenario-driven approach and often more than one scenario are needed to illustrate a real-life situation, it is necessary to demonstrate how multiple scenarios can simultaneously be presented to the users. We do agree that a real-life situation consists of multiple scenarios, and this is exactly why we develop UHRAF. During our actual discussion with users, we discovered that a top-down approach was more acceptable by users,

mainly due to its logical sense and people are familiar with top-down approach in the management of large organizations. But in a real-life CST system it may not be always possible, due to the complexity of the situation. Therefore in our UHRAF, we explore Problem Scenarios in a discrete approach, rather than top-down approach. But once we have identified a Problem Scenario, we then use the Network of Scenarios to describe the problem under investigation. The Network of Scenarios is a kind of presentation that is used to describe a set of multiple scenarios in a connected way. More importantly, the connections between scenarios within a Network of Scenarios provide us important clues about the interaction requirements. Furthermore, the users feel more comfortable of reviewing a Network of Scenarios (despite it is not always in top-down approach), plus all their connections, because the Network of Scenarios provides logical scenario flow across the Problem Scenario under investigation, and this scenario flow is used to identify, discover or develop the interaction requirements. Although in practice multiple scenarios may not be presented simultaneously, the concept of Network of Scenarios establishes a connection between these scenarios; as a result, the users are still be able to link these scenarios through the interaction requirements of the Interaction Models. In this regard, we consider that multiple scenarios are practically presented to the users.

6.3.3 **Effectiveness**

To become an effective analysis approach, it must be able to validate the outcome produced. This is the reason why we have the research question 3, as re-iterated below:

Research question 3 – How to validate the HCI analysis result and its representation can provide a solution towards the achievement of safety and usability for a heterogeneous safety-critical CST system?

SUM is designed to validate the HCI analysis result from the safety and usability perspective. It should be noted that SUM does not contain any linkage to the functionalities of domain specific systems. In the scenario of handling tunnel train-fire incident, SUM was used to validate the HCI analysis results and the HCI display artifacts designed by individual domain specific systems. The scenario under test was a complex scenario that involved three domain specific systems, however, the Safety and Usability Matrix (Table 4-4) had effectively pointed out that there was an issue in the aspect of Heterogeneous Information, under the Building Block: Characteristic of Work Environment, which subsequently caused safety and usability impacts to other aspects within SUM. We therefore argue that UEA is an effective approach, which provides a simple validation mechanism to ensure the validity of the analysis outcome.

It should be noted that SUM is a validation mechanism developed for high-level evaluation, regardless of domain specific systems' functionalities; therefore the assessment results and design recommendation are inherently in abstract level, instead of physical and functional level. This is consistent with the research objective and approach as stated in *Section 1.5 – Research Focus and Approach*. Due to the heterogeneity of domain specific systems, it would be impractical for any approach to address all the domain details of domain specific systems; otherwise, it would lose the holistic view of a heterogeneous safety-critical CST system. The approach of UEA enables a holistic view of the complete system to be developed, in particular the interaction requirements between domain specific systems. From the usability test reported in this thesis, it is proven to be feasible to adopt a set of high-level design recommendations and implement them into the physical and functional level of the heterogeneous domain specific systems.

It is possible to compare the HCI design based on UEA approach and the one that based on conventional approach. Apart from those heterogeneous HCI display artifacts as reported in *Chapter 5.3.3 – Safety and Usability Assessment Process*, there are four major critical HCI design factors, which make the differences between the two approaches and the advantages of UEA, as summarized in the following Table 6-1 below:

Table 6-1: Comparison of HCI design based on UEA approach and conventional approach

Critical Design Factors	**UEA Approach**	**Conventional Approach**
Mode switching	UEA addresses the problems of operational scenarios, regardless of individual domain specific systems' HCI characteristics; therefore it will discover the needs from the operational perspective, rather than a domain specific system's perspective. The result is that the HCI design based on UEA Approach will reduce the mode confusion problem by reducing the necessity of mode switching.	Operators are required to navigate individual domain specific systems' modes to locate the operational data; this includes browsing various kinds of HCI displays without coordinated design, which incur additional effort to operators.
Mental models	UEA facilitates operators to develop a mental model with holistic view of the CST system.	Mental models are developed based on individual domain specific systems' characteristics and therefore without a holistic view of the complete CST system.
Situation awareness	UEA helps to design HCI artifacts that enhance operators' situation awareness by providing an integrated information	Situation awareness is difficult to be fully implemented in a heterogeneous safety-critical CST system; it

Critical Design Factors	UEA Approach	Conventional Approach
	presentation, so that both Level 1 (perception of elements in current situation) and Level 2 (comprehension of current situation) of the situation awareness can be smoothly implemented. This will greatly facilitate Level 3 (projection of future status) implementation.	is mainly due to the lack of integrated information presentation.
Heterogeneous information	UEA analyzes the operational scenarios and identifies the information and communication required by the interactions between scenarios. This approach can discover the most important item in a heterogeneous safety-critical CST system, i.e. heterogeneous information, in a lightweight approach.	The concept of heterogeneous information has not been tackled by any conventional approaches.

Each of these four factors is not a new HCI research topic by itself; however, applying these factors to a heterogeneous environment with safety-critical context is a new approach that aims to tackle the problems commonly faced by heterogeneous safety-critical CST systems. As reported in the thesis, UEA has demonstrated it practicality to large-scale CST projects. Despite additional cost and time were incurred during the implementation of UEA at the early stage of the project, the ultimate result was leveraged by the avoidance of potential abortive work or re-design of flawed HCI artifacts, and the smooth execution of statutory inspection.

6.4 Accuracy, Constraints and Limitation

This section provides a summary on the accuracy, constraints and limitation of UEA, based on the experience on the application of UEA to a scenario as reported in *Chapter 5 – Application of the Usability Evaluation Approach*.

The tasks in the Operational Scenario Creation process had provided a relatively straightforward and efficient way to formulate the scenarios under study. It helped to organize a set of complex operating procedures into a Network of Scenarios that was easy to be visualized by analysts who might not be familiar with the domain problem (i.e. railway system). The notion of the Network of Scenarios also facilitated the discussion between the stakeholders and the analysts. In the Interaction Modeling process, the Level-1 Interaction and Level-2 Interaction also demonstrated that a thorough description of HCI was practical. Assessment criteria for heterogeneous HCI were efficiently established. The Safety and Usability Assessment process was conducted smoothly and deficiency conditions were identified by the assessors without major difficulties. In general the accuracy of the result obtained by UEA was plausible.

However, a few points should be noted for the constraints and limitation of UEA. The heterogeneous environment under the usability testing was a typical safety-critical CST system, and the standard operating procedures were generally in place, which facilitated the formation of the Network of Scenarios and Interaction Models for evaluation. If such standard operating procedures (SOP) were not in place, the Network of Scenarios and Interaction Models might take more time to develop and the accuracy might be different; therefore, the performance of UEA would need to be revisited for novel applications. We consider Problem Scenarios can still be identified from other tools, such as Goal Analysis, which can be done by

analyzing the high-level documents, such as the Operating Agreement between the owner / management of the CST System (e.g. the mass-transit railway company) and the governing authority (e.g. the transportation department of the government). Technically, Problem Scenarios can be independent from SOP. However, such high-level documents may not have details for developing Problem Scenarios, therefore it will take longer time to firstly study the high-level documents and then identify the goals, before Problem Scenarios can be developed. If SOP is not available, then the Operational Scenario Creation Process (Process_1) will need to utilize other tools in a more comprehensive way. In this situation, we recommend to explore the applicability of the following three tools:

(1) Guidelines.

Guidelines will become one of the primary sources for the Operational Scenario Creation Process (Process_1). Guidelines usually do not describe the target system in a prescriptive way; instead they only provide operation references, and most of the time such references are documented from other similar systems.

(2) Peer-group Review with operator representatives and safety experts.

This may not provide a direct input for novel applications; however, similar scenarios from established systems may be used to explore new scenarios in novel applications. E.g. In a mass-transit railway system, a driverless-operation will be very different with the traditional operation with train drivers, but certain basic principles in established systems should be able to facilitate the development of new Problem Scenarios.

(3) Safety Case Analysis

This is a conventional method of analyzing safety issues of a large-scale CST system. Its systematic approach to safety analysis continues to be useful in exploring novel scenarios and forming technical basis for Peer Group Review.

Furthermore, the Safety and Usability Assessment process remained to be an area that required expert adjustment; inputs from safety experts, system operators and HCI designers continued to be an important factor in order to obtain a satisfactory result, despite the assessment criteria were well discovered and captured in the Safety and Usability Matrix (Table 4-4).

6.5 Summary Remark

This chapter assesses the applicability, acceptability and effectiveness of UEA in response to the research statement of problem and 3 research questions raised in *Chapter 1, Section 1.4 – Research Statement of Problem*. The assessment is based on formative approach, which was carried out during the implementation on the scenario of handling the tunnel train-fire incident in a mass-transit railway system; and a summative assessment after the completion of all the processes of UEA.

Despite there are rooms for further research to enhance UEA, which will be addressed in the next chapter, we consider the proposed UEA has provided a resolution to the research statement of problem and also answered all issues raised by the three research questions. In addition, we are in the position to confirm that the research conducted matches the focus and approach, as stated in *Chapter 1, Section 1.5 – Research Focus and Approach*. UHRAF has demonstrated its capability to examine the orchestration of heterogeneous types of system-operator interaction, from a unified operational perspective. The Interaction Model has provided two levels of interaction that represent different level of abstraction; and SUM has shown its power to validate the design issues of heterogeneous HCI through the safety and usability assessment. In general we are in the position to declare that the proposed UEA has achieved the research objectives. A number of issues are worthwhile for further discussion as below.

6.5.1 Generality of UEA

Regarding the generality of UEA, it would be optimized if a wide choice of examples were used for establishing that the problems are broader in scope and the solution is general to other types of CST Systems. This research work, however, uses only a mass-transit railway system to illustrate a heterogeneous safety-critical CST system; it is mainly because of the following reasons:

(1) A mass-transit railway system fulfils all the "problem profile" of a heterogeneous safety-critical CST system, as described in *Chapter 3, Section 3.3 – Human Operators, System Operability and HCI in Heterogeneous Safety-critical CST Systems*.

(2) There are other large-scale heterogeneous safety-critical CST systems in Hong Kong, such as Power Generation & Energy Management System, Air-traffic Control System, Water Treatment & Plant Management System, etc.; however, accessing such systems for lengthy research work may require substantial coordination effort between the management of the system and the research team, which requires long-term planning and consultation from statutory authorities.

(3) Timing is also a critical factor; the research idea of UEA was incubated some time ago before the MTR LMC railway project was implemented. We developed UEA, and its subsequent application to the railway project for demonstrating its capability was a joint effort contributed by both the University and MTR. The participation of the candidate to the railway project was one of the most important success factors for the work.

To further establish the generality of UEA and its ability to resolve heterogeneous HCI problems in other large-scale CST systems is definitely a direction that will be pursued. Potential research cooperation between the

University and other major utilities (owners and operators of CST systems) should be explored.

6.5.2 Time and Cost Requirements of Using UEA

Time and cost of using UEA varies and depends on the scope of the CST system. However, there are some essential domain experts that must be required in the analysis team for every system to be analyzed and evaluated by UEA, as listed below:

- Safety specialist – as pointed out in *Chapter 6, Section 6.4 Accuracy, Constraints and Limitation*, safety experts continue to be an important factor to carry out activities related to SUM.
- Operator representative(s) – to carry out operational analysis activities that are related to both UHRAF and SUM. The number of operator representatives depends on the scenarios under investigation, and also the domain knowledge of the operator representatives.
- System integrator – general facilitator and expert in system integration.
- HCI designer(s) from each domain specific system.

In our research work, there were 7 people in the analysis team: 1 safety expert, 2 operator representatives, 1 system integrator, 3 HCI designers (1 from TCS, 1 from TVS and 1 from ICCS). It took about 6 weeks to complete the analysis and evaluation, plus all relevant documentation and work products. Certain members were participated on a part-time basis; it took approximately 30 man-weeks to complete all UEA processes. The exercise was considered longer than expected, because in general the HCI design stage of individual domain specific system is relatively short. Adding additional man-weeks to the project would cause scheduling problem. But as discussed in the thesis, safety cannot be compromised, and

therefore it was worthwhile to apply the UEA for the heterogeneous HCI design.

We argue that the time and cost spent on UEA is justified because it would avoid the occurrence of the HCI problems, as those reported in this thesis; and therefore it would save the cost and time of any abortive work or re-work caused by heterogeneous HCI problems. Furthermore, UEA optimizes the operability of the CST system, and it would significantly reduce the time required for system inspection by the statutory authority. In the tunnel train-fire scenario reported in the thesis, the heterogeneous HCI design that implemented the design recommendation by UEA had received quite positive feedback from the members of the statutory authority. This had significantly reduced the time and cost required for statutory inspection.

6.5.3 Criteria for Resolving Conflicting Views and Defining Success of the System

In real-life projects, time and cost are always important. Stakeholders do have different perspectives on issues and criteria for defining success of the system. In the Problem Scenario that we have reported in the thesis, during the interviewing process operators in the control room playing different roles with associated mental model have expressed their expectation, which were not necessarily consistent with each other. We adopt the following principles to confirm stakeholders' satisfaction of the HCI design:

(1) Risk Assessment.

One of the main purposes of SUM's Building Block: Human Performance & Hazard is to address hazard issues, and risk assessment is the tool to mitigate the risks associated to hazards. Very often we cannot completely remove the hazards, but we can mitigate the risks associate with the hazards, by introducing

appropriate mitigating measures, to "As Low As Reasonable Practical (ALARP)". Once all risks are identified during the design stage and are mitigated and documented with ALARP measures, the design of the system can be considered as completed, from the project point of view. A risk assessment workshop will be conducted together with stakeholders to confirm their acceptance. Therefore it is important to manage the hazards in a proper way with traceability and auditability. Documenting all risks in the form of Risk Register becomes a mandatory process for any heterogeneous safety-critical CST systems. Monitoring and measuring any outstanding items in the Risk Register is a simple but practical process to ensure whether the HCI design issues are properly addressed or not. Risk assessment is a mature process; however, few HCI development methodologies have explicit processes that incorporate risk assessment as their basic component for requirements analysis; UEA is developed to fill the gap between HCI development methodology and safety evaluation.

(2) Prototype Usability Testing

UEA provides an approach to test the design of heterogeneous HCI from domain specific systems; however, it is not aimed to replace the actual prototype testing. In the Problem Scenario reported in the thesis, UEA provides HCI requirements analysis, evaluation, and design recommendation. The design recommendation was subsequently incorporated into the design of respective domain specific systems (also reported in *Chapter 5, Section 5.3.3 – Safety & Usability Assessment Process*), prototypes were then developed and operators were requested to carry out a usability test to ensure the design is acceptable by the majority of operators.

6.5.4 Ramifications and Challenges of Using UEA

There is no apparent ramification for using UEA to carry out the heterogeneous interaction requirements analysis and safety and usability evaluation, despite the essential concept of SUM was required to be introduced to analysis team members. Time consumed on this concept introduction was negligible compared with the entire processes of UEA. There was, however, extra time on operator training to get familiar with the new HCI design reconciled after UEA was applied. This was mainly due to the difference of information representation for TVS zones, track circuits and train run number (TRN) compared with individual domain specific systems' HCI practice. Each operator involved in the tunnel train-fire scenario was provided a half-day training, which included technical briefing and practical session. The total training time required for all responsible operators was considered acceptable. In addition, annual refreshing training (standard training practice for all operators) has included this specific subject into the standard training material, which helped to promote the concept of safety and usability of heterogeneous HCI.

UEA consists of UHRAF and SUM. Analysis team members were familiar with the techniques and tools adopted by UHRAF; therefore, the implementation of UHRAF was relatively straightforward. The main challenge was the Safety and Usability Assessment process. In particular, in the Building Block: Cognitive Characteristics of Human Operators, the aspects of Human Cognition, Mental Model and Situation Awareness involve abstractive and psychological concepts that may not be familiar with analysts, operator representatives and HCI designers. Assessments of these aspects were mainly qualitative despite quantitative time measurement was collected; therefore, it was not uncommon that different opinions and views were raised during the assessment. Furthermore, the mental model of the operators was difficult to alter and it required a lot of effort to convince

the operators to create a new mental model adoptable to the new situation. To overcome the challenge, proper training for analyst members on the subjects related to the Cognitive Characteristics of Human Operators is required.

Chapter 7

Conclusions and Suggestions for Future Research

This chapter concludes the research work and offers some suggestions for future work.

7.1 Conclusions

In our research we have demonstrated how the proposed Usability Evaluation Approach (UEA) was used to analyze and evaluate the heterogeneous HCI design for optimizing the operability of a heterogeneous safety-critical complex socio-technical (CST) system. UEA consists of a Unified HCI Requirements Analysis Framework (UHRAF) and a Safety and Usability Model (SUM), which involves a consideration of safety and usability in three Building Blocks: Characteristics of Work Environment; Human Performance and Hazard; and Cognitive Characteristics of Human Operators. A usability test has shown how UEA was applied in a mass-transit railway system, in a way that can be useful in many other domain applications.

In addition, we have illustrated how a safety-critical operational scenario – a tunnel train-fire incident was handled by collaboration of operators' activities. During the execution of collaborative activities, coherency of heterogeneous HCI reduced the cognitive gap between operators' mental

models, which subsequently enhanced the situation awareness; thus the operation efficiency from perception to actions was improved. On the other hand, incoherent heterogeneous HCI could cause misinterpretation of information with consequent of human errors. We have also demonstrated how assessment was provided by UEA to facilitate the heterogeneous HCI design by identifying the deficiency of incoherent of heterogeneous information that would ultimately cause human errors with serious consequence. The advantage of UEA is that it can be used in the early stage of the HCI design where heterogeneous system designs are carried out concurrently. In our usability test the assessment had identified that there was a gap in the design consideration for train's position between the TCS and TVS, which was confirmed to be one of the vital information for operators to select the correct TVS emergency mode.

UEA requires participation from operator representatives, safety specialists and domain specific systems' designers as assessors. Although the evaluation needed a considerable effort, it was still a practical evaluation that did not involve final HCI products to be developed. We consider safety and usability evaluation is extremely important to govern the design of heterogeneous HCI that can have high impact and serious consequence, therefore allowing assessors to spend additional time and effort to better understand the possible consequences of heterogeneous HCI problems and obtain a design that can prevent operator errors is justified. UEA also allows designers to bridge the operators' cognitive gap caused by information presentations from heterogeneous domain specific systems.

The design of HCI for a heterogeneous safety-critical CST system is a complex process. This is especially the case when designers from various domain specific systems are involved to design a system with high degree of collaborative work in a safety-critical environment, such as a mass-transit railway control room as described in this thesis. When safety-critical

operational scenarios are analyzed, such as the scenario of handling the tunnel train-fire incident described in this thesis, both safety and usability have to be carefully considered in a unified way, which needs to take a holistic view on safety and usability. Although UEA has no conclusive approach to determine an absolute balance between safety and usability, it does however create opportunity for discovering common issues faced by safety and usability. As described in *Chapter 5 – Application of the Usability Evaluation Approach*, the design recommendation actually addressed both safety and usability issues in a coherent way so as to ensure the system operability is acceptable to statutory authority.

UEA was applied to a real world scenario – handling tunnel train-fire incident in a mass-transit railway system, which is a typical heterogeneous safety-critical CST system, with analysis results and design recommendation that eventually resolved issues with safety and usability impact. We can therefore conclude that UEA has achieved its mission to provide a resolution to the research statement of problem, and fully answered the three research questions raised in the beginning of the thesis (*Chapter 1, Section 1.4*). Furthermore we consider the contribution of this work has been achieved as stated in *Chapter 1, Section 1.6 – Research Contribution*.

7.2 Suggestions for Future Research

Despite it is our position that UEA meets the research objective of this thesis and worked well enough in the scenario as described in this thesis, we do consider there is opportunity for additional investigation on enhancing UEA for heterogeneous safety-critical CST systems. To enhance UEA for conducting the safety and usability evaluation, we have identified three main areas that need further research work.

Firstly, the discovery of Problem Scenario in our implementation to the scenario of tunnel train-fire incident in a mass-transit railway system was relatively straight forward. However, this cannot be assumed to be a trivial process for other domain applications, especially for novel applications. We need to explore more research work on this issue, such as developing new tools for capturing operational goals, and to investigate how to link high-level social goals to CST system's operational goals. The tools in particular should lend themselves to a description of operational goals for a specific CST system, for example, operational goals of a mass-transit railway system may be different with an Air Traffic Control system. Goals analysis has not been emphasized currently in UEA, however in order to achieve a more effective Operational Scenario Creation process, we consider future research work on goal analysis for UEA is worth to pursue.

Secondly, UHRAF focuses on the analysis of heterogeneous HCI issues; but we consider the same analysis concept could be applied to the analysis of requirements for interface functions between heterogeneous domain specific systems. As discovered in our scenario in a mass-transit railway system reported in this thesis, train position and Tunnel Ventilation System (TVS) zones are two different concepts exist in separate domain specific systems. However, no such connection was identified by the designers of the Train Control System (TCS) and TVS. We are convinced that this was just one of the many "missing requirement" examples. Without a proper analysis tool such interface information, which is vitally required for the operations of a CST system with heterogeneous domain specific systems, continues to be hidden from the system design, until discovered by system operators at the very late stage, presumably in usability testing stage. Therefore, extending the concept of UHRAF to analyze interface functions requirements is justified for further research effort.

Thirdly, in this thesis UEA is applied to capture and analyze the requirements related to the design of HCI for heterogeneous domain specific systems within a safety-critical CST system; it also defines criteria for safety and usability evaluation. However, the idea advocated by UEA can be further explored for the validation of the HCI design. Validation is the process of confirming that the specification of a phase, or of the complete system, is appropriate and is consistent with the user requirements. In the case of HCI design, the validation involves the confirmation of the design that satisfies the user requirements. It should be emphasized that "user requirements" do not only mean user requirements specifications, but the actual usage of the HCI. By using the scenario-based approach of UEA and its Interaction Modeling process, the actual usage of HCI can be accurately described and modeled. The final HCI design can therefore be validated by checking whether the interactions facilitated by the HCI design are consistent with the actual usage modeled by UEA. Detailed of the validation processes, resources required, and its practicality etc. will need more in-depth studies; however, this is definitely a potential work for future research.

References

ACM, (1997). ACM SIGCHI CURRICULA FOR HUMAN-COMPUTER INTERACTION, 1997. ACM Press.

ANNETT, J. (2004). Hierarchical task analysis. In DIAPER, D. & STANTON, N. (EDS.): *The handbook of task analysis for human-computer interaction*. Lawrence Erlbaum Associates, Mahwah, NJ, USA, pp67-82.

ANTON, A. I. & POTTS, C. (1998). A representational framework for scenarios of system use, *Requirements Engineering*, Vol 3, 1998, pp219-241.

ANTON, A. I. & POTTS, C. (1998b). The use of goals to surface requirements for evolving systems. In *Proceedings of the 1998 International Conference on Software Engineering,* 19-25 April, 1998, Kyoto, Japan, pp157-166.

BAXTER, G. D. & BASS, E. J. (1998). Human error revisited: some learns for situation awareness. In the *4th Symposium on human interaction with complex systems, HICS'98*, pp81-87.

BEDNY, G. & MEISTER, D. (1997). *The Russian theory of activity: current applications to design & learning*. Mahwah, N.J. Lawrence Erlbaum Associates.

BEGG, I. M., GNOCATO, J. & MOORE, W. E. (1993). A prototype intelligent user interface for real-time supervisory control systems. In *Proceedings of the ACM, Intelligent User Interfaces '93*, pp211-214.

BEYNON-DAVIES, P. (1999). Human error and information systems failure: the case of the London ambulance service computer-aided dispatch system project. *Interacting with Computers* 11 (1999), pp699-720.

BLACKBURN, J. ET AL. (2000). Concurrent software development. *Communications of the ACM,* 43, 11, pp200-214.

BOOCH, G. ET AL. (2005). *The unified modeling language user guide.* Upper Saddle River, NJ: Addison-Wesley.

BOURNE, A. & CAREY, M. (2001). Integrating human factors into the development of railway systems. People in Control: *An International Conference on Human Interfaces in Control Rooms, Cockpits and Command Centres,* (June 2001), pp25-30.

BRANKI, N. E. (1993). *An AI based framework for collaborative design.* AAAI Technical Report WS-93-07.

BREHMER, B. (1991) Distributed decision making: some notes on the literature. In RASSMUSSEN, J., BREHMER, B. & LEPLAT, J. (EDS.): *Distributed decision making: cognitive models for co-operative work.* Chichester: Wiley and Sons.

BRIDGER, R. S. (2009). *Introduction to Ergonomics*. CRC Press.

CACCIABUE, P. C. (1997). A methodology of human factors analysis for system engineering: theory & applications. *IEEE Transactions on system, man and cybernetics – Part A: Systems and Human,* Vol. 27, No. 3, May 1997, pp325-339.

CALVARY, G., COUTAZ, J. & THEVENIN D. (2001). A unified reference framework for the development of plastic user interfaces. In *Proceedings of the EHCI 2001,* LNCS 2254, pp179-192.

CARD, S. K., MORAN, T. P. & NEWELL, A. (1983). *The Psychology of Human-Computer Interaction.* Lawrence Erlbaum Associates.

CARROLL, J. M. (1997). Human-computer interaction: psychology as a science of design. *International Journal of Human-Computer Studies* 46 (1997), pp501-522.

CARROLL, J. M. (2000). *Making use: scenario-based design of HCI,* Cambridge MA, MIT Press.

CARROLL, J. M. & OLSON, J. R. (1987). *Mental models in human-computer interaction: research issues about what the user of software knows,* Washington, D.C., National Academy Press.

CENELEC (2001). *Railway applications – software for railway control and protection systems. EN50128.* 17, Avenue Marinx, B-1000 Brussels, Belgium.

CERN (2006). *Engineering Data Management Service.* European Organization for Nuclear Research.

CHANDLER, D. (2007). *Semiotics: the basics, 2nd edition.* Routledge, London, UK.

CONNORS, M. M., HARRISON A. A. & SUMMIT, J. (1994). Crew systems: integrating human and technical subsystems for the exploration of space, *Behavior Science*, 39 (3), 1004, pp183-212.

CRAIK, K. J. W. (1943). *The Nature of Explanation*, Cambridge: Cambridge University Press, UK.

CRYSTAL, A. & ELLINGTON, B. (2004). Task analysis and HCI: approaches, techniques, and level of analysis. In *Proceedings of the Tenth Americans Conference on Information Systems*, New York, NY, August 2004, pp1-9.

DAABAJ, Y. (2002). An evaluation of the usability of HCI methods in support of the development of interactive systems. In *Proceedings of the 35th Hawaii International Conference on System Sciences.*

DIAPER, D. (2002). Human-computer interaction. In: MEYERS, R.B. (EDS.), 3rd ed*., the Encyclopedia of Physical Science and Technology,* Vol. 7, Academic Press, pp 394-400.

DIAPER, D. (2004). Understanding task analysis for human-computer interaction. In DIAPER, D. & STANTON, N. (EDS.*): The handbook of task analysis for human-computer interaction.* Lawrence Erlbaum Associates, Mahwah, NJ, USA, pp5-47.

DIAPER, D. & SANGER, C. (2006). Tasks for and tasks in human-computer interaction. *Interacting with Computers*, 18 (2006), pp117-138.

DILLON, A. (1997). Introduction to Current Research in Human-Computer Interaction. *Journal of the American Society for Information Science*, 48(11), pp965-969.

DIX, A. ET AL. (2004). *Human-computer interaction, 3rd edition.* Prentice Hall.

EARTHY, J. V. (1995). *Full HAZOPS of programmable electronic systems. Contesse Project Report No. 7266-9-0-0.3.* Lloyds Register, Croydon, UK.

EASON, K. (1988*). Information Technology and Organizational Change.* Taylor and Francis, London, UK.

EMERY F. E., & TRIST, E. L. (1960). Socio-technical systems. In C. W. CHURCHMAN, & VERHULST, M. (EDS.), *Management Science Models and Techniques (Vol. 2, pp. 83-97).* Oxford, UK: Pergamon.

ENDSLEY, M. R. (1996). Automation and situation awareness. In PARASURAMAN & MOULOUA (EDS.): *Automation and human performance: Theory and applications.* Mahwah, NJ, Lawrence Erlbaum, pp163-181.

ENDSLEY, M. R. (2000). Theoretical underpinnings of situation awareness: a critical review. In ENDSLEY, M. R. & GARLAND, D. J. (EDS.): *Situation awareness analysis and measurement.* Mahwah, NJ., Lawrence Erlbaum Associates, pp3-29.

ENDSLEY, M. R. (2001). Designing for situation awareness in complex systems. In *Proceedings of the 2nd international workshop on symbiosis of humans, artifacts and environment*. Kyoto, Japan.

FAA. (1996). *Federal Aviation Administration Human Factors team report on: The interfaces between flightcrews and modern flight deck systems*. FAA, USA.

FAULKNER, X. (2000). *Usability Engineering*. Macmillan Press Ltd., USA.

FILGUEIRAS, L. V. L. (1999). Human performance reliability in the design-for-usability life cycle for safety human-computer interfaces. In FELICI, KANOUN & PASQUINI (EDS.): *SAFECOMP'99*, LNCS 1698, Springer Berlin/Heidelberg, pp79-88.

FINKELSTEIN, A. & DOWELL, J. (1996). A comedy of errors: the London Ambulance Service case study. In *Proceedings of the 8th International Workshop on Software Specification and Design (IWSSD '96).* IEEE, pp2-4.

FISCHER, G. (2001). User modeling in human-computer interaction. *User Modeling and User-Adapted Interaction,* 11, pp65-86.

GALLIERS, J., SUTCLIFFE, A. & MINOCHA, S. (1999). An impact analysis method for safety-critical user interface design. *ACM Transaction on Computer-Human Interaction,* Vol. 6, No. 4, December 1999, pp341-369.

GO, K. & CARROLL, J. M. (2004). Scenario-based task analysis. In DIAPER, D. & STANTON, N. (EDS.): *The handbook of task analysis for human-computer interaction*. Lawrence Erlbaum Associates, Mahwah, NJ, USA, pp117-134.

GODDARD, P. L. ET. AL. (2000). Software FMEA techniques. In *Proceedings Annual Reliability and Maintainability Symposium,* IEEE, pp118-123.

GOULD, J. D. & LEWIS, C. (1983). Designing for usability: Key principles and what designers think. In *Proceedings CHI'83*, ACM Press, NY, USA, pp50-53.

GRUDIN, J. (2005). Three faces of human-computer interaction. *IEEE Annals of the History of Computing*, pp46-62.

HERRMANN, T. & LOSER, K. U. (1999). Vagueness in models of socio-technical systems. *Behavior & Information Technology*, 1999, Vol., 18, No. 5, pp313-323.

HOC, J-M (2000). From human-machine interaction to human-machine cooperation. *Ergonomics*, 2000, Vol. 43, No. 7, pp833-843.

HOLLAN, J., HUTCHINS, E. & KIRSH, D. (2000). Distributed cognition: toward a new foundation for human-computer interaction research. *ACM Transactions on Computer-Human Interaction*, Vol. 7, No. 2, June 2000, pp174-196.

HOLLNAGEL, E. (1993). *Human Reliability Analysis – context and control*. Academic Press Inc., New York, US.

HOLLNAGEL, E. (1998). *Cognitive Reliability and error analysis method – CREAM*. Elsevier.

HUA, Q. ET AL. (2005). From conceptual modeling to architecture modeling – a User-Centered Design (UCD) method for interactive systems. In: REN, X., & DAI, G. (EDS.): *Evolution of the human-computer interaction.* Nova Science Publishers, Inc. pp103-108.

HUGO, J. 2005. The semiotics of control room situation awareness. In *Proceedings of the 4th International Cyberspace Conference on Ergonomics*, Johannesburg, International Ergonomics Association Press.

HUTCHINS, E. (1994). In search of a unit of analysis for technology use. *Human-Computer Interaction*, Vol. 9, pp78-81.

HUTCHINS, E. (1995). How a cockpit remembers its speed. *Cognitive Science*, Vol. 19, pp265-288.

IBM (1993). IBM Dictionary of Computing (1993).

IEC, (1998). International Electrotechnical Commission, *International standard – functional safety of electrical/electronic/programmable electronic safety-related systems.* IEC 61508.

IEC, (2002). International Electrotechnical Commission, *Functional safety and IEC 61508 – A basic guide.*

INAGAKI, T. (2006). Design of human-machine interactions in light of domain-dependence of human-centered automation. *Cognition, Technology & Work* (2006) 8, pp161-167.

ISO, (1998). International Organization for Standardization, *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 11: Guidance on usability*. ISO 9241-11.

ISO, (1999). International Organization for Standardization, *Human-centred design processes for interactive systems.* ISO 13407.

ISO/IEC TR 9126-4, (2004). International Organization for Standardization, *Software engineering -- Product quality -- Part 4: Quality in use metrics*.

JARKE, M. ET AL. (1998). Scenario management: an interdisciplinary approach. *Requirements Engineering* (1998), 3, pp155-173.

JEROME, B. & KAZMAN, R. (2005). Surveying the solitudes: an investigation into the relationships between human-computer interaction and software engineering in practice. In SEFFAH, A. (EDS.): *Human-centered software engineering – integrating usability in the development process,* Springer, pp59-70.

KIERAS, D. (2004). GOMS models for task analysis. In DIAPER, D. & STANTON, N. (EDS.): *The handbook of task analysis for human-computer interaction.* Lawrence Erlbaum Associates, Mahwah, NJ, USA, pp83-116.

KOTONYA, G. & SOMMERVILLE, I. (1998). *Requirements engineering: process and techniques*, Chichester: John Wiley.

LAMSWEERDE, A. V. (2000). Requirements engineering in the year 00: a research perspective. In *Proceedings of the 22nd International Conference on Software Engineering*, January 2000, ACM Press, pp5-19.

LAWRENCE, J. D. (1995). *Software safety hazard analysis, version 2.0, prepared for US Nuclear Regulatory Commission.* Lawrence Livermore National Laboratory, USA.

LEITE, J. C. S. P. ET AL. (2000). A scenario construction process. *Requirements Engineering,* 2000 (5), pp38-61.

LEVESON, N. G. (1995). *Safeware: System Safety and Computers.* Addison-Wesley Longman Publish Co., Inc., Reading, MA.

LEVESON, N. G. & TURNER, C. S. (1993). An investigation of Therac-25 accidents. *IEEE Computer* 26, 7, July 1993, pp18-41.

LIMBOURG, Q. & VANDERDONCKT, J. (2004). Comparing task models for user interface design. In DIAPER, D. & STANTON, N. (EDS.): The handbook of task analysis for human-computer interaction. Lawrence Erlbaum Associates, Mahwah, NJ, USA, pp135-154.

LINDGAARD, G. ET AL. (2006). User needs analysis and requirements engineering: theory and practice. *Interacting with Computers,* 18 (2006), pp47-70.

MAIDEN, N. ET AL. (1998). CREWS-SAVRE: Systematic scenario generation & use. In *Proceedings 3rd International Conference on Requirements Engineering*, 6-10 April, 1998, pp148-155.

MALONE, T. W. & CROWSTON, K. (1993) What is coordination theory and how can it help design cooperative systems? In BAECKER (ED): *Readings in groupware and computer-supported cooperative work: assisting human-human collaboration*, California: Morgan Kaufman, pp375-388.

MAVIN, A. & MAIDEN, N. (2003). Determining socio-technical systems requirements: experience with generating and walking through scenarios. In *Proceedings 11th IEEE International Requirements Engineering Conference*, 8-12 Sept, 2003, USA, pp213-222.

MAYHEW, D. J. (1999). *The Usability Engineering Lifecycle - A Practitioner's Handbook for User Interface Design*. Morgan Kaufmann Publisher, USA.

MAYHEW, D. J. (2003). Requirements specifications within the usability engineering life cycle. In JACKO, J. A. & SEARS, A. (EDS.): *The human-computer interaction handbook: Fundamentals, evolving technologies and emerging applications,* Lawrence Erlbaum Associates, Mahwah, NJ, USA.

McDERMID, J. A. & PUMFREY, D. J. (1994). A development of hazard analysis to aid software design. In *Proceedings COMPASS '94 'Safety, Reliability, Fault Tolerance, Concurrency and Real Time, Security*, pp17-25.

MELGUIZO, M. ET AL. (2004). Groupware task analysis and distributed cognition: task modeling in a case of multiple users and multiple organizations. In: VIDAL, J.L. (EDS.): *HCI related papers of Interaccion* 2004. Springer, Netherlands.

MERRILL, M. D. (2000). Knowledge objects and mental models. In *Proceedings of the International Workshop on Advanced Learning Technologies*, 2000, pp244-245.

MILLER, R. B. (1971). Human ease of use criteria and their tradeoffs. *IBM Technical Report TR 00.2185*. Poughkeepsie, NY: IBM Corporation.

MIREL, B. (2004). *Interaction design for complex problem solving*. Morgan Kaufmann, USA.

MONK, A. F. & GILBERT, N. (1995). *Perspectives on HCI – Diverse approaches.* Academic Press, London, UK.

MORAN, T. (1981). The command language grammar: A representation for the user interface of interactive computer systems. *International Journal of Man-Machine Studies* 15.

MTRC, 2010. *MTRC Annual Report.*

MYERS, B. A. (1998). A brief history of human-computer interaction technology. *Interactions,* March-April, 1998.

NEWELL, A. (1990). *Unified theories of cognition.* Cambridge, MA., Harvard University Press.

NIELSEN, J. (1993). *Usability Engineering.* Boston, MA: Academic Press.

NORMAN, D. (1983). Some observations in mental models. In GENTNER, D. & STEVENS, A.L. (EDS.): *Mental Models*, Lawrence Erlbaum Associates, USA, pp7-14.

NORMAN, D. (1988). *The Psychology of Everyday Things.* Basic Books, USA.

NORMAN, D. (1991). Cognitive artifacts. In CARROLL, J. M. (EDS.): *Designing interaction: psychology at the human-computer interface*, Cambridge, Cambridge University Press, pp17-38.

NTUEN, C. A. & PARK, E. H. ET AL. (1996). *Human interaction with complex systems: conceptual principles and design practice.* Kluwer Academic Publishers.

ORAVEC, J. A. (1996). *Virtual individuals, virtual groups: human dimensions of groupware and computer networking*, Cambridge University Press, N.Y. USA.

PALANQUE, P. ET AL. (2004). Safety-critical interaction: usability in incidents and accidents. *CHI 2004,* April 24-20, 2004, Vienna, Austria, ACM, pp1600-1601.

PICCINI, M. (2002). Human factors in the design of supervisory control systems and human-machine interfaces for highly automated complex systems. *Cognition, Technology & Work*, 4 (2002), pp256-271.

POTTS, C. (1999). ScenIC: A strategy for inquiry-driven requirements determination. In *Proceedings IEEE Fourth International Symposium on Requirements Engineering (RE'99)*, University of Limerick, Ireland, pp58-65.

REDMILL, F. & RAJAN, J. (1997). *Human factors in safety-critical systems*. Butterworth-Heinemann, UK.

RIERA, B. (2001). Specifications, design and evaluation of an advanced human-adapted supervisory system. *Cognition, Technology & Work*, 3 (2001), pp53-65.

ROGERS, Y. & ELLIS, J. (1994). Distributed cognition: an alternative framework for analyzing and explaining collaborative working. *Journal of Information Technology*, 9, pp119-128.

ROGNIN, L., SALEMBIER, P. & ZOUINAR, M. (2000). Cooperation, reliability of socio-technical systems and allocation of function. I*nternational Journal of Human-Computer Studies,* 52, pp357-379.

ROLLAND, C., SOUVEYET, C., ACHOUR, C. B. (1998). Guiding goal modeling using scenarios. *IEEE Transaction on Software Engineering,* 1998, 24(12), pp1055-1071.

ROSSON, M. B. & CARROLL, J. M. (2002). *Usability engineering – scenario-based development of HCI*. Morgan Kaufmann Publishers.

SANDOM, C. (1999). Situational awareness through the interface: evaluating safety in safety-critical control systems. *People in Control: An International Conference on Human Interfaces in Control Rooms, Cockpits and Command Centers,* 21-23 June 1999, Conference Publication No. 463, IEE, pp119-124.

SARTER, N. B. & WOODS, D. D. (1995). How in the world did I ever get into that mode: more error and awareness in supervisory control. *Human Factors*, 37 (1), pp5-19.

SEC, (2003). Safeware Engineering Corporation, *white papers – human computer interaction.* http://www.safeware-eng.com.

SEFFAH, A., DESMARAIS, M. & METZKER, E. (2005). HCI, usability and software engineering: present and future. In SEFFAH, A. (EDS.): *Human-centered software engineering – integrating usability in the development process*, Springer, pp37-57.

SEFFAH, A. & GULLIKSEN, J. (2005). An introduction to human-centered software engineering: integrating usability in the development process. In SEFFAH, A. (EDS.): *Human-Centered Software Engineering – Integrating Usability in the Development Process*, Springer, pp3-14.

SEFFAH, A. & METZKER, E. (2004). The obstacles and myths of usability and software engineering. *Communication ACM,* 47 (12), pp71-76.

SHACKEL, B. (1959). Ergonomics for a computer. *Design* 120, pp36-39.

SHACKEL, B. (1986). Ergonomics in design for usability. In *Proceedings of the Conference of British Computer Society Human Computer Interaction Specialist Group*; York (UK) pp44-64.

SHACKEL, B. (1997). Human-computer interaction – whence and whither? *Journal of the American Society for Information Science*, 48 (11), pp970-986.

SHARP, H., ROGERS, Y. & PREECE, J. (2007). *Interaction design, beyond human computer interaction*. Wiley & Son, Inc.

SHNEIDERMAN, B. (1998). *Designing the user interface – strategies for effective human-computer interaction, 3rd edition.* Addison and Wesley.

SIMON, H. A. (1996). *The sciences of the artificial*, 3rd edition, MIT Press, USA.

SMITH, A. (1997). *Human-computer factors: a study of users and information systems*. McGraw Hill, England.

STAMATIS, D. H. (1995). *Failure mode and effect analysis: FMEA from theory to execution.* Milwaukee, Wisc. : ASQC Quality Press.

STANTON, N.A. (2004). The psychology of task analysis today. In DIAPER, D. & STANTON, N. (EDS.): *The handbook of task analysis for human-computer interaction.* Lawrence Erlbaum Associates, Mahwah, NJ, USA, pp569-584.

STOREY, N. (1996). *Safety-critical computer systems*. Addison Wesley Longman, Essex, UK.

SUTCLIFFE, A. G. (2000). Requirements analysis for socio-technical system design. *Information System,* Vol. 25, No. 3, pp213-233.

SUTCLIFFE, A. G. (2002). *User-Centred Requirements Engineering – theory & practice*, Springer, London, UK.

SUTCLIFFE, A. G. (2003). *Scenario-based requirements engineering*. RE 2003 Mini-tutorial.

SUTCLIFFE, A. G. ET AL. (1998). Supporting scenario-based requirements engineering. *IEEE Transactions on Software Engineering*, Vol. 24, No. 12, pp1072-1088.

SUTCLIFFE, A. G. & MINOCHA, S. (1999). Linking business modeling to socio-technical system design. *CaiSE'99, LNCS 1626*, 1999, pp73-87.

SUTCLIFFE, A. G. & RYAN, M. (1998). Experience with SCRAM, a Scenario Requirements Analysis Method. In *Proceedings 3rd International Conference on Requirements Engineering*, 6-10 April, 1998, pp164-171.

SWAIN, A.D. & GUTTMAN, H.E. (1983): *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications NUREG/CR-1278*, Sandia Laboratories, Albuquerque, NM 97185.

SWEBOK. (2000). *Guide to the software engineering body of knowledge, Stone Man version.* Software Engineering Coordinating Committee, IEEE, April 2000.

TAYLOR, F.W. (1947). *The principles of scientific management*. New York : Norton, 1947.

TE'ENI, D., CAREY, J. & ZHANG, P. (2007). *Human computer interaction - developing effective organizational information systems.* John Wiley & Sons, Inc.USA.

TERVEEN, L. G. (1995). An overview of human-computer collaboration. *Knowledge-based Systems Journal, Special Issue on Human-Computer Collaboration* 8 (2-3), pp67-81.

VAN DER VEER, G. C., LENTING, B. F. & BERGEVOET, B. A. J. (1996). GTA: Groupware task analysis - modeling complexity. *Acta Psychologica,* 91, pp297-322.

VAN DER VEER, G. C. & PUERTA-MELGUIZO, M. C. (2003). Mental Models. In JACKO, J. A. & SEARS, A. (EDS.): *The human-computer interaction handbook: fundamentals, evolving technologies and emerging applications*, Lawrence Erlbaum Associates, Mahwah, NJ, USA, pp52-80.

VICENTE, K. J. (2000). HCI in the global knowledge-based economy: designing to support worker adaptation. *ACM Transaction on Computer-Human Interaction,* Volume 7, No.2, June 2000, pp263-280.

VINTER, O., POULSEN, P. M. & LAUESEN, S. (1996). Experience driven software process improvement. *Software Process Improvement '96,* 3rd-5th December 1996, Brighton.

VREDENBURG, K. ET AL. (2002). *User-centered design: An integrated approach.* Prentice-Hall, NJ, USA.

WILSON, J. R. & NORRIS, B. J (2006). Human factors in support of a successful railway: a review. *Cognition, Technology & Work* (2006) 8: pp4-14.

WRIGHT, P. C., FIELDS, R. E. & HARRISON, M. D. (2000). Analyzing human-computer interaction as distributed cognition: the resource model. *Human-Computer Interaction*, Volume 15, pp1-41.

ZHANG, P. & GALLETTA, D. (2006). Foundations of human-computer interaction in management information systems – an introduction. In ZHANG, P. & GALLETTA, D. (EDS.): *Human-computer interaction & management information systems: foundations*. Advances in management information systems. Vladimir Zwass series editior. Published by M.E. Sharpe Inc. NY.