Sistemas Críticos sob a Perspectiva do Design de Interação e Comunicação

Este exemplar corresponde à redação final da Tese devidamente corrigida e defendida por Marcos Salenko Guimarães e aprovada pela Banca Examinadora.

Campinas, 27 de outubro de 2010.

Profª. Drª. Maria Cecília Calani Baranauskas
(Orientadora)

Eliane Martins

Profa. Dra. Eliane Martins
(Co-orientadora)

Tese apresentada ao Instituto de Computação, UNICAMP, como requisito parcial para obtenção do título de Doutor em Ciência da Computação.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP
Bibliotecária: Maria Fabiana Bezerra Müller – CRB8 / 6162

Guimarães, Marcos Salenko

G947s Sistemas críticos sob a perspectiva do design de interação e comunicação/Marcos Salenko Guimarães-- Campinas, [S.P. : s.n.], 2010.

Orientadores : Maria Cecília Calani Baranauskas ; Eliane Martins.

Tese (doutorado) - Universidade Estadual de Campinas, Instituto de Computação.

1.Semiótica. 2.Interação homem-máquina. 3.Comunicação. 4.Engenharia de software. I. Baranauskas, Maria Cecília Calani. II. Martins, Eliane. III. Universidade Estadual de Campinas. Instituto de Computação. IV. Título.

Título em inglês: Critical systems under the perspective of interaction design and communication

Palavras-chave em inglês (Keywords): 1. Semiotics. 2. Interaction human-computer. 3.Communication. 4. Software engineering.

Titulação: Doutor em Ciência da Computação

Banca examinadora: Profa. Dra. Cecília Calani Baranauskas (IC – UNICAMP)
Dra. Maria de Fátima Mattiello Francisco (INPE)
Prof. Dr. Osvaldo Luiz de Oliveira (FACCAMP)
Profa. Dra. Regina Lúcia de Oliveira Moraes (FT – UNICAMP)
Profa. Dra. Ariadne Maria Brito Rizzoni Carvalho (IC – UNICAMP)

Data da defesa: 27/10/2010

Programa de Pós-Graduação: Doutorado em Ciência da Computação

TERMO DE APROVAÇÃO

Tese Defendida e Aprovada em 27 de outubro de 2010, pela Banca examinadora composta pelos Professores Doutores:

Profª. Drª. Maria de Fátima Mattiello-Francisco
INPE

Prof. Dr. Osvaldo Luiz de Oliveira
Faculdade Campo Limpo Paulista

Ariadne M. B. R. Carvalho

Profª. Drª. Ariadne Maria Brito Rizzoni Carvalho
IC / UNICAMP

Profª. Drª. Regina Lúcia de Oliveira Moraes
Faculdade de Tecnologia / UNICAMP

Profª. Drª. Maria Cecília Calani Baranauskas
IC / UNICAMP

Instituto de Computação
Universidade Estadual de Campinas

Sistemas Críticos sob a Perspectiva do Design de Interação e Comunicação

Marcos Salenko Guimarães

Outubro de 2010

Banca Examinadora:

- Profª. Drª. Maria Cecília Calani Baranauskas (Orientadora)
- Drª. Maria de Fátima Mattiello Francisco
  Instituto Nacional de Pesquisas Espaciais - INPE
- Profª. Drª. Ariadne Maria Brito Rizzoni Carvalho
  Instituto de Computação - UNICAMP
- Prof. Dr. Osvaldo Luiz de Oliveira
  Faculdade Campo Limpo Paulista - FACCAMP
- Profª. Drª. Regina Lúcia de Oliveira Moraes
  Faculdade de Tecnologia - UNICAMP

Para minha noiva e
minha família.

"... pelo apoio, amor e
pela paciência com a
minha ausência."

“Homens razoáveis se adaptam ao mundo. Homens não razoáveis adaptam o mundo a eles. Por isso é que todo progresso depende de homens não razoáveis.”

(Bernard Shaw)

Resumo

Sistemas críticos têm sido definidos como sistemas cujo fracasso provoca conseqüências catastróficas ou inaceitáveis para a vida humana. A literatura tem relatado vários casos reais de falhas relacionadas à interação e comunicação que levaram a perdas de vidas humanas. Na aviação, muitos incidentes têm causas originadas de falha de interação de pessoas com sistemas computacionais. Este trabalho introduz a perspectiva de comunicação ao sistema crítico utilizando Semiótica e Semiótica Organizacional como bases teórico-metodológicas que sustentam esta pesquisa. Tais bases devem ser capazes de considerar o sistema (crítico) como um todo e também suas partes específicas (por exemplo, interação com o usuário), tanto em seus aspectos técnicos quanto no contexto organizacional; a comunicação está sempre presente entre as pessoas e sistemas envolvidos. O objetivo principal da tese é investigar e propor um modelo de processo de base semiótica para o desenvolvimento de sistema crítico com ênfase na interface de usuário em seus aspectos de comunicação e interação entre seres humanos e sistemas computacionais. Para verificação de aplicabilidade, partes do modelo foram experimentadas em estudos de caso de sistemas aviônicos e espaciais com resultados analisados e trabalhos futuros indicados.

Abstract

Critical systems are defined as systems whose failures provoke catastrophic or unacceptable consequences for human lives. Literature reported several cases of real facts regarding interaction and communication failures that led to losses of human lives. In aviation, many incidents which are originated from failures on interaction with computer systems are examples. This work introduces the communication perspective for critical systems using Semiotics and Organizational Semiotics as theoretical and methodological background. This base provides support for understanding the (critical) system as a whole and also its specific parts (e.g. user interaction), both in technical and organizational aspects; communication is always present among the people and involved systems. The main goal of this thesis is to investigate and propose a process model based on semiotics for the development of critical systems with emphasis on critical aspects of communication and interaction between humans and computer systems. To verify applicability, parts of the model were experimented in case studies in avionics and space systems with analyzed results and future work indicated.

Agradecimentos

Em primeiro lugar, gostaria de agradecer a Deus por permitir a finalização deste trabalho. Aprendi muito no desenvolvimento deste trabalho que se não houvesse cooperação entre pessoas diretamente ou indiretamente, este trabalho não seria realizado com sucesso. Para que atinjamos o objetivo desejado, precisamos de duas bases importantes que nos fortalecem para atingir o objetivo. Por mais difícil que seja para alcançá-lo, é necessário ter a base emotiva, onde envolve sentimentos humanos tais como: o amor fraternal, convivência com amigos, brincadeiras de colegas de trabalho, atividades relacionadas à solidariedade que nos levam ao bem-estar e, conseqüentemente, nos dão sentido de vida que motivam a realização de trabalho. A segunda base é o lado da razão onde adquirimos conhecimentos técnicos, utilizamos a nossa capacidade de discussão técnica para atingir um determinado consenso ou objetivo. Acredito que se não tivéssemos essas duas bases sólidas, teríamos maiores dificuldades, obstáculos para atingir o objetivo desejado. Portanto, agradeço a todas as pessoas que envolveram o desenvolvimento deste trabalho indiretamente ou diretamente, particularmente os seguintes nomes:

1 - Aos meus pais e meus irmãos pela compreensão, pela força e pelo apoio contínuo para realizar os objetivos de vida e até mesmo dos sonhos.

2 - À Luciana e sua família por compreenderem o meu projeto de vida.

3 - À professora Cecilia Baranauskas pelas orientações, dicas, críticas, elogios, pela paciência enquanto eu tinha dificuldade de entender a idéia nova.

4 - À professora Eliane Martins, além das orientações importantes do trabalho, nos ajudou a encontrar um projeto para aplicar como estudo de caso depois de muito esforço e dedicação.

5 - À Fátima Francisco do Instituto Nacional de Pesquisas Espaciais (INPE) por oferecer a oportunidade valiosa em trabalhar no projeto SAPOP como estudo de caso da tese e também permitiu o nosso acesso aos controladores de operação do INPE, por fornecerem detalhes importantes na operação do sistema de controle de satélite.

6 - Ao grupo Conversando com a Cecília e InterHAD pelas críticas e elogios dos meus ensaios; das conversas descontraídas e valiosas trocas de experiências.

7 - Aos líderes de projeto do Instituto Eldorado por permitirem algumas horas de trabalho para me dedicar ao trabalho acadêmico.

8 - Aos funcionários do Instituto de Computação por me passarem informações úteis nas questões burocráticas.

Gostaria de destacar o grande apoio financeiro do Instituto de Computação da UNICAMP e parte dos recursos da FAPESP viabilizando a realização de apresentações em conferências internacionais.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

ATC	Air Traffic Control
FMC	Fractal Model of Communication
FS	Framework Semiótico
HCI	Human-Computer Interaction
IHC	Interação Humano-Computador
MEASUR	Methods for Eliciting, Analysing *and Specifying Users' Requirements*
MFC	Modelo Fractal de Comunicação
NAM	Norm Analysis Methods
OC	Operation Coordinator
PAM	Problem Articulation Methods
PAV	Personnel Air Vehicle
QA	Quadro de Avaliação
SAPOP	Sistema de Apoio à Operação de Cargas Úteis de Satélites Científicos
SL	Semiotic Ladder
SO	Semiótica Organizacional
SVS	Synthetic Vision Systems
UI	User Interface

Capítulo 1

Introdução, Objetivos e Metodologia

1.1 Visão Geral

Atualmente, há uma demanda crescente por sistemas de hardware e software em áreas críticas que eram executadas por seres humanos. Há vários estudos relativos a este tipo de sistemas, e o conceito de sistema crítico tem sido discutido por vários autores.

Apesar de não haver um consenso sobre a definição de sistemas críticos, a maioria dos pesquisadores define sistemas críticos como sendo sistemas cujo fracasso provoca conseqüências catastróficas ou inaceitáveis para a vida humana. Palanque et al. (1998) complementa esta definição informando que o fator de custo também é importante: o custo de desenvolvimento de um sistema crítico é menor que o custo potencial gerado pela falha do sistema. A ênfase das definições está nas conseqüências da falha de sistema que podem conduzir a situações catastróficas, inadmissíveis ou grandes danos que envolvem questões financeiras ou perda de vida humana. Paulson (1997) estende ainda mais este estudo conceitual classificando tais sistemas em três tipos da seguinte forma:

- Safety-critical system – é um sistema cujo fracasso afeta a vida humana. Por exemplo, aviônicos (sistema de hardware e software para aeronaves), sistemas de navegação, controle de tráfego aéreo, alguns sistemas militares, sistemas automotivos (por exemplo, ABS ou sistema de frenagem anti-bloqueio), usinas nucleares, sistemas hospitalares (por exemplo, corações artificiais);

- Mission-critical system – é um sistema que é visto como parte essencial de um produto específico. Se o software (geralmente, software embarcado) não funciona corretamente, o produto se torna total ou parcialmente inútil. Geralmente, esta falha de software conduz a grandes danos financeiros que forçam os fabricantes a realizarem um recall, chamada aos consumidores para troca do produto ou para substituição de uma peça a fim de corrigir um defeito. Por exemplo, se o software embarcado de um telefone celular ou de um televisor possui um defeito que é considerado grave, o fabricante terá que substituir este produto incluindo a correção do software. Se for um defeito grave de software embarcado em um satélite espacial, o custo é muito elevado ou até mesmo pode ser inviável tecnicamente ou financeiramente fazer correções.

- Security-critical system – é um sistema relacionado à segurança de informação. Em outras palavras, o sistema tem que evitar o acesso não-autorizado a uma informação. Por exemplo, um portal Web para compra de um produto não deve permitir uma intrusão para obter números do cartão de crédito de um cliente. Se isso ocorrer, a empresa não só terá danos financeiros, mas também perderá a confiança dos consumidores levando a grandes prejuízos financeiros e de reputação.

Uma diferença entre safety-critical systems e security-critical systems, além do efeito direto na vida humana no caso dos primeiros, está na intencionalidade que leva ao fator crítico. Os safety-critical systems são sistemas que devem lidar com defeitos causados por erros não intencionais (usuário trocou dois dígitos tornando um número inválido para o sistema); já os security-critical systems, com erros intencionais (por exemplo, intrusão causada por pessoas com intenção de atacar o ponto vulnerável de um sistema).

Existem outras áreas de pesquisa relacionadas direta ou indiretamente a sistemas críticos, envolvendo os conceitos de Dependabilidade e Resiliência, brevemente descritos a seguir:

1.1.1 Dependabilidade

Avizienis. et. al. (2001) apresentam as primeiras definições de dependabilidade e mostram que estas vem evoluindo ao longo dos últimos anos. Knight (2004) define dependabilidade como sendo um sistema que possui seis atributos (o atributo Manutenibilidade foi adicionado à definição do Avizienis):

- Confiabilidade – o sistema deve operar corretamente quando usado;
- Disponibilidade - o sistema deve ser operacional quando necessário;
- Segurança - o sistema deve operar sem perigo;
- Confidencialidade - nenhuma informação sem autorização é usada durante a execução de sistema;
- Integridade - nenhuma modificação sem autorização de informação é feita durante o uso do sistema;
- Manutenibilidade - possibilidade de manutenção de software.

1.1.2 Resiliência

O projeto ReSIST (ReSIST, 2008) foi criado como sendo um novo campo de estudo, o de Sistemas Resilientes, que inclui os sistemas críticos. Vários gaps e desafios relacionados à tecnologia de resiliência foram discutidos pelos pesquisadores em termos de arquitetura, algoritmos, fatores sócio-técnicos, aspectos de verificação e avaliação. A resiliência necessita englobar vários aspectos incluindo a usabilidade de sistemas e, particularmente, em sistemas ubíquos. Para contribuir na interação de usuários com os sistemas ubíquos, há necessidade de entendimento de efeitos potenciais de suas ações e também prevenções deles das ações indesejadas e das dificuldades para antecipar os possíveis efeitos no nível de sistemas. A usabilidade é considerada um dos mais importantes aspectos a serem considerados em sistemas críticos; gaps e desafios ainda se encontram na fase inicial de identificação no projeto ReSIST.

1.2 Justificativa e Objetivos

A literatura tem relatado vários casos reais de falhas na interação humano-sistemas computacionais resultando grandes perdas de vidas humanas. Um dos casos emblemáticos é o do Therac-25, que se trata de um sistema hospitalar com dupla função: a emissão de raios-X para obtenção de imagens da estrutura óssea e emissão de radiação para tratamento de tumores. O caso de emissão de radiação causou a morte de várias pessoas por um longo período de tempo devido a mensagens obscuras "Malfunction 54." do sistema. Felciano (1997) e Mackie e Sommerville (2000) mencionam que esta mensagem de erro não teve nenhum significado para os operadores do equipamento, que a ignoraram. Porém, para o desenvolvedor do software, a mensagem estaria informando que a dosagem de radiação estava acima do normal. Devido a este problema de comunicação na interface de usuário, a conseqüência deste episódio foi desastrosa levando a várias mortes devido a radiação extrema injetada em pacientes. Mais dramaticamente, como o efeito da alta dosagem não era instantâneo, foram necessários vários anos de investigação para que o problema fosse identificado.

Na aviação, muitos incidentes (eventos inesperados que podem ou não ser considerados como acidentes com ou sem conseqüências fatais) têm causas originadas de falha na interação de pessoas com sistemas computacionais. Harrison (2004b) mostra as seguintes estatísticas: de 34 incidentes investigados entre 1979 a 1992, 1.100 mortes acidentais estavam relacionadas à falha do sistema computacional; 4% das mortes foram atribuídas a causas físicas; 3% das mortes foram atribuídas a erro de software; 92% das mortes foram associadas a problemas relacionados à interação entre pessoas e sistemas de computador. De acordo com a ATC (Air Traffic Control), 90% dos incidentes de tráfego aéreo são devidos à falha atribuída a pilotos ou controladores.

Em caso recente ocorrido em setembro de 2006, no acidente da Gol (nome de uma companhia aérea que foi envolvida no acidente), duas aeronaves se colidiram no ar na região norte do Brasil levando à morte de 154 pessoas; foi considerado o maior acidente aéreo na história Brasileira. Cantanhêde (2007) menciona que as gravações (transcrições de diálogos entre pilotos e ATC) indicaram que houve uma sucessão de erros e mal-entendidos na interação com a aeronave e também houve problemas de comunicação com o ATC.

No dia 17 de julho de 2007, a aeronave Airbus A320, ao pousar na pista do aeroporto de Congonhas, na cidade de São Paulo (Brasil), não parou no final da pista, extrapolando a área do aeroporto e colidindo com um prédio, resultando na morte de 199 pessoas. Este acidente passou a ser o maior acidente na história da aviação do país, já superando o acidente da Gol. Uma das possibilidades mencionadas para explicar o ocorrido é o erro operacional do piloto devido ao problema do sistema de reverso do motor direito da aeronave. Ao pousar, o piloto com conhecimento de que o reverso do motor direito estava desabilitado, puxou somente o manete do motor esquerdo para trás para acionar o reverso do motor correspondente, mas deixou o manete do motor direito posicionado ligeiramente para frente, ou seja, com uma leve aceleração do motor direito para frente. A combinação do motor esquerdo na frenagem e o direito na leve aceleração levou a aeronave a virar para o lado esquerdo e o efeito da frenagem foi fraco devido à pista molhada impossibilitando que a aeronave pudesse atingir uma velocidade menor desejada causando a tragédia. Portanto, uma das possibilidades para a ocorrência deste acidente parece ter sido o erro relativo à interação com a aeronave.

Segundo Aith et. al.(2007), no dia 27 de março de 1977, no aeroporto Los Rodeos na ilha de Tenerife, ocorreu uma colisão em solo de duas aeronaves de grande porte, o Boeing 747. Este acidente foi o pior acidente aéreo envolvendo aeronaves civis da história da aviação. Houve 583 mortes e 64 sobreviventes. Os relatos em Freissinet (2007) e Victor (2007) mostram claramente que uma das principais causas do acidente foi relacionada a comunicação; o uso de algumas palavras levou a múltiplas interpretações. Por exemplo, um membro do ATC utilizou a palavra "OK" e o piloto da viação aérea KLM, que se mostrava apressado, interpretou que o "OK" se referia à autorização para decolagem, mas para o membro do ATC, se referia à concessão da autorização da rota fornecida pelo ATC que é feita na saída de decolagem do aeroporto. O piloto, de acordo com a sua interpretação, iniciou o procedimento para decolagem. No outro lado da pista, se encontrava a aeronave da viação PANAM. O ATC tinha autorizado a decolagem desta aeronave. Dessa forma, têm-se as duas aeronaves iniciando os procedimentos para decolagem localizadas na mesma pista, mas em extremos opostos. Não foi possível realizar desvio para evitar a colisão; devido ao mal tempo, a visibilidade era limitada. Quando houve a colisão, um motivo que levou a ainda mais mortes foi o incêndio posterior à colisão, pois ambas as aeronaves estavam reabastecidas com tanques repletos de combustível.

Estes relatórios mostram a necessidade de interfaces de usuário confiáveis que levem a melhor interação entre humano e sistema computacional, contribuindo para o uso correto de artefatos críticos e auxiliando na tomada de decisões durante situações de emergência quando os usuários estão em situação potencial de pânico. Um dos fatores que contribui para uma interface de usuário confiável é a qualidade da comunicação, possibilitada via essa interface[1]. Em outras palavras, a qualidade da comunicação pode depender diretamente da qualidade do design da interação. Por outro lado, um design de interface confiável depende da eficiência do sistema de comunicação como um todo.

O objetivo principal deste trabalho é investigar e propor um modelo de processo de base semiótica para o desenvolvimento de sistema crítico com ênfase em seus aspectos de comunicação e interação entre seres humanos e sistemas computacionais. Este trabalho introduz a perspectiva de comunicação ao sistema crítico utilizando Semiótica e Semiótica Organizacional como bases teórico-metodológicas que sustentam esta pesquisa. Tais bases consideram o sistema (crítico) como um todo, tanto em seus aspectos técnicos quanto no contexto sócio-organizacional.

1.3 Visão Geral do Trabalho

Uma análise de literatura baseada em artefato da Semiótica Organizacional constata que os trabalhos realizados ainda não cobrem todas as necessidades dos sistemas críticos. A pesquisa bibliográfica apresentada identifica que há poucas contribuições na camada informal do sistema de informação onde se tem as crenças, culturas e não há trabalhos que sejam abrangentes o suficiente para cobrir todas as camadas de informação necessárias ao desenvolvimento de sistemas críticos.

A Semiótica e Semiótica Organizacional são os principais referenciais teórico-metodológicos utilizados neste trabalho por oferecerem recursos ferramentais que cobrem os níveis informal, formal e técnico de sistemas de informação. A Semiótica é uma disciplina que estuda os signos focando explicitamente em comunicação e a SO é um ramo da Semiótica voltada para os aspectos organizacionais.

Na fase inicial do trabalho, foram identificadas as lacunas de estudos presentes na literatura. Esse estudo identificou a ausência de um processo de desenvolvimento de software que possuísse foco na comunicação de forma explícita. Este trabalho propõe um modelo de processo para ser executado por uma equipe composta por pessoas que não necessariamente executam atividades do processo de desenvolvimento de software (para

[1] "Interação" e "comunicação" são termos utilizados neste texto com significados relacionados, porém distintos. A "interação" significa troca de ações e reações (se houver) entre pessoas e artefatos. O termo "comunicação" envolve compartilhar código e portanto conhecimentos, entre pessoas ou entre artefatos (se aplicável).

menor interferência de trabalho), de forma independente do ciclo de vida definido para o desenvolvimento do software. Este modelo de processo permitirá obter uma nova visão do sistema crítico onde a comunicação será apresentada de forma explicita.

A Figura 1.1 ilustra as áreas de pesquisa em que o modelo de processo proposto neste trabalho se apoia, que correspondem a área comum entre três campos de estudos: Semiótica (na área de Comunicação), Engenharia de Software e Interação Humano-Máquina. Quando um processo de software se encontra na fase de requisitos ou de design, este trabalho provê atividades aplicáveis a estas fases de desenvolvimento propondo artefatos e métodos que permitirão obter uma nova visão (perspectiva) do sistema para a realização de análises no contexto de comunicação; ou seja, auxiliando na identificação de problemas e soluções relacionadas à comunicação. Assim sendo, o resultado esperado envolve obter um sistema com melhorias nos aspectos de comunicação entre sistemas, incluindo maquina e usuário, conseqüentemente na melhoria de interação humano-máquina.

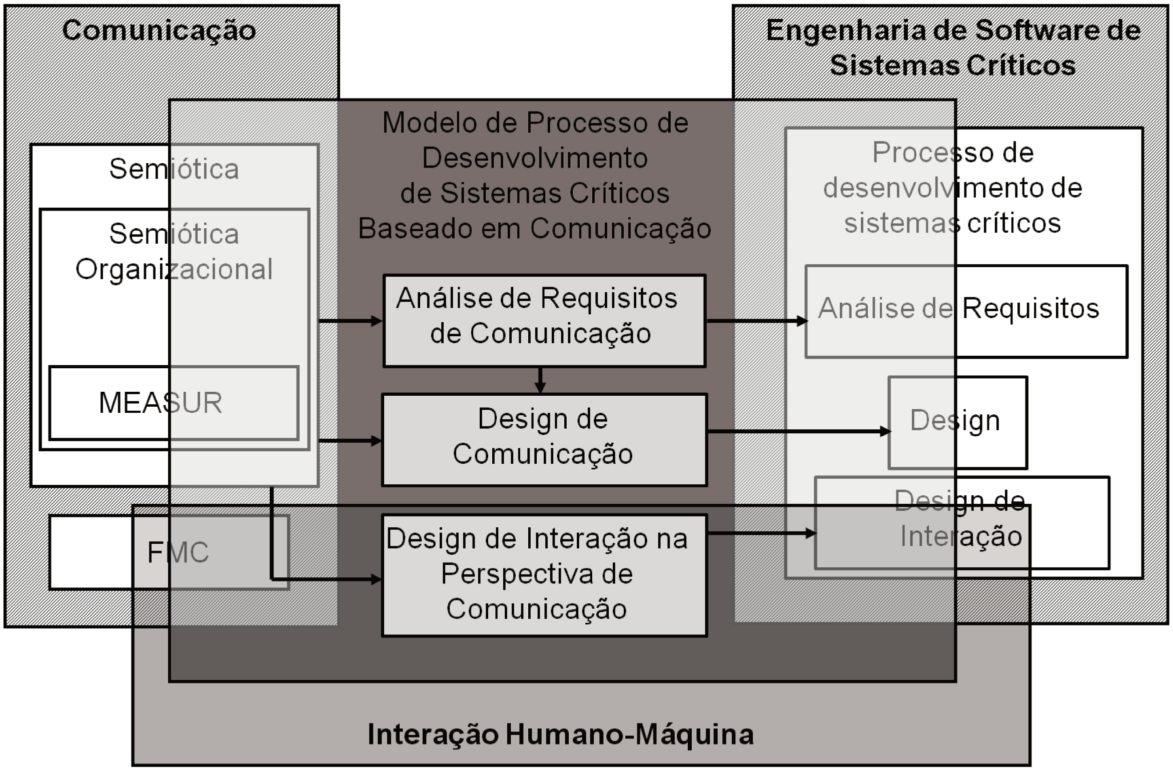

Comunicação
Engenharia de Software de Sistemas Críticos
Modelo de Processo de Desenvolvimento de Sistemas Críticos Baseado em Comunicação
Semiótica
Semiótica Organizacional
MEASUR
FMC
Análise de Requisitos de Comunicação
Design de Comunicação
Design de Interação na Perspectiva de Comunicação
Processo de desenvolvimento de sistemas críticos
Análise de Requisitos
Design
Design de Interação
Interação Humano-Máquina

Figura 1.1: Modelo Contextual de Áreas de Estudos Envolvidas

A comunicação é considerada um recurso bastante utilizado no desenvolvimento de software. Por exemplo, conceitualmente, o analista de requisitos precisa se comunicar com clientes para identificar requisitos do sistema. A comunicação está sempre presente em todas as fases de desenvolvimento de software dentro da organização, da equipe de desenvolvimento e enfim, entre todos os stakeholders envolvidos no sistema. Portanto, em cada fase de desenvolvimento de software, o modelo de processo apoia os aspectos de comunicação no decorrer do desenvolvimento de sistemas, iniciando na fase de requisitos, em seguida, na fase de design e finalmente, na fase de design de interação.

Começando pela fase de elicitação de requisitos do sistema, o modelo de processo para a elicitação, análise e especificação de requisitos utiliza da SO o Método para Elicitação, Análise e Especificação de Requisitos do Usuário (MEASUR, em inglês) (Stamper, 1993). Já o Modelo Fractal de Comunicação (Salles, 2000) oferece um modelo útil para estruturar a comunicação definindo quais elementos (agentes) se comunicam com outros agentes. Com esses modelos, é possível obter informações relacionadas aos requisitos do sistema nos aspectos de comunicação.

Em seguida, na fase inicial de design, os artefatos produzidos durante a fase de requisitos devem ser verificados (inspecionados); o objetivo é encontrar possíveis faltas de informações que serão úteis para a fase de design do sistema. A inspeção consiste em fazer investigações conectando os artefatos produzidos e verificando as consistências das informações especificadas nos artefatos.

Na fase de design, foi desenvolvido um framework que representa uma estrutura de um sistema crítico interativo na perspectiva de comunicação. Além do framework, há procedimentos que permitem gerar, a partir dos artefatos produzidos nas fases anteriores, modelos mais detalhados de um sistema crítico no aspecto de comunicação.

Em seguida, o trabalho trata o design da interação, focando mais nos aspectos de comunicação entre humano e máquina. Apresenta-se o procedimento para a geração de wireframes (estruturas) de interface de usuário a partir dos artefatos produzidos durante a fase de design.

Em cada etapa de desenvolvimento de sistema crítico desde a fase de requisitos, design e design da interação, foram utilizados dois diferentes estudos de caso de um sistema crítico para ilustrar a aplicação do framework e procedimentos; também para analisar os resultados produzidos.

1.4 Contribuições e Organização da Tese

O restante deste texto está organizado em capítulos contendo o texto integral de artigos publicados e um artigo submetido para revista, como segue:

- Capítulo 2: "Interaction in Critical Systems: Conquests and Challenges", Guimarães M. S., Baranauskas M. C. C., Martins E. Em 9th International Conference on Enterprise Information Systems (ICEIS), pp 170-175, INSTICC Press, ISBN: 978-972-8865-92-4, 2007.
    - Este trabalho resume as principais contribuições de diferentes áreas para sistemas críticos, apresenta uma análise baseada em classificação que auxilia na obtenção de diferentes pontos de vista e descobre novas direções de investigação possíveis para melhorar a qualidade de interação com este tipo de sistema.
- Capítulo 3: "A Communication-based Approach to Requirements Elicitation for Safety-Critical Systems". Guimarães M. S., Baranauskas M. C. C., Martins E. Em Complexity in Organizational and Technological Systems, Proceedings of 10th International Conference on Organisational Semiotics, pp 66-75, ISBN 1-87412-15-2/978-1-87412-15-6, 2007.
    - Comunicação é um fator crucial, não só entre stakeholders durante o processo de desenvolvimento, mas principalmente entre os usuários durante a execução de um sistema crítico. Este trabalho investiga uma abordagem semiótica no processo de elicitação de requisitos de comunicação para sistemas críticos. O enfoque é ilustrado com um estudo de caso no domínio de sistemas aviônicos.
- Capítulo 4: " Communication-Based Modelling and Inspection in Critical Systems", Guimarães M. S., Baranauskas M. C. C., Martins E.. Em 10th International Conference on Enterprise Information Systems (ICEIS), pp 215-220, INSTICC Press, ISBN: 978-989-8111-36-4, 2008.
    - O Personal Air Vehicle (PAV) representa uma nova geração de aeronaves de pequeno porte a ser concebida para estender o transporte aéreo pessoal para um segmento maior da população propondo novos conceitos de interação e comunicação na aviação. Neste domínio, a comunicação é um fator crítico, especialmente entre os usuários durante a execução do sistema através de suas interfaces. Este trabalho apresenta uma técnica de modelagem e inspeção de comunicação na interface de usuário no domínio de aviônicos; um estudo de caso ilustra a proposta de artefatos do domínio PAV.
- Capítulo 5: "A Case Study on Modelling the Communication Structure of Critical Systems", Guimarães, M.S., Baranauskas, M.C.C. Em Information Systems in the Changing Era: Theory and Practice, Proceedings of 11th International Conference on Informatics and Semiotics in Organisations, pp 465-472, Aussino Academic Publishing House, ISBN: 978-0-9806057-2-3, 2009.

    - Apresenta um estudo de caso em que o modelo de estrutura de comunicação deste tipo de sistema é representado visando apoiar o design de interação em Safety-Critical systems. A abordagem é baseada na teoria e artefatos da semiótica.

- Capítulo 6: "A Communication based Process Model in Critical Systems Design". Guimarães M. S., Baranauskas M. C. C., Martins E. (Paper submitted), 2010.
    - Propomos um modelo de processo no design de sistemas críticos sob a perspectiva de comunicação, incluindo os aspectos de interação homem-máquina. Semiótica é utilizada como referencial teórico e metodológico. O modelo de comunicação é aplicado em Scientific Satellite Payload Operation Support System (SAPOP), para ilustrar o potencial que essa perspectiva traz para safety-critical systems.

- Capítulo 7: "Interaction Design and Redundancy Strategy in Critical Systems", Guimarães M. S., Baranauskas M. C. C., Martins E. Em Pervasive Informatics in the Digital Economy, Proceedings of 2010 IFIP WG 8.1 Working Conference of 12th International Conference on Informatics and Semiotics in Organisations, pp 165-172, SciTePress, ISBN: 978-989-8425-26-3, 2010.
    - Propomos um procedimento para design de interação em sistemas críticos sob a perspectiva da comunicação, o procedimento possui como saída um wireframe de interface de usuário como resultado. Semiótica é utilizada como referencial teórico e metodológico no procedimento proposto de design. O Scientific Satellite Payload Operation Support System (SAPOP) é usado para ilustrar o potencial dessa perspectiva traz para os safety-critical systems.

Capítulo 2

Interaction in Critical Systems: Conquests and Challenges

2.1 Introduction

Currently, we have experienced a growing demand on hardware and software systems to support the work on critical areas that use to be managed mostly by human beings.

The concept of a critical system has been discussed by several authors, encompassing conceptual to the technical issues. Most of the researchers define critical systems as software-based systems whose failure would provoke catastrophic or unacceptable consequences for human life.

Some authors relate the concept of criticality with dependability in systems. Marhan et. al. (2004) describe a method aiming to support dependability in interactive-safety critical systems. Knight (2004), defines a "dependable system" as a system which has six attributes: Reliability (to operate correctly when used); Safety (to operate with no danger); Confidentiality (no unauthorized information is used during the system execution); Integrity (no unauthorized modification of information is made during the use of the system); and Maintainability (possibility of software maintenance). Precise definitions of terms related to dependability have been developed over a period of many years and are described in Avizienis et. al. (2001).

Literature on critical systems has shown several cases of human-system failures that resulted in people's deaths. Therac-25 is a typical case: an X-ray used to obtain bone images (through x-ray emission) or to treat tumors (through radiation emission). Mackie and Sommerville (2000) mention that this error message had no meanings for the operators, who just ignored it. However, for the software developer, the message intended to inform that the radiation dosage was above normal. Due to this communication problem reflected in the user interface, the consequence of this episode was disastrous leading to several deaths because of the extreme radiation injected to patients. More dramatically, as the effect of over dosage was not instantaneous, it took several years for the problem to be identified.

In aviation systems, many incidents (incidents are unexpected events that may or may not lead to accidents that may lead to deaths) have reasons originated from failures during user-system interaction. Harrison (2004b) shows some statistics: from 34 total incidents, 1.100 computer-related accidental deaths (1979-1992); 4% of the deaths due to physical causes; 3% of the deaths due to software error; 92% of the deaths due to problems related to human-computer interaction. According to ATC (Air Traffic Control), 90% of the air traffic incidents were due to fault attributed to pilots or controllers.

These reports show us the role a reliable user interface (better human-computer interaction) has in enabling the correct use of critical artefacts and supporting decision making mainly during emergency situations when the users are in panic.

We understand that the Human-Computer Interaction (HCI)-related subjects have a role to play and responsibilities to assume in this particular domain. The objective of this work is to summarize some of the main contributions of literature to the field and identify gaps and new challenges related to interaction design in safety-critical systems.

This paper is organised as follows: the next section synthesises relevant contributions for critical systems coming from different fields. Section 2.3 groups the main findings, aiming to help with different views about the conquests so far and new challenges. Section 4 presents new possible directions for research and Section 2.5 concludes.

2.2 Contributions of Literature for Critical Systems

Several disciplines have historically contributed to development in the field of critical systems; the main contributions can be categorized into the following groups:

- Human Factors has contributed especially to our understanding of human errors in critical systems. The main findings in this area have been used to explain human reaction when dealing with critical situations.

- Software Design and Usability focuses on improvements in some parts of a software development process that can be applied to the user interface component. Some authors contribute providing some additional or modified steps in the software development process to improve the quality of the user interface regarding critical systems.

- Socio-Technical Approaches have many critical systems depend on the interaction among a group of people. Socio-technical approaches are necessary to understand the interaction among team members using an artefact.

Several works are proposed in literature for critical systems for improving the quality of human-computer interaction. Most of them involve the areas of human factors and cognitive theories, software design and usability, and socio-technical theories. Some studies can't be categorized only in one approach because they are multidisciplinary in nature. For example, Filipe et. al. (2003) not only focuses on socio-technical but also mentions some user interface design because this work can be applicable for improvements in user interface design. Therefore, the categorization below considered the main topic of each work. The main contributions, grouped by their approaches, are summarized in Table 2.1.

HCI still has more to contribute for critical systems regarding interaction design issues, communications, evaluation and validation techniques. Table 2.1 also shows that the amount of work related to socio-technical aspects applicable to safety critical systems is significantly reduced when compared with the other categories of contributions. This finding doesn't mean that this approach is less important; quite the contrary, the most cited cases related to safety-critical systems, Air Traffic Control (ATC) systems, are socio-technical systems. More details about this system can be found in Hopkin (1995). It clearly involves social issues, human-computer interaction, human-human interaction, besides human factors, cognition, software design and usability.

Table 2.1: Main contributions in interaction for critical systems

Approach	Researcher	Contribution
Human Factors and Cognitive related Theories	(Baxter and Besnard, 2004)	The "glass cockpit" could mean that a pilot would have fewer tasks and problems but the pilot needs to know not only about aviation but also about how to use the system.
	(Hollnagel, 1993)	A model for human behaviour and cognition is presented for understanding emergencies when the operator maintains control, loses control, and/or regains control of the situation.
	(Harrison, 2004a) (Harrison, 2004b)	Methods for obtaining a number (or several numbers) that represents the "dimension" of

	(Smith and Harrison, 2002a) (Smith and Harrison, 2002b)	the human error calculating the error probability and its impact if it occurs.
	(Galliers and Minocha, 2000)	A technique based on BBN (Bayesian Belief Network) model for calculating of probabilities of human error is executed based on this graph.
	(Daouk and Leveson, 2001)	A new approach to structuring specifications, called Intent Specifications, which captures the design rationale and assumptions made throughout the design process.
	(Vicente and Rasmussen, 1992) (Vicente et. al., 1998) (Vicente et. al., 1995) (Vicente, 2002)	A theoretical framework called Ecological Interface Design (EID) for designing user interfaces focusing on environment-human relationship analyzing the perception of the work environment that affects human behaviour.
Software Design and Usability	(Palanque et. al., 1997) (Palanque and Schyn, 2003)	A method is proposed with related tools and techniques to engineer the design and development of usable user interfaces. This method uses Petri Net to formally model the system behaviour.
	(Reeder and Maxion, 2006)	This work is not only lists several criteria for detecting the user hesitation but also defines a method that can be automated for detecting instances of user difficulty based on identifying hesitations during system use.
	(Fields et. al., 2000)	A method is presented for evaluating and comparing design options (task performance, analysis of user deviations and consequent hazards, and coordination) for allocating communication media in an interactive safety-critical system.
	(Connely et. al., 2001)	Extend and evaluate existing pattern

		language for safety-critical user interface development.
	(Paternò et. al., 2005)	A method to help designers to identify and derive interfaces that support users in their activities.
	(Pap and Petri, 2001)	The design patterns of user interface for safety-critical systems is presented for helping the reuse as much proven solutions and structures as possible.
Socio-technical	(Filipe et. al., 2003)	The timed knowledge approach is presented showing enhancements the ability to model, design and analyse procedures in socio-technical systems.
	(Gurr and Hardstone, 2001)	The potential of diagrammatic representations of the knowledge of system users and designers is shown during the implementation process, in order to support communication between the two groups.

Table 2.1 also shows that most of these works have practical contributions directed to the design phase of safety-critical system development. There is still a lack of contributions for supporting the other phases of safety-critical system development.

Methods for developing requirement analysis applicable to critical systems are still rare in literature. Are the existing requirements analysis techniques adequate for critical systems? According to Johnson (2003), the requirement analysis is also a known problem for developing a critical system. One of the reasons of misunderstandings among stakeholders is the vocabulary used. In critical systems, this problem is a fundamental one. A common ground understanding among software developers, HCI experts and the domain stakeholders, regarding the ontology for the field seems to be still missing.

The impact of usability regarding emergency situations in critical applications deserves deeper analysis. The disturbance caused by emergency alarms may affect the user's mental model causing more mistakes and slips in interaction with the system. In socio-technical systems such as an Air Traffic Control system, this problem may be more complex because it involves the consideration of much more interaction factors.

To have a big picture of the contributions so far and to analyse the gaps still remaining in the field we situate them in the Semiotic Onion, which is described in the next section.

2.3 A Step Beyond HCI: The Semiotic Onion

The contributions listed in Table 2.1 can be understood from a global view of information systems by using Organizational Semiotics (Liu, 2000; Stamper, 1973) artefacts. OS (Organizational Semiotics) understands that any organized behaviour is governed by a system of social norms which are communicated through signs. The "Semiotic Onion" represents any information system including the critical ones, as situated in a Society, in which several entities cause direct or indirect influences in the automated artefact. In the informal system level, there is a sub-culture where meanings are established, intentions are understood, beliefs are formed and commitments with responsibilities are made, altered and discharged. At a formal system level (this term is more generic when compared to the same term used in Software Engineering. Formal system level includes, but is not limited to the formal methods), form and rule replace meaning and intention and finally, in technical level, part of the formal system is automated by a computer-based system. The informal level embodies the formal that, by its turn, embodies the technical level, meaning that changes in any level have impact in the other levels.

Using this model to distribute the previously discussed works, we can have another view of the impact of the contributions. Figure 2.1 illustrates that the contributions so far are mostly situated in the formal layer, with methods, processes and patterns related to the formal aspects of developing critical systems. Not much was found regarding the informal systems layer. Johnson (2003) acknowledges the needs of a safety culture within an organization for contributing to safety improvement. If people are not aware of the importance of safety, it will be difficult to apply any formal method related to safety. Studies related to informal information systems may bring important contributions for safety-critical systems in general through improvements in their interaction design.

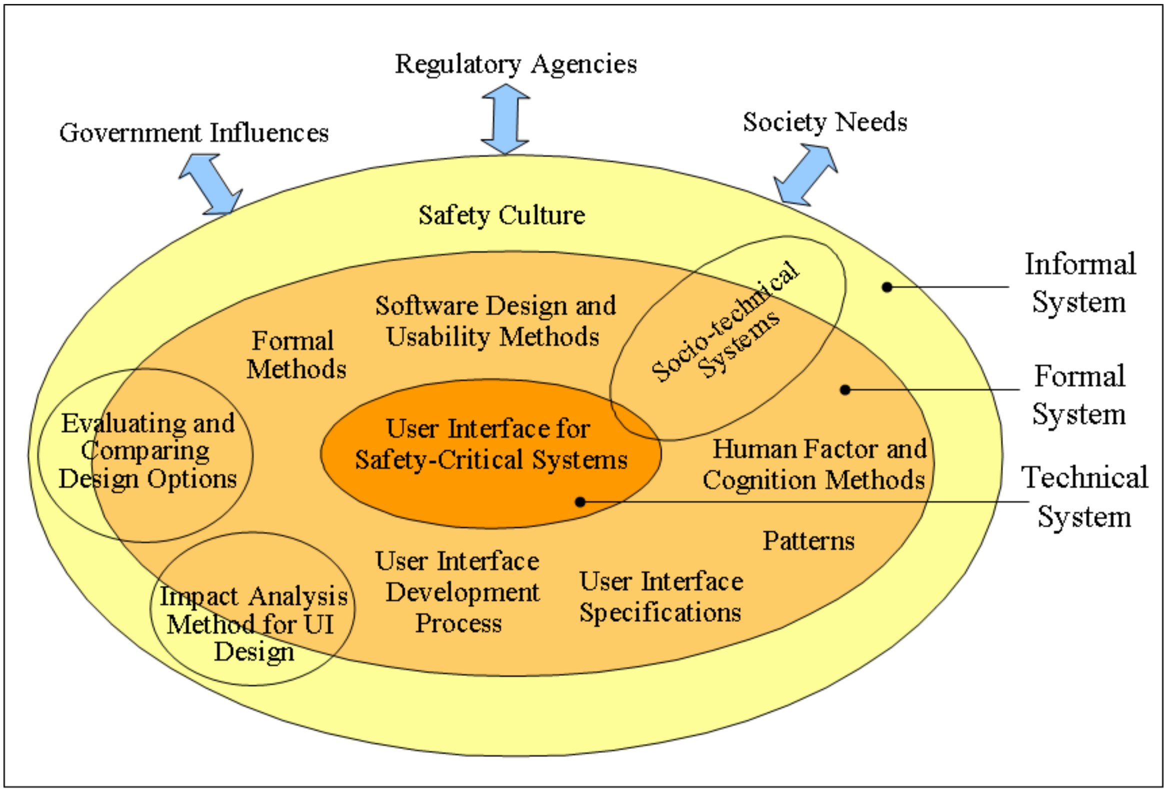

Regulatory Agencies
Government Influences
Society Needs
Safety Culture
Informal System
Software Design and Usability Methods
Formal Methods
Socio-technical Systems
Formal System
Evaluating and Comparing Design Options
User Interface for Safety-Critical Systems
Human Factor and Cognition Methods
Technical System
Patterns
User Interface Development Process
User Interface Specifications
Impact Analysis Method for UI Design

Figure 2.1: The "onion" model instantiated

Based on the theoretical model of OS we are now investigating the use of norms as a basis for generating a user interface in compliance with specific safety situations. Two kinds of norms are being proposed: generic and specific ones. Generic norms would be useful for generating abstract user interfaces which can be "tailored" to accommodate specific situations in concrete user interfaces.

The norms shouldn't be restricted to norms related to safety and dependability such as: availability, reliability, integrity, confidentiality and maintainability, but must encompass the informal layer of the critical system specific context.

This norm approach may contribute to norm-oriented design patterns. It can be useful for designing interfaces in conformance to norms defined by government, regulatory agencies or defined by experienced designers that usually are based on successful cases.

One of the challenges to the field of critical systems involves providing methods to construct a meaningful understanding of the organizational context of safety-critical systems. Artefacts and methods to cross the frontiers between the informal, formal and technical layers of the semiotic onion would benefit both HCI and Software Engineering specialists. The investigation domain must be wide and a framework is still necessary to deal with the influence of the organizational aspects of social nature in the definition of critical system requirements for designing a smooth user-system interaction.

2.4 Conclusion

This paper presented a literature survey regarding design for critical systems and identified three main classes of contributions: a class related to human factors and cognitive approaches, a class related to software design in general and usability in particular, and a class related to socio-technical approaches. The first class focuses on the human in isolation, especially for analyzing human cognition in critical situations that lead to error.

Considering the software design as a whole, there are some efforts towards the identification of problems in earlier steps of the software development process. The contributions mostly propose specifying formally the user interface as a way of avoiding future misunderstandings of developers.

Contributions focusing on the socio-technical aspects of critical situations focus on analyses to discover the cause of problems in the socio-technical context, in which groups of people interact with the artefact.

Summarizing, theories of interaction design still have a contribution to make regarding quality improvement of critical systems user interfaces. Further work involves analyzing the potential of other theories to capture the informal social system implications on design; methods and artefacts for sharing problem understanding in the safety-critical application domain, especially during requirement analysis.

Capítulo 3

A Communication-based Approach to Requirements Elicitation for Safety-Critical Systems

3.1 Introduction

Currently, we have experienced a growing demand on hardware and software systems to support the work on critical areas that used to be managed mostly by human beings. The concept of a critical system has been discussed by several authors, involving from conceptual to technical issues. In general terms, critical systems are software-based systems whose failure would provoke catastrophic or unacceptable consequences for human life. Moreover, the cost of developing a critical system is less than the potential cost of the system fault (Palanque et. al., 1998).

Literature on critical systems has shown several cases of human-system communication that resulted in people's deaths. Therac-25 is a typical case: an X-ray used to obtain bone images (through x-ray emission) or to treat tumours (through radiation emission). This was a sad case in which radiation emission caused the death of many people during a long time, due to a misunderstanding of obscure messages such as "Malfunction 54". Felciano (1997) and Mackie and Sommerville (2000) mention that this error message had no meaning for the operators, who just ignored it. However, from the perspective of the software developer, the message was intended to inform the diagnostician that the radiation dose exceeded the safety margin. Due to this communication problem reflected in the user interface, the result of this episode was disastrous leading to several patient deaths due to radiation exposure. Tragically the consequence of that communication problem was not immediately obvious; it took several years for the problem to be identified.

In this paper, we define an incident as an unexpected event that may or may nor lead to accidents or deaths. In aviation systems, many incidents have reasons originated from failures during user-system interaction. Harrison (2004b) provides some statistics: from 34 total incidents, 1100 computer-related accidental deaths occurred from 1979 to 1982; 4% of the deaths due to physical causes; 3% of the deaths due to software error; 92% of the deaths due to problems related to human-computer interaction failures. According to the Air Traffic Control (ATC), 90% of the air traffic incidents occur due to fault attributed to pilots or controllers. These reports show us the role a reliable user interface (better human-computer interaction) has in enabling the correct use of critical artefacts and supporting decision making mainly during emergency situations when the users are in panic. We understand that the Human-Computer Interaction (HCI)-related subjects have a role to play and responsibilities to assume in this particular domain. Another aspect that deserves consideration is the requirements analysis for critical systems: methods oriented to this type of system are still rare in literature. Are the existing requirements analysis techniques adequate for critical systems? According to Johnson (2003), the requirements analysis is a known problem in the development of a critical system. One of the reasons is the misunderstanding among stakeholders due to the vocabulary used. In critical systems, this problem is a fundamental one. A common ground understanding among software developers, HCI experts and the domain stakeholders, regarding the ontology for the field seems to be still missing.

Eliciting requirements has strong connection with communication issues because there are different persons and roles involved in the process. Moreover, a lot of communication takes place while running a critical system. Analysts need to understand how communication takes place during the work; therefore, communication is a crucial factor not only among stakeholders during the elicitation process, but while running a critical system.

The study of the signs used for communication and the rules operating upon them and upon their use form the core of the communication study. As there is no communication without a system of signs, Semiotics as a discipline concerned with the analysis of signs or the study of the functioning of sign systems may offer an appropriate foundation. Organisational Semiotics (OS) is one of the branches of Semiotics particularly related to business and organisations (Liu, 2000). The study in OS is based on the fundamental observation that all organized behaviour is made effective through the communication and interpretation of signs by people, individually or in groups. The aim of OS studies is to find new and insightful ways of analyzing, describing and explaining the structure and behaviour of organisations, including their inner workings, and the interactions with the environment and with one another.

The goal of this paper is to investigate a communication-based approach to the process of eliciting requirements for critical systems. The paper is organized as follows: Section 3.2

presents an overview of the main disciplines contributing to critical systems. Section 3.3 presents a Semiotic-informed proposal for requirements elicitation focusing on communication issues. Section 3.4, discusses a case study involving the analysis of an aircraft cockpit. Section 3.5 concludes.

3.2 Literature Findings

Several works have been proposed in literature for improving the quality of human-computer interaction in critical systems. Most of them involve the areas of human factors and cognitive theories, software design and usability, and socio-technical theories (Guimarães et. al., 2007b):

- Human Factors and Cognitive-related Theories – Papers in this field have contributed especially to our understanding of human errors and the human cognition in critical systems. The main findings in this area have been used to explain human reaction when dealing with critical situations;
- Software Design and Usability – Contributions in this field have focused on improvements in parts of the software development process that can have impact on the user interface component. Some additional or modified steps in the software development process have been proposed to improve the quality of the user interface regarding critical systems;
- Socio-Technical Approaches - Many critical systems depend on the interaction among a group of people. Socio-technical approaches have been used to understand the interaction among team members using a critical system.

The main contributions, grouped by their approaches, are summarized in Guimarães et. al. (2007b) and can be mapped with the "organizational onion": an Organizational Semiotics (OS) artefact (Liu, 2000; Stamper, 1973). The semiotic "onion" represents, metaphorically, any information system as being situated in a framework of information layers constituted by informal, formal and technical systems (Figure 3.1). Any information system, including the critical ones, is situated in a Society, in which several layers of information cause direct or indirect influences in the automated artefact. In the informal level, there is a sub-culture where meanings are established, intentions are understood, beliefs are formed and commitments with responsibilities are made, altered and discharged. At a formal system level 2, form and rule replace meaning and intention and finally, in the technical level, part of the formal system is automated by a computer-based system. The informal level

[2] This term is more generic when compared to the same term used in Software Engineering. Formal system level includes, but is not limited to the formal methods.

embodies the formal that, by its turn, embodies the technical level, meaning that changes in any level have impact on the other levels.

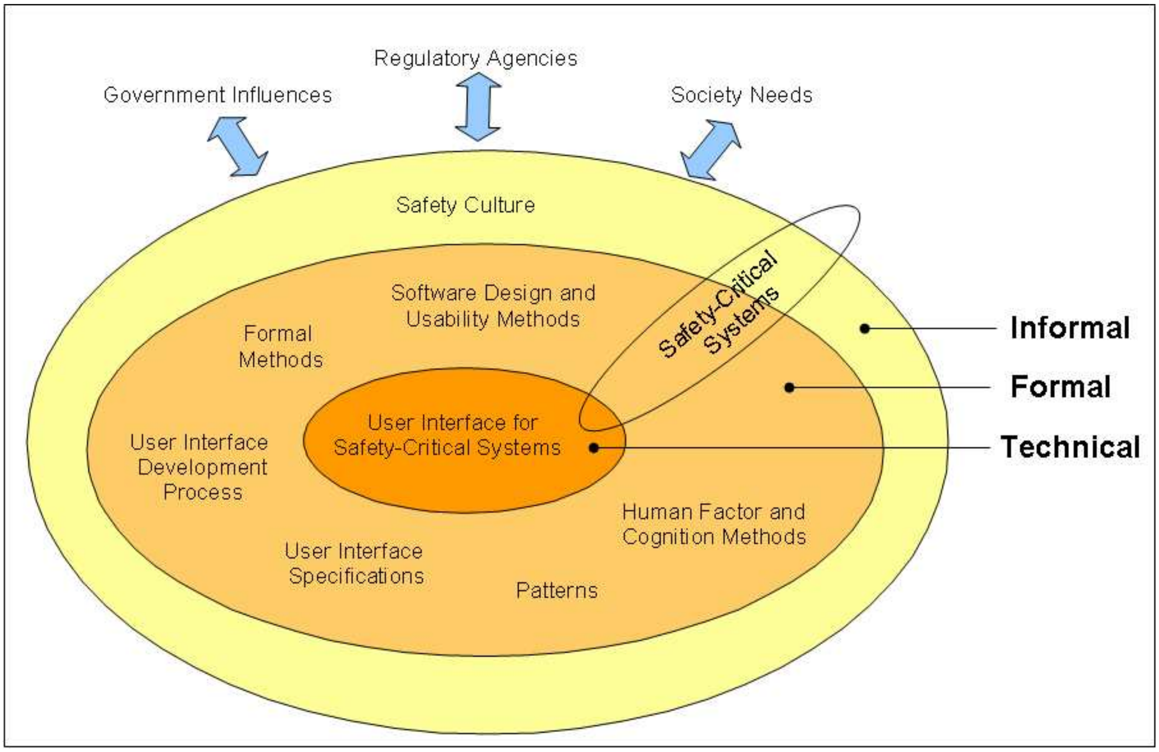

Regulatory Agencies
Government Influences
Society Needs
Safety Culture
Software Design and Usability Methods
Formal Methods
Safety-Critical Systems
Informal
Formal
Technical
User Interface for Safety-Critical Systems
User Interface Development Process
Human Factor and Cognition Methods
User Interface Specifications
Patterns

Figure 3.1: The "onion" model instantiated

Figure 3.1 illustrates that literature in the field so far are mostly situated in the formal layer, with methods, processes and patterns related to the formal aspects of developing critical systems. Not much was found regarding the informal systems layer. Johnson (2003) acknowledges the needs of a safety culture within an organization for contributing to safety improvement. If people are not aware of safety, it will be difficult to apply any formal method related to safety. Studies related to informal information systems may bring important contributions for safety-critical systems in general through improvements in their interaction design.

Communication is a subject present in the three layers of information fields: informal, formal and technical. Filipe et. al (2003) have discussed communication motivated by a real case - an air collision of two aircrafts which may have been caused by failure in communication. This paper draws on the use of Semiotics (Liu, 2000) to focus on the communication aspects involved during the requirements elicitation. The proposed approach aims at guiding the analysts in eliciting requirements regarding communication and its possible failures. This may help them to get information about what a system should do if a specific communication fails.

The requirements elicitation is part of the requirements analysis (Nuseibeh and Easterbrook, 2000). Information gathered during requirements elicitation has often to be interpreted, analyzed, modelled and validated before the requirements engineer can feel confident that a complete set of requirements of a system have been collected. Therefore, requirements elicitation is closely related to other Requirements Engineering activities and the elicitation technique used is usually driven by the choice of a modelling scheme, and vice versa: many modelling schemes imply the use of particular kinds of elicitation techniques.

While Contextual Design (Baker et. al., 2004) may be useful for eliciting requirements related to communication among the team which will develop the system and the group of users, the approach proposed in this work aims at eliciting communication requirements for a situation of a critical system usage. As discussed by Liu (2000) the study of the signs used in communication and the rules operating upon them and upon their usage constitute the core of the study on communication. There is no communication without a system of signs. Semiotics considered as a discipline concerns the analysis of signs or the study of the functioning of sign systems. Organisational Semiotics (OS), one of the branches of Semiotics particularly related to business and organizations, provides the foundations for our proposal.

3.3 Background

OS methods can provide a better understanding for the interested parts of a focal problem, their requirements, as well as the restrictions not only regarding the information system, but the software system as well (Bonacin et. al., 2006).

Our approach considers some of the MEASUR (Methods for Eliciting, Analysing and Specifying Users' Requirements) methods, combined with other artefacts to capture aspects of communication requirements.

3.3.1 MEASUR Methods

Eliciting communication-related requirements can be accomplished by following two basic steps: identifying the agents that participate in the communication among all interested parts and modelling the communication among them. Semiotics provides good instruments to analyze these aspects.

MEASUR, which resulted from a Stamper's research work in the late 70´s (Stamper, 1993), constitutes a set of methods to deal with all aspects of information system design: the use of signs, their function in communicating meanings and intentions, and their social consequences. The Problem Articulation Method (PAM) consists of a set of methods to be applied to the initial phase of a project, when the problem definition is still vague and complex. The methods and artefacts we are using for identification of the agents involved in communication through channels are based on the Stakeholder Analysis, the Evaluation Framing, the Semiotic Diagnosis and Norm Analysis.

Stakeholder Analysis: allows to investigate all the interested parts (the stakeholders), that direct or indirectly have influences or interest in the information system in analysis. In the stakeholders analysis all interested parts are categorized in different groups: Operation, Actors/Responsible, Clients/Providers, Partners/Competitors and Spectators /Legislators.

Evaluation Framing: is an extension of the Stakeholder analysis, which allows identifying, for each stakeholder category, their interests, questions and problems, in order to discuss possible solutions.

Semiotic Diagnosis: traditional system development methodologies emphasize technical issues (physical world, empirics and syntactic) and the analyst misses the opportunity of analyzing other levels of relationship (semantic, pragmatic and social), which direct or indirectly affect the aspects of the system design.

The Semiotic Ladder (SL) is an artefact of the Semiotic Diagnosis (Liu, 2000; Stamper, 1973) primarily used to clarify some important Information System notions such as information, meaning and communication (Cordeiro and Felipe, 2004). Stamper (1973) extended the traditional semiotic divisions of syntactic, semantics and pragmatics by adding three other: social world, physical world and empirics as depicted in Figure 3.2, which, all together, form the SL.

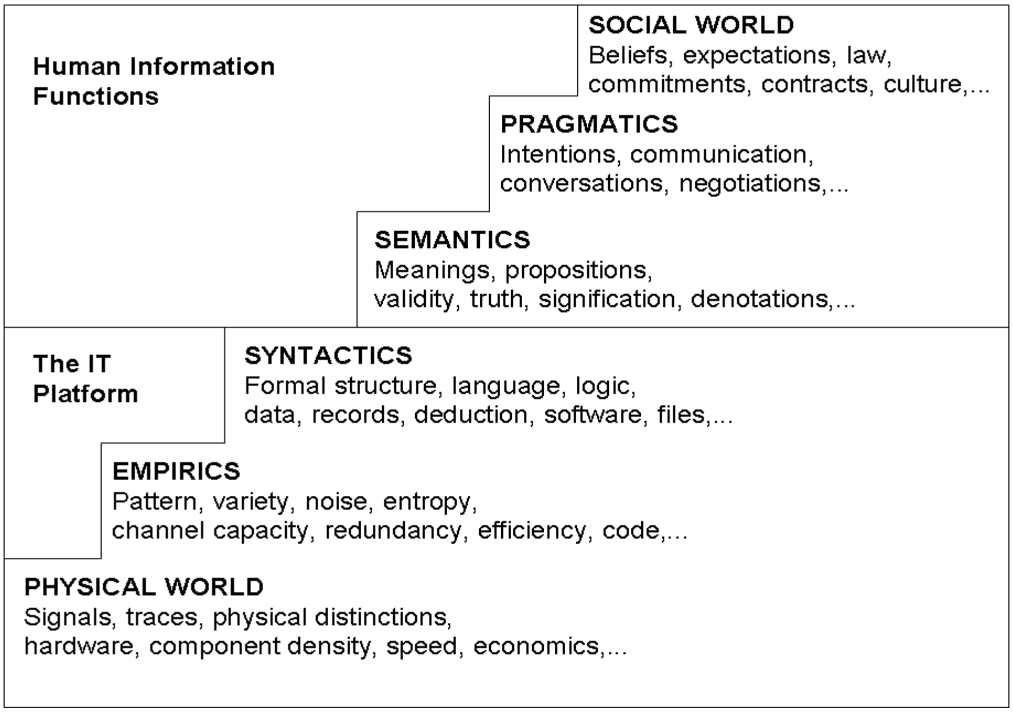

Human Information Functions
SOCIAL WORLD
Beliefs, expectations, law, commitments, contracts, culture,...
PRAGMATICS
Intentions, communication, conversations, negotiations,...
SEMANTICS
Meanings, propositions, validity, truth, signification, denotations,...
The IT Platform
SYNTACTICS
Formal structure, language, logic, data, records, deduction, software, files,...
EMPIRICS
Pattern, variety, noise, entropy, channel capacity, redundancy, efficiency, code,...
PHYSICAL WORLD
Signals, traces, physical distinctions, hardware, component density, speed, economics,...

Figure 3.2. Semiotic Framework adapted from Stamper (1973)

The six steps of the SL provide different views for analysis of different aspects of signs. The Physical World deals with the physical aspects of signs. In communication, for example, there are some physical signs for communication such as those transported by cable or radio waves. The Empirics level deals with the statistical properties of signs such as channel capacity, patterns, efficiency. In the Syntactic level, there are signs and their relations to other signs forming a structure, language, data and records. The Semantics deals with signs and their relations to mean that users perceive. In the Pragmatics level, the signs and their effect on users are gathered, identified. Finally, in the Social World, the signs and their relation to social implications are considered. If there is a failure in the Semantics level, it means that the problem is not originated from the technical information system, but it is related to human information function. It means that the source of the problem may be originated from human interpretation. Therefore, the SL may link Human Factors and Social Science issues. We argue that the Semiotic Ladder can help the requirements analysts to understand different levels of communication.

In a critical system context, an artefact that may be one of the most crucial is the Evaluation Framing. The list of questions and problems with correspondent solutions would ideally lead to an expressive amount of problems that might happen.

Norm Analysis: within MEASUR, the Norm Analysis Method (NAM) focuses on the social, cultural and organizational norms that govern the actions of agents in the business domain. A norm, in the formal and informal sense, defines the responsibility of an agent involved in a task or conditions under which a certain action can (should or should not) be executed by the agent. The norm describes the pattern of behaviour expected in the system. For example, the safety procedures could be understood in terms of norms. If something wrong happens, then certain procedures should be applied. Some system constraints could also be defined by using NAM.

In the context of critical systems, the norms would be very robust because there are several norms defined by governmental agencies, for example: (Federal Aviation Administration (FAA). The norms involve several aspects such as safety, symbols, piloting patterns resulted from previous experiences, occurred disasters and incidents. The human-artefacts interaction component should have additional norms based on good practices captured by experienced workers or organizations.

3.3.2 Modelling communication

Communication has been studied from different points of view, with associated models (Baranauskas et. al., 2002). The "process" school sees communication as the transmission of messages. It is concerned with how senders and receivers encode and decode information and how the transmitters use channels as media for communication, with efficiency and accuracy. The semiotic school understands communication as the production and sharing of meaning (Baranauskas et. al., 2002). It is concerned with how messages interact with people in order to produce meanings. It does not consider misunderstanding to be necessarily evidence of communication failure, as they may result from the cultural differences between the parts involved in communication.

To understand the semiotic view of communication, Salles et. al. (2000) exemplify the concept in the process of software design showing a Fractal Model of Communication (FMC) to capture the structure of the communication process involved in the whole process of software design. It stresses the fact that, in order to design the primary message (the system's interface), other fractionated messages must be carefully designed and appropriate channels must be chosen to convey them.

The FMC models agents in communication through channels. A communicant agent shares information with other agents through channels. Figure 3.3 represents this concept of communication in which, in one level, agents B and C communicate through channel A. In another level, A assumes the role of an agent in communication with C through channel AC.

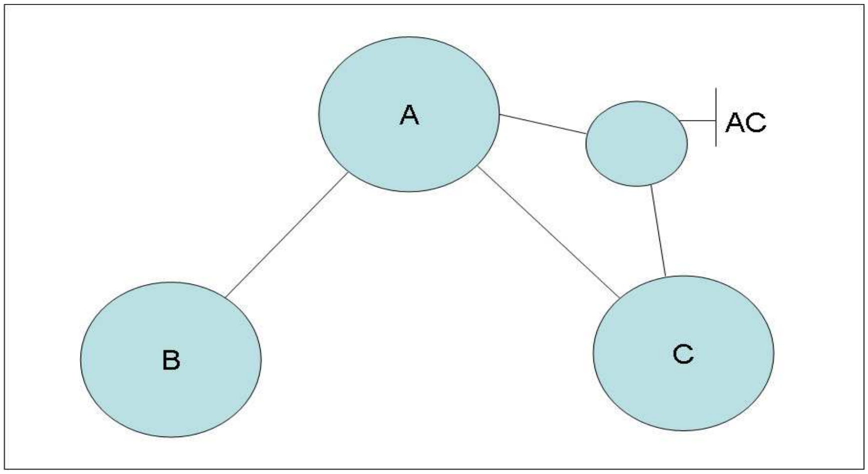


Figure 3.3: Fractal Model of Communication

We argue that a Fractal Model of Communication is appropriate for representing the communication aspect in critical systems. This model makes explicit important information about the agents and all the media used in their communication; it allows capturing potential communication failures and to provide redundancy that would be extremely useful for designing the interaction for critical systems.

3.3.3 Articulating MEASUR Artefacts with the Fractal Model of Communication

In order to elicit requirements related to communication we articulate contributions of some MEASUR methods with the Fractal Model of Communication. Results of the MEASUR methods are input to FMC, as Figure 3.4 illustrates. In the proposed model, four artefacts are used for eliciting requirements related to communication regarding the system under consideration: the Stakeholder Analysis, the Evaluation Framing, the Semiotic Diagnosis and Norm Analysis. The artefacts feed the FMC in representing communication in several fractal dimensions.

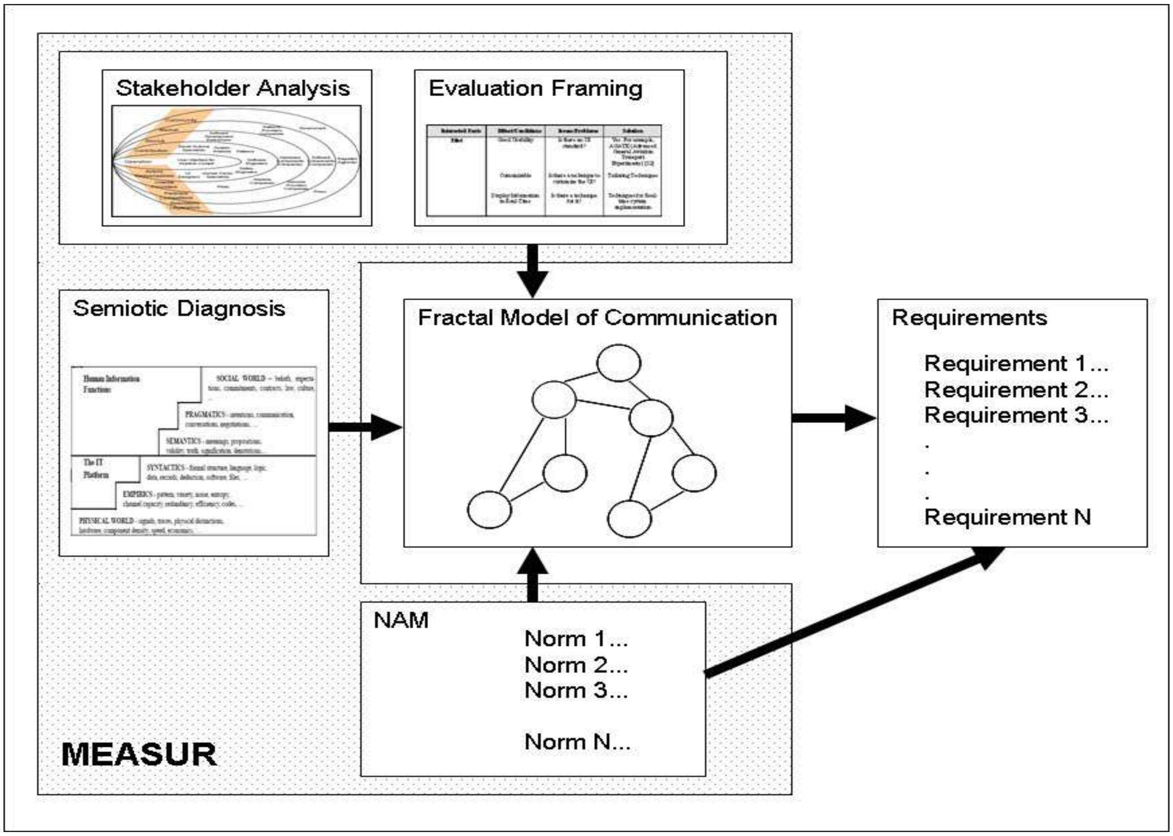

Stakeholder Analysis
Evaluation Framing
Semiotic Diagnosis
Human Information Functions
SOCIAL WORLD – beliefs, expectations, commitments, contracts, law, culture, ...
PRAGMATICS - intentions, communication, conversations, negotiations, ...
SEMANTICS - meanings, propositions, validity, truth, signification, denotations, ...
The IT Platform
SYNTACTICS - formal structure, language, logic, data, records, deduction, software, files, ...
EMPIRICS - pattern, variety, noise, entropy, channel capacity, redundancy, efficiency, codes, ...
PHYSICAL WORLD - signals, traces, physical distinctions, hardware, component density, speed, economics, ...
Fractal Model of Communication
Requirements
Requirement 1...
Requirement 2...
Requirement 3...
.
.
.
Requirement N
NAM
Norm 1...
Norm 2...
Norm 3...
Norm N...
MEASUR

Figure 3.4: Proposed model for eliciting communication requirements

The first step in the communication requirements elicitation involves the identification of the stakeholders that are people or organizations affected by the system under consideration. The identified stakeholders are categorized according to the groups defined by the stakeholder analysis practice.

The Evaluation Framing raises several questions related to the stakeholders and enables consideration of possible solutions that are important for critical systems. As illustrated in Figure 3.5, stakeholders range from the technical people to community-related people. Therefore, the questions raised in the Evaluation Framing reflect the multidisciplinary nature of the problem. It is especially important for critical systems because several possibilities of faults are discussed and solutions are proposed. The alternative solutions for a problem may be crucial for critical systems. For example, it is common practice to provide redundant component(s) to cope with fails.

The Semiotic Diagnosis allows an inspection of the channels used in communication, considering from the physical to the social ones.

Norms represent the behaviour of some involved agents and channels contributing to the identification of new agents/channels in other dimensions of the FMC. The Norm Analysis Method (NAM) in this model refers to the analysis of norms related to communication.

In safety-critical systems, it is the best practice to use redundant communication because any channel may fail. Therefore, some channel else is used only if another channel fails. NAM can be used to specify the behavioural part of communication. Therefore, in the proposed model, two important sources for generating requirements related to communication are the FMC and the set of norms. The FMC represents the static structure of communication and the norms the dynamic behaviour of communication.

In the next section, a case study illustrates the information that this model can represent regarding communication aspects of a critical system under design.

3.4 An Aircraft Cockpit Design: a Case Study

This case study illustrates a communication-based approach for eliciting requirements for the user interface of an aircraft cockpit.

A cockpit is the place in civil aircrafts where pilot and co-pilot are located with the instruments that provide information about air pressure, speed, altitude, oil pressure, navigation information, communication resources as well as information about engines, flaps, gears, rudder and other artefacts used during the aircraft flight.

Basically, in the aircraft, there are two groups of people: (1) the crew, composed by pilot, co-pilot and flight attendants and (2) the passengers. All aircrafts must have, at least, one radio for communication with the controllers who are located at the ground. The ATC (Air Traffic Control) people use the radio to communicate with pilots/co-pilots and telephones to communicate with other people at ground. The RADAR (Radio Detection and Ranging) system provides a two dimensional representation of an aircraft moving along pre-defined routes within an air sector, while paper flight strips allow controllers to track and modify information about aircraft and their flight plans. More details about this system can be found in Hopkin (1995). Certainly this scenario constitutes a safety-critical system. A communication failure may lead to a fatal accident. A communication failure between the pilot and the air traffic controller may lead to the collision of aircrafts with no survivors.

3.4.1 Instantiating the PAM artefacts

Considering as a target the user interface for critical systems, the resulting model of stakeholder analysis is shown in Figure 3.5.

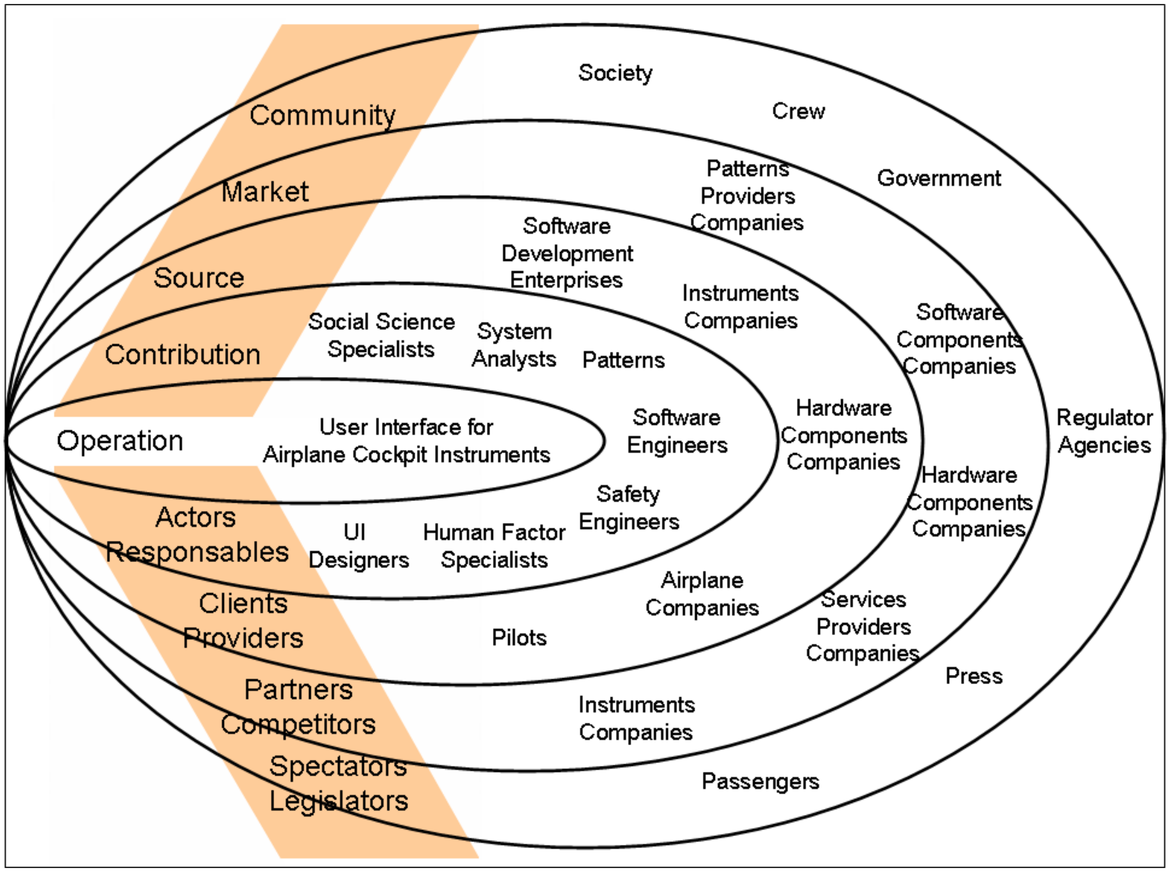


Figure 3.5: Model of Stakeholder Analysis

The stakeholder analysis shows some stakeholders categorized in groups related to several knowledge and responsibility areas ranging from the technical to the community-related ones. Table 3.1 illustrates the Evaluation Framing for the "Pilots" category of stakeholders.

Table 3.1: The Evaluation Framing instantiated for the Pilots

Stakeholder	Effect/ Conditions	Issues/ Problems	Solution
Pilot	Good Usability	Is there an UI standard?	Yes. For example, AGATE (Advanced General Aviation Transport Experiments) (SATS, 2007)

	Customizable	Is there a technique to customize the UI?	Tailoring Techniques
	Display Information in Real-Time	Is there a technique for it?	Techniques for Real-time system implementation

The Semiotic Diagnosis method uses the Semiotic Ladder (SL) to get information regarding communication of the aircraft cockpit. With this framework, the eliciting analyst tries to answer questions centred on communication aspects for each stakeholder. Table 3.2 illustrates the SL used to analyze the cockpit sign "Instruments".

Table 3.2: Questions related to Instruments

Semiotic Framework Layer	Questions	Involved Areas
Physical World	What are the signal, traces, physical distinctions, speed and component density of the Instruments?	Electronic engineering, software engineering, user interface design, safety engineering
Empirics	What are the pattern, noises, channel capacity used for this communication between Aircraft and Instruments and between Instruments and Pilot?	Electronic engineering, software engineering, user interface design, safety engineering
Syntactic	What are the structure, used languages, logic, data, records, deductions, software, files of these Instruments?	Electronic engineering, software engineering, user interface design, safety engineering
Semantics	What are the meanings, validity, denotations and propositions of the Instruments?	User interface design, software engineering, regulatory agency norms, safety engineering

Pragmatic	What are the intentions, in terms of communication of these Instruments?	Press, project management, risk assessment project
Social World	What are the belief, expectations, culture, commitments, contracts, law regarding the Instruments and its development?	Safety culture, law, regulatory agency, contracts, juridical activities

Table 3.2 shows each layer of the Semiotic Framework and the correspondent example of questions raised. The third column shows that these questions demand a multidisciplinary approach helping to articulate discussions in several topics.

3.4.2 Defining the Dynamics of Communication

While the FMC model represents communication in a static way, norms represent the behaviour of the agents in communication. In our case study, when the pilot requests authorization from ATC and the aircraft is ready for taking off, the aircraft can take off only if ATC authorizes this action. This is an example of communication between two agents: the pilot and the controller, whose behaviour is governed by norms. The media in this case (channel) is the radio. The norm for his example is depicted in Figure 3.6.

When an aircraft is prepared to take off

then the Pilot

is obliged to ask permission to ATC and wait for the authorization to execute the taking off procedure

Figure 3.6: An instantiated norm

This norm shows that the taking off procedure enters in action when the aircraft is ready for taking off and the pilot has the authorization for taking off. The “Radio” is used as a channel for this communication.

3.4.3 Modelling Communication Elements

Each agent communicates by sharing messages with other agent. Figure 3.7 shows part of Fractal Model of Communication applied to our case study. Some examples of agents and channels modelled are passengers, pilot/co-pilot, sensors, crew, voice, speech, instruments, ATC, radio, noises and vibrations. Data link was raised by questioning about alternative communication if the radio fails; it represents a communication channel between Instruments and ATC. The complete FMC model is huge because there are several levels of communication ranging from the social context to the lower level, when we consider the physical devices. Nevertheless, the FMC representation allows us to zoom in and out depending on the fractal dimension one wants to examine.

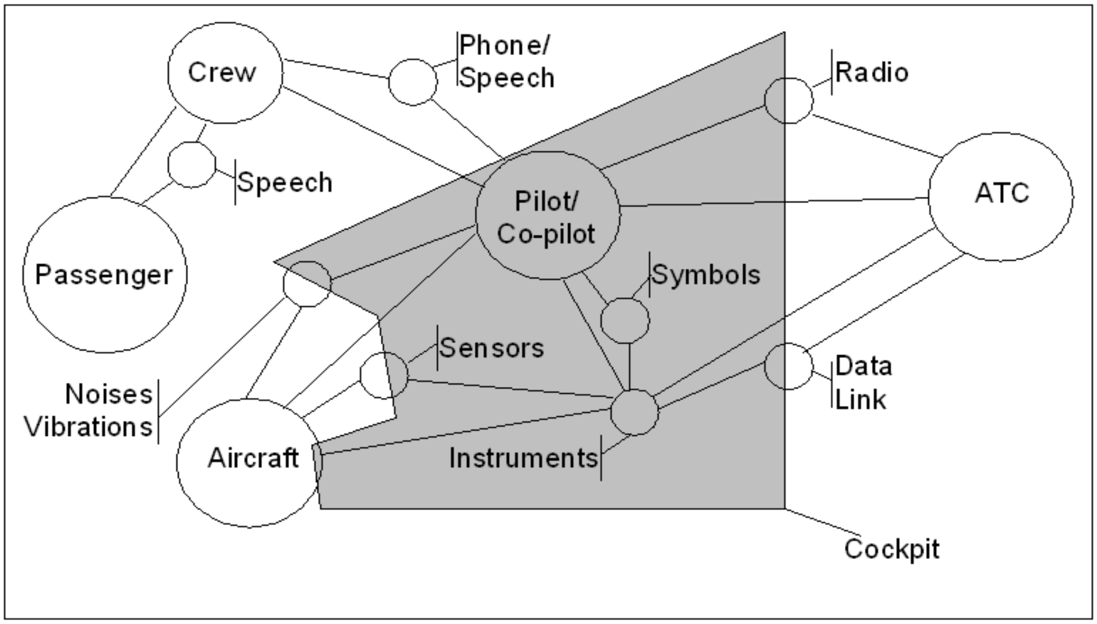


Figure 3.7: Fractal model of communication for an aircraft cockpit

Figure 3.7 shows that “Instruments” is a communication channel between Pilot/Co-pilot and Sensors. At the same time, “Instruments” is an agent communicating to Pilots and co-Pilots through Symbols that should make sense for pilots and co-pilots. For example, the external temperature is measured by a sensor and indicated through this instrument. The pilot interprets this symbol and understands that the temperature is high or normal or low thanks to his knowledge about aviation. If the temperature is high, for example, he/she could use the radio for communicating to ATC requesting the nearest airport to land because of the problem suggested by the temperature indication.

Several standards of communication in aviation can be retrieved from aeronautical agencies such as FAA, the American regulatory agency that has norms for air traffic control, navigation, piloting aircrafts, flight operations (landing, taxing, taking off) and several other norms such as safety procedures, information signs in airports (e.g. runways markings, runway lightings) etc.

The document of requirements related to communication can be elaborated based on the FMC and the norms list. While the norms express information related to safety procedures, standards of user interface for the instruments, quality related requirements etc, the FMC models communication based on agents and channels (human, hardware and software) and their internal and external interactions.

The norms and the FMC “inform” the specification of communication-related requirements, as Figure 3.4 suggests. An example of a communication requirement based on the norms related to the communication between the agents Pilot/co-pilot and ATC can be defined as illustrated by Figure 3.8.

> *Elements in the system’s user interface should be provided so that the Pilot/Co-pilot is obliged to ask permission from ATC and wait for that permission before starting the taking off procedure. A* radio channel *may be used for that communication. The user interface should prevent and notify the Pilot/Co-pilot from taking off without that explicit permission.*

Figure 3.8: Example of communication requirement

The communication requirement has part of sentence extracted from the norm complemented with communication-related details extracted from FMC model indicated using italics.

3.5 Conclusion

Current literature has shown that requirements elicitation have not paid the due attention to the communication aspects involved in the information system domain. This paper investigates some methods and techniques for eliciting requirements related to communication aspects, an essential issue in safety critical systems.

Several methods from MEASUR such as PAM, NAM, and the Fractal Model of Communication (FMC) together provided to be useful guidance for eliciting requirements of communication for critical systems. The proposed approach represents a potential contribution for safety-critical systems as it guides the analyst to get requirements with scenarios which consider what a system should do if a specific communication fails. This approach helps to anticipate different communication failures in several levels. Further work is being conducted towards the formal integration between MEASUR and FMC.

Recent studies indicate considerations regarding, for example the design of Personal Air Vehicles (PAV) (Cafe, 2007) that could be piloted by a person with no rigorous trainings because the piloting complexity will be assisted by a critical system. PAV will demand better methods for eliciting requirements which will impact the human-artefact interaction.

Capítulo 4

Communication-based Modelling and Inspection in Critical Systems

4.1 Introduction

Safety-critical systems are systems whose failure would provoke injury or death to human beings (Palanque, 1998). The term incident is defined as unexpected events that may or may not lead to accidents or deaths (Johnson, 2003). In aviation systems, many incidents have reasons originated from failures during communication mediated by the user interface artefacts as some statistics of the problems in the avionics domain show: from 34 total incidents, 1100 computer-related accidental deaths occurred from 1979 to 1982; 4% of the deaths due to physical causes; 3% of the deaths due to software error; 92% of the deaths due to problems related to human-computer interaction failures (Harrison, 2004b). According to the Air Traffic Control (ATC), 90% of the air traffic incidents occur due to fault attributed to pilots or controllers. These reports show us the role a reliable user interface has in providing a better human-computer interaction enabling the correct use of critical artefacts and supporting decision making mainly during emergency situations.

Some significant evolution regarding the user interfaces in cockpits of aircrafts has happened recently. The flight decks (or cockpits) today utilize multifunction computer displays – where huge amounts of information are stored and the pilot navigates through layers and layers to find the required information (Carver and Turoff, 2007). He/she thus becomes more a system engineer than a pilot. This modern cockpit, named “glass cockpit”, represents information using graphical elements through diagrams and symbols. The automated systems may produce conflicting data from different sources and they will force decisions about which information to act upon (Carver and Turoff, 2007).

The concept behind the Personal Air Vehicle (PAV) represents a new generation of small aircraft that can extend personal air travel to a much larger segment of the population. PAV must provide simplified operation akin to driving a car. Although several tasks will be executed by the automation system because users are persons not supposed to be trained in pilot's course, others will be allocated for humans. Within this scenario, the future of aviation is being discussed by the CAFE Foundation (Cafe, 2007) and the National Aeronautics and Space Administration (Young and Quon, 2006). There are several research sectors specialized in technologies related to PAV such as flight instructors systems (Allen, 2007), synthetic vision information system (Schnell et. al., 2002; Glaab et. al., 2003) and distributed decision-making (Rong et. al., 2005).

As cockpits have evolved technically, there are demands for new fundamentals, theoretical and methodological backgrounds that contribute on understanding the interaction and communication issues between human and machine.

We understand that the Human-Computer Interaction (HCI) field has a role to play and responsibilities to assume in this particular domain. HCI is a field of study concerned with human and machine in communication. It draws on knowledge on both the machine and the human sides. On the machine side, computer graphics, operating systems, programming languages, and development environments are relevant disciplines. For the human side, communication theory, graphic and industrial design, linguistics, social sciences, cognitive psychology, and ergonomics are important disciplines. Moreover, engineering and design methods are naturally relevant (Hewett et al., 2007).

The concepts of communication and interaction are sometimes blurred in the HCI context. Communication has been studied from different points of view, with associated models. The semiotic school understands communication as the production and sharing of meaning (Baranauskas et. al., 2002). Therefore, in the context of this work, we understand "communication" as implying code (anything that has a meaning for something or someone) sharing among systems. Regarding human and computer systems, they can communicate by interacting through icons, windows, progress bar, buttons and other user interface elements.

To our knowledge, literature on user interface analysis in the domain being considered has not paid special attention to communication issues. This work presents an exploratory approach for analysing the user interface of safety-critical systems regarding communication aspects. The proposed approach is applied to the analysis of the Synthetic Vision Systems (SVS) display that is one of the user interaction technologies required by PAV aircrafts.

The paper is organized as follows: Section 4.2 presents the theoretical background which serves as foundations for the proposed analysis. Section 4.3 applies the approach to an exploratory study of a PAV cockpit. Section 4.4 presents conclusions and points to further work.

4.2 Theoretical and Methodological Background

The theoretical and methodological background considered in this work is Semiotics that consists on the study of the signs that are used for communication. The rules operating upon them and upon their use form the core of the communication study. As there is no communication without a system of signs, Semiotics as a discipline concerned with the analysis of signs or the study of the functioning of sign systems may offer an appropriate foundation.

Organisational Semiotics (OS) is one of the branches of Semiotics particularly related to business and organisations (Liu, 2000). OS understands that any organized behaviour is governed by a system of social norms which are communicated through signs. Methods for Eliciting, Analysing and Specifying Users' Requirements (MEASUR), resulted from a Stamper's research work in the late 70´s (Stamper, 1993), constitutes a set of methods to deal with all aspects of information system design: the use of signs, their function in communicating meanings and intentions, and their social consequences. The relevant methods for the specific scope of this work are described as follows:

- The Stakeholder Analysis allows all the interested parts (stakeholders) to be investigated that directly or indirectly have influences or interests in the information system under analysis. In the stakeholders analysis all interested parts are categorized in several groups whose context covers all the organization.

- The Evaluation Framing is an extension of the Stakeholder Analysis, which allows identifying, for each stakeholder category, their questions and problems, in order to discuss possible solutions.

- The Semiotic Ladder (SL) is an artefact primarily used to clarify some important Information System notions such as information, meaning and communication (Cordeiro and Filipe, 2004). Stamper (1973) extended the traditional semiotic divisions of syntactic, semantics and pragmatics by adding three other layers: social world, physical world and empirics as depicted in Figure 4.1, which, all together, form the SL.

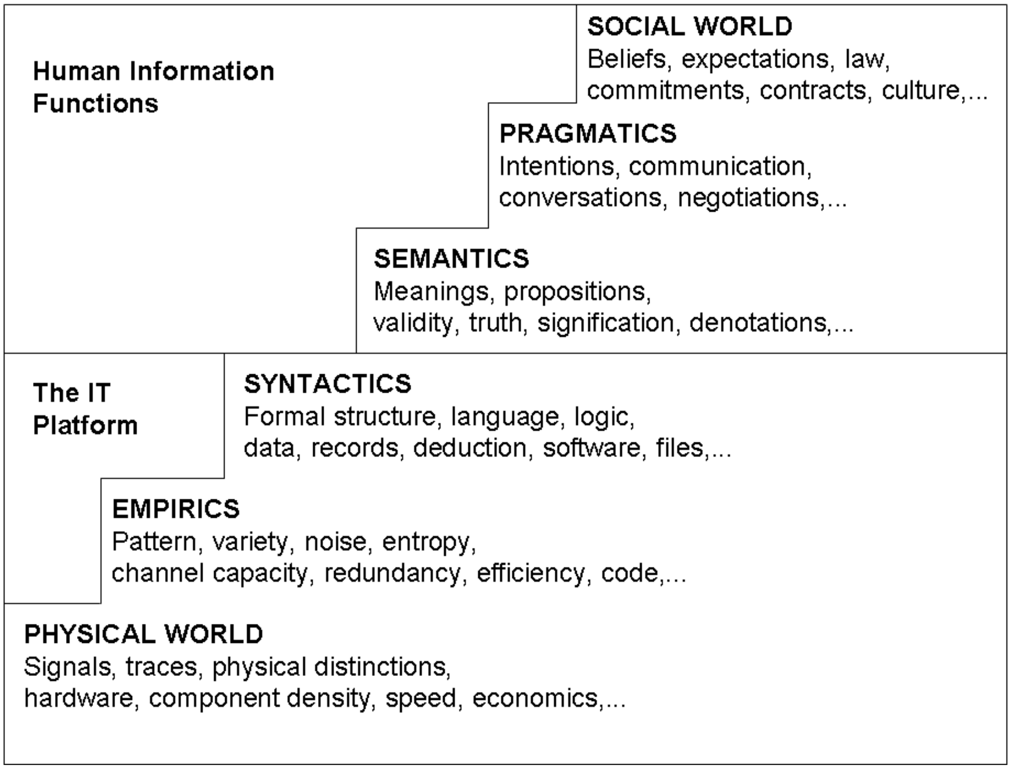

SOCIAL WORLD
Beliefs, expectations, law,
commitments, contracts, culture,...
Human Information
Functions
PRAGMATICS
Intentions, communication,
conversations, negotiations,...
SEMANTICS
Meanings, propositions,
validity, truth, signification, denotations,...
The IT
Platform
SYNTACTICS
Formal structure, language, logic,
data, records, deduction, software, files,...
EMPIRICS
Pattern, variety, noise, entropy,
channel capacity, redundancy, efficiency, code,...
PHYSICAL WORLD
Signals, traces, physical distinctions,
hardware, component density, speed, economics,...

Figure 4.1: Semiotic Ladder, adapted from Stamper (1973)

A communication is considered successful only if all these six levels of the SL are successfully accomplished. The communication in upper levels depends on the result of the communication on lower levels. The Physical World deals with the physical aspects of signs such as cable or radio waves. The Empirics level deals with the statistical properties of signs such as channel capacity, patterns, efficiency. In the Syntactic level, there are signs and their relations to other signs forming a structure, language, data and records. The Semantics deals with signs and their relations to meaning that users perceive. In the Pragmatics level, the signs and their effect on users are identified. Finally, in the Social World, the signs and their relation to social implications are considered. If there is a failure in the Semantics level, it means that it is related to the human information function. Therefore, the SL may link human factors and social issues focusing on different levels of communication.

The Fractal Model of Communication (FMC) (Salles et al., 2001; Salles, 2000) captures the structure of the communication process involved in the application domain. The FMC models agents in communication through channels. A communicant agent shares information with other agents through channels. Figure 4.2 represents this concept of communication in which, in one level (or one fractal dimension), agents B and C communicate through channel A. In another level, A assumes the role of an agent in communication with C through channel AC.

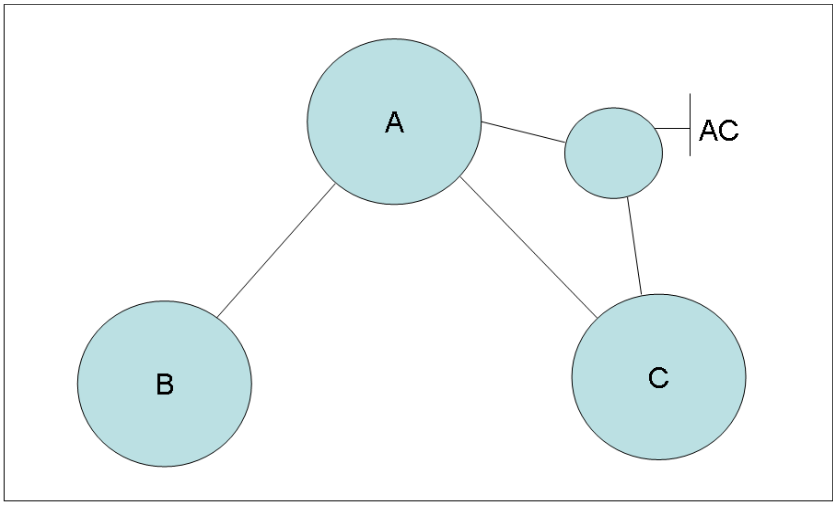


Figure 4.2: The Fractal Model of Communication (Salles, 2000)

The artefacts of Stakeholder Analysis and Evaluation Framing can be developed during the requirements analysis (Guimarães et. al., 2007a). These artefacts can be reused for modelling and inspection using artefacts of Stakeholder Analysis and the Evaluation Framing for defining agents and channels for FMC. The communication inspection is accomplished by analysing all the six levels of the SL for each channel represented in FMC model.

The FMC models communication in any fractal dimension: from the organizational context (business) to a small pixel in the screen (user interface elements). For example, if the context of requirements is relative to the user interface, then the FMC should have a channel representing the user interface. If the requirements refer to a specific interaction object, the channel regarding the user interface should be exploded reaching to lower fractal dimension to have specific channel regarding this interaction object. Therefore, the FMC should be adjusted according to the requirements contexts.

The presented artefacts can be articulated for modelling and inspecting the communication as proposed in this work. Figure 4.3 illustrates it.

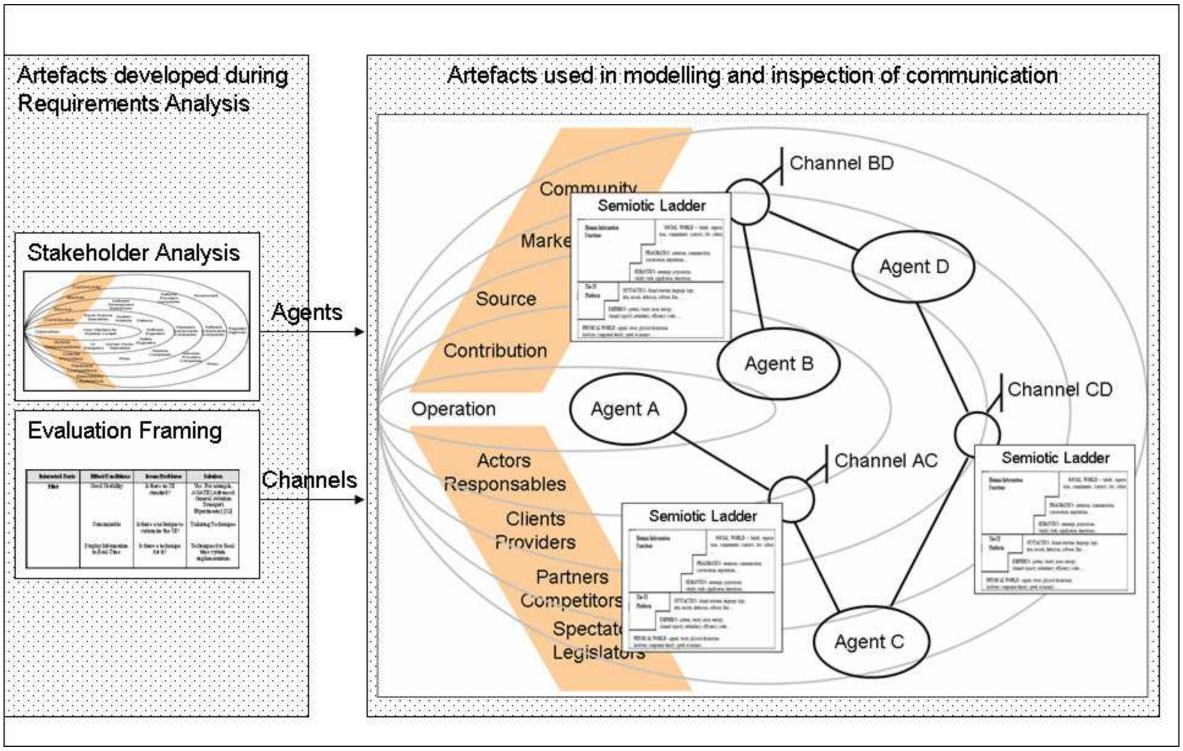


Figure 4.3: Modelling and inspecting communication

The inspection is conducted by verifying all levels of the SL in all FMC channels. Examples of questions defined for each SL level are listed in Table 4.1.

Table 4.1: Questions for the six levels of the Semiotic Ladder

Layer	Question
Physical world	How is communication being accomplished regarding physical aspects (signals, traces, physical distinctions, hardware component, etc)?
Empirics	What are the empirical characteristics (pattern, capacity, speed, noise) of this communication?
Syntactic	How is communication being accomplished in syntactic terms (language, formal structure, files, software)?
Semantics	How is communication being accomplished regarding semantics (Meanings, propositions, validity, truth, signification, denotations)?
Pragmatics	How is communication being accomplished regarding pragmatics aspects (Intentions, communication, conversations, and negotiations)?

Social world	How is communication being accomplished in social terms (Beliefs, expectations, law, commitments, contracts, culture)?

The SL allows exploring each communication channel with a wide coverage. The physical, empirics and syntactic levels focus on information technology and the levels of semantics, pragmatics and social world focus on the human context.

In the next section, these modelling and inspection techniques will be applied in a case study related to the PAV context.

4.3 Modelling and Inspecting a PAV Display

This section presents the modelling and inspection for the SVS display, one of the technologies proposed for human-vehicle interaction for PAV, based on outcomes from the analysis of the problem domain carried out using the OS methods (Guimarães et. al., 2007a). Due to the specificity for SVS Display, in this section the FMC is adapted for the context of this display.

Literature proposes several elements for the user interface of SVS displays including symbolic, textual and graphical representations. Not all SVS displays are designed for PAV. Although Domino (2006) proposed a user interface layout for a SVS display without mentioning whether it was designed for PAV or not, it provides a SVS display layout. The horizon (composed by sky and terrain) is presented as 3D objects; all obstacles (fog, clouds and darkness) are removed as this display provides a synthetic view, i.e. data related to visualization is obtained from a database and not from the real world. It provides information (represented as Indicator) regarding current altitude (represented as Tape), current speed (as Tape), pathway display elements and other information that can help the user to get a situational awareness. This SVS display will be analysed regarding communication aspects considering the PAV context. Figure 4.4 depicts the FMC in a fractal dimension representing display SVS proposed by Domino with more specific agents and channels. There is no limit for the number of fractal dimensions allowing any detail degree when necessary.

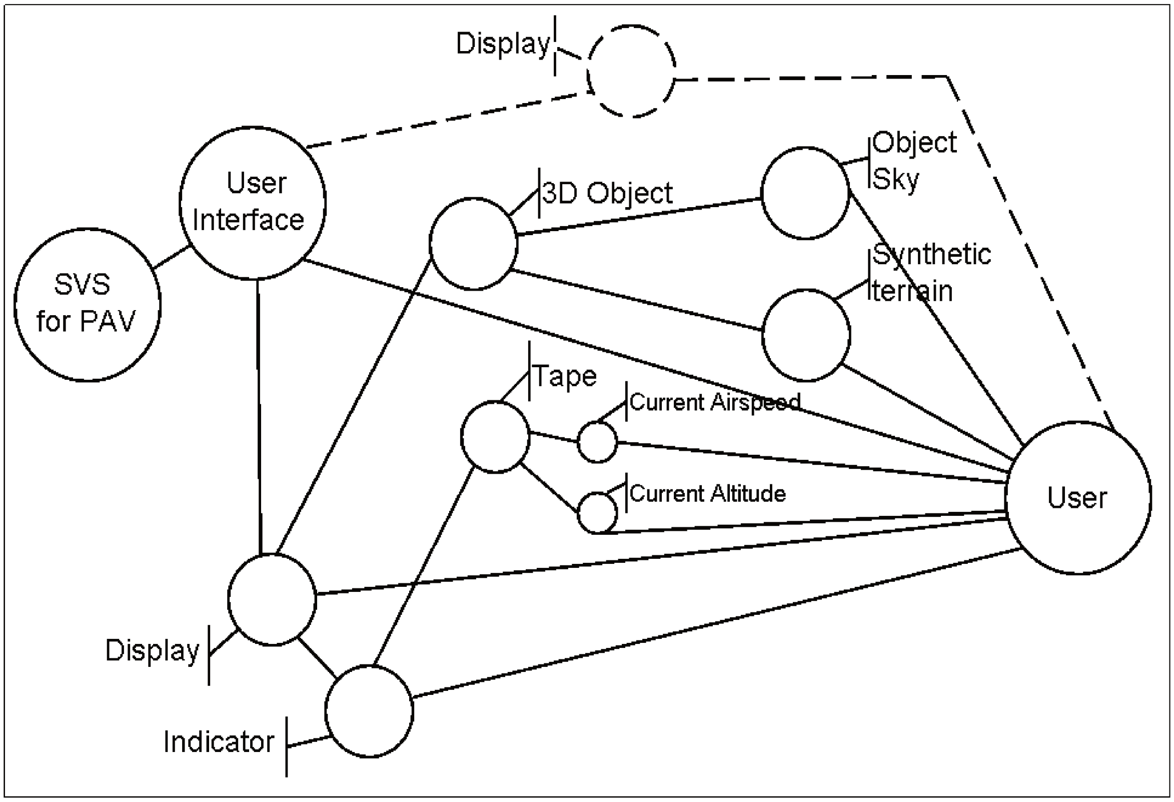


Figure 4.4: Modelling SVS display using FMC

In interactive systems, the FMC represents the communication between two agents (the display and the user) through a channel called user interface acting as communication media. One important concept related to modelling in safety-critical systems is redundancy. For example, aircraft with redundant displays is a typical configuration. We model redundancy in FMC by using dashed connections and dashed circles as Figure 4.4 depicts.

This communication related inspection technique consists on answering questions listed in Table 4.1 for all channels represented in FMC and in all fractal dimensions for obtaining a complete view. The answers should be easy to understand explaining how the communication is accomplished in each layer of SL. In this case study, we have the answers regarding the channel Tape presented in the Table 4.2.

Table 4.2: Answers of SL for channel Tape

Layer	Answer
Physical world	Tape consists on several colored pixels
Empirics	The tape may show any range of values depending on the context (altitude, speed).

Syntactic	The rectangle is presented with scale of values and a current value pointed by a triangle.
Semantics	This object is well known by pilots which means that there is a current value with specific range and scale.
Pragmatics	This object represents for pilots the current value with scale information.
Social world	Providing better situation awareness, the pilots feel safe during the flight.

The analysis of the SVS Display proposed by Domino based on the Table 4.2, shows that the communication channels through tapes seem adequate for pilots. In the case of PAV, the users are not only the pilots but people without intensive training. Therefore, this artefact may not be sufficient for PAV.

The artefacts (Stakeholders Analysis, FMC and SL) allow rich information related to communication with wide coverage. The organization can be prepared for most of communication failures studying alternative ways if a communication fails. The alternative ways can be obtained focusing on the FMC to identify the redundant communication channels supposing situations of each specific channel or agent is unavailable. The SL provides a more specific focus on context directed to the cause of communication failure for each channel. This list of possible communication failures and respective ways for treating failures also contribute to improvements in communication. Consequently, it leads to improvements in the quality of the technical product.

4.4 Conclusion

Communication is a critical factor to be addressed in safety-critical systems, especially in the avionics and aviation domain. Semiotics as a discipline focused on communication may provide a good foundation to inform the modelling and inspection of communication in these systems. This paper proposed using artefacts of Organizational Semiotics allied to a framework for modelling communication: the Fractal Model of Communication (FMC). The approach was illustrated with the modelling and inspection of communication regarding a SVS display of Personal Air Vehicles.

The FMC represents agents and channels of communication with unlimited fractal dimensions. In this way, the communication model can be presented in overview and with detailed information of each channel, with the six layers of communication of the Semiotic Ladder. FMC and Semiotic Ladder provide support for inspecting a communication system (e.g. the user interface) helping to detect problems related to communication. This technique allows seeing the connection between the organizational view and the user interface contexts. The overall communication quality depends on the quality of communication in each channel. Nevertheless, the FMC may grow in complexity presenting many agents and channels making the reading difficult. Some visualization tools may allow the presentation of the FMC model with a configurable filter to allow visualizing each fractal dimension separately, zooming in and out to show only the agents and channels needed for a specific consideration.

As an extension of the communication-based modelling, some adjustments of this technique could inform the system development for improving the quality of the communication among agents in the organization. Moreover, part of this communication based modelling upon FMC may be automated by a tool. This tool would be valuable for defining redundancy points, obtaining alternative ways (channels and agents) to maintain communication.

Capítulo 5

A Case Study on Modelling the Communication Structure of Critical Systems

5.1 Introduction

A safety-critical system is defined as “a computer, electronic or electromechanical system whose failure may cause injury or death to human beings” (Palanque et. al., 1998). In terms of cost, safety-critical systems may be defined as “a system whose design cost is much smaller than the potential cost of a system failure” (Palanque et. al., 1998). The term incident, very frequent in this domain, is defined as unexpected events that may or may not lead to accidents or deaths (Johnson, 2003). In aviation systems, many incidents have reasons originated from failures during communication mediated by the user interface artefacts as some statistics of the problems in the avionics domain show: from 34 total incidents occurred from 1979 to 1982; 4% of the deaths were due to physical causes; 3% were due to software error; 92% were due to problems related to human-computer interaction failures (Harrison, 2004b). According to the Air Traffic Control (ATC), 90% of the air traffic incidents occur due to faults attributed to pilots or controllers. These reports show us the role a reliable user interface has in providing better human-computer interaction enabling the correct use of critical artefacts and supporting decision making mainly during emergency situations.

The experiences on the airplane cockpits have led to research that has contributed to the understanding of the attributes of automation and how it affects tasks, as well as situational awareness which is commonly understood to be a critical aspect in managing complexity. Carver and Turoff (2007) mention that the flight decks (or cockpits) utilize nowadays multifunction computer displays – where huge amounts of information are stored and the pilot navigates through layers and layers of information to find the required information. He/she thus becomes more a system engineer than a pilot. This modern cockpit, named "glass cockpit", represents information using graphical elements through diagrams and symbols. Carver and Turoff (2007) also mention that the automated systems may produce conflicting information from different sources and they will force decisions about which information to act upon. Understanding the impact of automation on the human and how tasks should be allocated between human and machine have been a key area of HCI research in safety-critical systems.

While this technical evolution happens, the future of aviation is being discussed by the CAFE Foundation (Cafe, 2007) and the National Aeronautics and Space Administration (Young and Quon, 2006). PAV is a new generation of small aircrafts that can extend personal air travel to a much larger segment of the population (Cafe, 2007). Near all-weather Short Take-Off and Landing (STOL) PAV will be able to transport people to their destination at speeds three to four times faster than airlines or cars. PAV will provide very robust automation systems with decisions regarding the distribution of tasks between the human and the vehicle. Several tasks will be executed by the automation system because users are persons not supposed to be trained in pilot course. Although the PAV automated system will be prepared for executing most tasks, some will be allocated to humans. One of the "enabling technologies" related to the human-vehicle interaction is Synthetic Vision Systems (SVS) (Cafe, 2007). One of the impediments to the wide-spread adoption of small aircraft for on-demand travel is its inability to fly in low-visibility conditions. Synthetic vision systems that match the aircraft's GPS position speed and altitude to a terrain database can overcome this problem. SVS presents the pilot with a moving, ego-centric 3D view of the world even when flying in total fog.

Guimarães et. al. (2007b) mention that there are few contributions regarding the informal aspects related to safety-critical systems. The informal aspect involves a sub-culture where meanings are established, intentions are understood, beliefs are formed and commitments with responsibilities are made, altered and discharged. There are also demands that ask for better communication systems due to technical evolution experienced by the regular aircrafts industry with impact on the pilot-avionic system communication.

We understand that the Human-Computer Interaction (HCI) field has a role to play and responsibilities to assume in this particular domain. HCI is a field of study concerned with the communication between human and machine. It draws on knowledge of both the machine and the human sides. On the machine side, computer graphics, operating systems, programming languages, and development environments are relevant disciplines. For the human side, communication theory, graphic and industrial design, linguistics, social sciences, cognitive psychology, and ergonomics are important disciplines. Moreover, engineering and design methods are naturally relevant (Hewett et. al., 2007).

This work aims at shading light on methodological artefacts for modelling safety-critical systems focusing on communication. The concepts of communication and interaction are sometimes blurred in the HCI context. Communication has been studied from different points of view, with associated models (Baranauskas et. al., 2002). The "process" school sees communication as the transmission of messages. It is concerned with how senders and receivers encode and decode information and how the transmitters use channels as media for communication, with efficiency and accuracy. The semiotic school understands communication as the production and sharing of meaning (Baranauskas et. al., 2002). Therefore, in the context of this work, we understand "communication" as implying code sharing among systems through channels.

In this paper we carry on a case study in which a semiotic-based structuring of communication is made considering the user interaction within a PAV.

As communication issues are fundamental factors in safety-critical systems, this work presents an approach for building a detailed view of communication, its agents and channels, in a critical system. The proposed approach is instantiated in the PAV context. The paper is organized as follows: Section 2 presents the theoretical and methodological background which serves as foundations for the proposed approach. Section 3 instantiates it in an exploratory study of a PAV cockpit. Section 4 concludes and points out to further work.

5.2 Theoretical and Methodological Backgrounds

The study of the signs and the rules operating upon them and upon their use composes the core of the communication study. As there is no communication without a system of signs, Semiotics, as a discipline concerned with the analysis of signs or the study of the functioning of sign systems, may offer an appropriate foundation.

Organisational Semiotics (OS) is one of the branches of Semiotics particularly related to business and organisations (Liu, 2000). OS understands that any organized behaviour is governed by a system of social norms which are communicated through signs. OS methods can provide a better understanding of the interested parties of a focal problem, their requirements, as well as the restrictions regarding the information system and the software system as well (Bonacin et. al., 2006). Methods for Eliciting, Analysing and Specifying Users' Requirements (MEASUR), resulted from a Stamper's research work in the late 70´s (Stamper, 1993), constitute a set of methods to deal with all aspects of information system design: the use of signs, their function in communicating meanings and intentions, and their social consequences. The relevant methods for the specific scope of this work are Stakeholder Analysis, the Evaluation Framing, and the Semiotic Ladder, described as follows:

(i) The Stakeholder Analysis (Liu, 2001) allows all the interested parties that directly or indirectly have influences or interests in the information system under analysis to be investigated. In the stakeholders analysis all interested parties are categorized into different groups: Operation, Actors/Responsible, Clients/Providers, Partners/Competitors and Spectators /Legislators.

(ii) The Evaluation Framing (Baranauskas et. al., 2005) is an extension of the Stakeholder Analysis, which allows identifying, for each stakeholder category, their questions and problems, in order to discuss possible solutions.

(iii) The Semiotic Ladder (SL) is an artefact primarily used to clarify some important Information System notions such as information, meaning and communication (Cordeiro and Felipe, 2004). Stamper (1973) extended the traditional semiotic divisions of syntactic, semantics and pragmatics by adding three other layers: social world, physical world and empirics, which, all together, form the SL.

A communication is considered successful only if all these six levels of the SL are successfully accomplished. The communication in upper levels depends on the result of the communication on lower levels. These levels provide different views for analysis of different aspects of signs. The SL layers are described as follows:

(i) Physical World - deals with the physical aspects of signs. In communication, for example, there are some physical signs such as those transported by cable or radio waves.

(ii) Empirics - deals with the statistical properties of signs such as channel capacity, patterns, efficiency.

(iii) Syntactic – deals with signs and their relations to other signs forming a structure, language, data and records.

(iv) Semantics - deals with signs and their relations to meaning, propositions, validity, truth, denotations that users perceive.

(v) Pragmatics – deals with signs and their effect on users.

(vi) Social World – deals with signs and their relation to social implications.

The Semiotic Ladder focuses on different levels of communication linking human factors to both the physical and the social worlds.

To capture the structure of the communication process we use the Fractal Model of Communication (FMC) (Salles et. al., 2001; Salles, 2000). The FMC stresses the fact that, in order to design the primary message (the system interface), other fractionated messages must be carefully designed and appropriate channels must be chosen to convey them. The FMC models agents in communication through channels. A communicant agent shares information with other agents through channels. Figure 5.1a represents this structure of communication in which, in one level, agents B and C communicate through channel A. In another level, A assumes the role of an agent in communication with C through channel AC.

The FMC is appropriate for critical systems as it makes explicit important information about the agents and all the media used in their communication. It allows capturing potential communication failures and to provide redundancy that would be extremely useful for designing the interaction in critical systems.

The integration of the OS artefacts to the FMC, necessary for the dynamics of eliciting requirements and modelling communication, as previously discussed in Guimarães et. al. (2007a) and Guimarães et. al. (2008). All needed artefacts are listed in Guimarães et. al. (2007a). The artefacts of Stakeholder Analysis and the Evaluation Framing help to define agents and channels for FMC.

The SL allows exploring each communication channel with a wide coverage. The layers physical world, empirics and syntactic focus on information technology and the layers semantics, pragmatics and social world focus on the human context. In the SL, there is already information about "how" to accomplish the communication.

The FMC model is considered as input for the design of the communication aspect of critical systems.

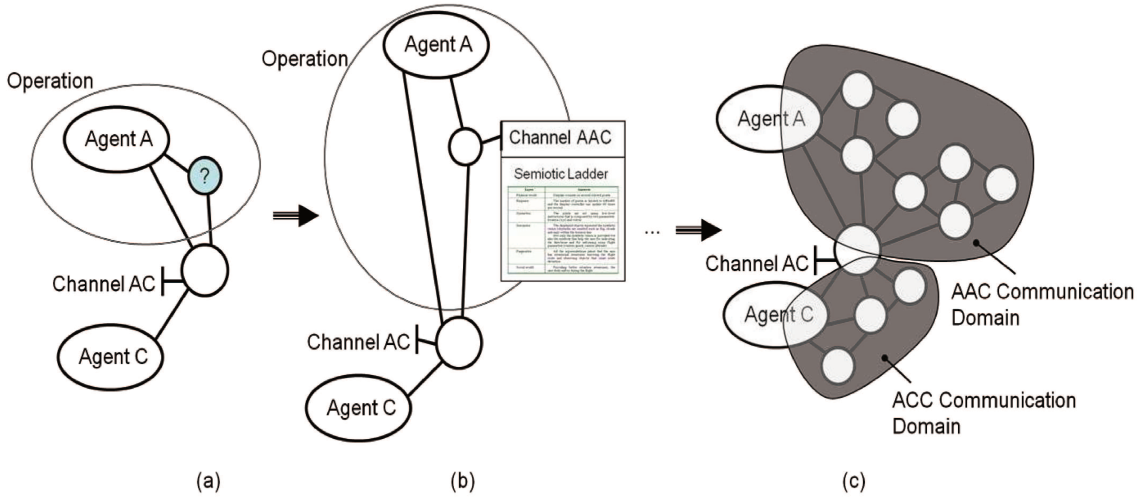


Figure 5.1: Channels Instantiated

The instantiation starts by considering the stakeholders in the group "Operation" given by the PAM artefact. They are instantiated to obtain smaller granularities of the FMC and SL. Therefore, the result of the instantiation is the expanded group as Figure 5.1b depicts.

Figure 5.1 illustrates an iteration of the instantiation process. Figure 5.1a shows the FMC with one agent "Agent A" inside the "Operation" group. To instantiate the context between Agent A and channel AC, the channel needs to be identified answering the following question: "Who is intermediating Agent A and Channel AC?" The answer to this question identifies the channel that should be considered. The next step involves defining the correspondent SL for these new channels with information about how to accomplish this communication. Figure 5.1b represents the generic structure after inserting new channel AAC with correspondent SLs. The next iteration of the instantiation process is repeated questioning the new channels indicated by "?". Therefore, the instantiation procedure is repeated for obtaining the expanded group of "Operation" and the result consists on a more detailed (fine-grained) view of the communication inside this group.

The instantiation process is executed repeatedly with several iterations starting with two agents. The resulting set of channels originated by a pair of agents can be denominated as the domain of these agents. Figure 5.1c represents two domains: AAC and ACC.
The Domain represents the context of communication between two originated agents or channels. In the case of Figure 5.1c, all agents and channels inside the domain AAC are in the context of the communication between the Agent A and channel AC because they are the instantiation results with some number of iterations originated from agent A and channel AC. In the other example, the ACC communication domain refers to the context of communication between Agent C and channel AC.

The next section presents an overview of applying the instantiation process to the PAV case study.

5.3 A Case Study with PAV

This section presents the modelling of the communication structure for PAV based on the outcome from the analysis of the problem domain carried out using the OS methods (Guimarães et. al., 2007a).

5.3.1 Stakeholder Analysis for PAV

Based on PAV literature, several stakeholders were identified and categorized using the Stakeholder Analysis model for the PAV cockpit. The Stakeholder Analysis shows some stakeholders categorized into groups related to several knowledge and responsibility areas ranging from the technical to the community-related ones. For each stakeholder, an Evaluation Frame is filled with information regarding conditions or effects, problems they may have, proposed solutions and the resources needed for the solution. The stakeholders PAV and the User are considered as agents and the Evaluation Frame has information about the channel between these agents i.e., SVS Canvas. The Evaluation Framing contains one additional column, differently from Guimarães et. al. (2007a), named Resource that will help to define the channels needed between the agents. This column has information about what resources are needed by the stakeholder for finding out or executing the solution. Table 5.1 shows only the columns Problem, Solution and Resource listing the resources used by the stakeholder User. For example, the resources Display, User Interface and Canvas are channels for the user communication to the PAV system.

Table 5.1: Evaluation Framing for the User Stakeholder

Problem	Solution	Resource
PAV is not easy to use	Use HCI-related guidelines	Display, User Interface, Canvas
PAV is not safe	Use safety-related guidelines	Society legislation
PAV is not affordable	Study how to provide low cost development and manufacturing.	Market prices

5.3.2 The PAV Communication Structure

In the PAV Stakeholder Analysis model, the category Operation has four agents: SVS, PAV, Automation Instrument and Status. The agent SVS represents the whole SVS Display system; the PAV demands requirements focusing on the target system PAV as a whole; the Automation Instrument represents all automation systems which have displays for the user interaction, and Status consists on information about the status related to vehicle statuses such as fuel level, temperature, maintenance data and so on. Figure 5.2 illustrates part of the FMC instantiated for PAV representing these four agents with new channels and agents.

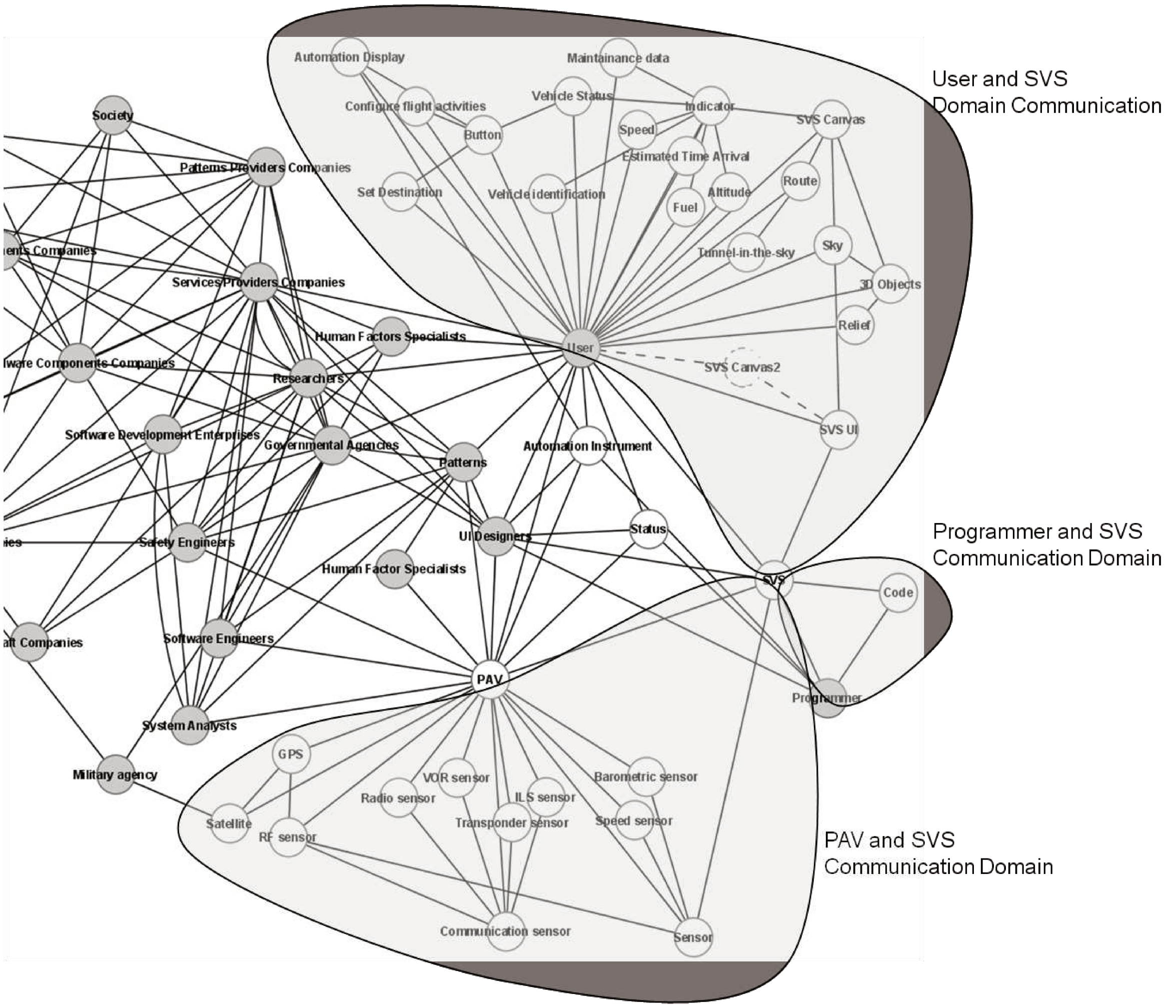


Figure 5.2: The FMC instantiated for PAV

The agent User belongs to the Contribution group; all greyed nodes represent agents which belong to the Stakeholder Analysis model, the white nodes (SVS, Automation Instrument, Status and PAV) represent agents and channels which belong to the group Operation of the Analysis Stakeholder model and all the nodes placed inside of the communication domain regions are new agents and channels generated after executing the instantiation procedure.

Basically, Figure 5.2 shows the FMC as a graph in which the nodes are agents and channels and the edges represent the communication between these nodes. After instantiation execution, the resulting model has three communication domains. The first domain is in the context of communication of agent User and SVS agents of group Operation in the Stakeholder Analysis artefact. The second communication domain is the communication between PAV and SVS both belonging to the group Operation. In some cases, after executing the instantiation procedure, new agents and channels may connect to other agents because of the necessity of communication with other stakeholder groups. For example, the agent Military Agency (in category Legislator of Stakeholder Analysis model) has connection to channel Satellite. The third represented domain has only one iteration of instantiation identifying the channel Code between agents Programmer and SVS. Therefore, the instantiation procedure can provide several iterations representing the number of fractal dimensions (granularity degree) of the FMC model. Therefore, the definition of what domain to explore and which number of iterations to consider will depend on the context of the system analysis under consideration.

Figure 5.2 also shows the redundant channel SVS canvas that is represented by a dashed line. If a display is damaged, the other display is started showing the same information (the same canvas) of the former display.

The communication structure in Figure 5.2 can be detailed with SL for all channels represented in the FMC and in the fractal dimensions for obtaining a complete view. The answers should be easy to understand explaining how the communication is accomplished in each layer of SL. In this case study, we illustrate the answers regarding the channel SVS Canvas in the Table 5.2.

Table 5.2: SL for channel SVS Canvas

Layer	Question
Physical world	15” touch screen Liquid Crystal Display (LCD)
Empirics	The number of pixels is limited to 640x480 and the display controller can update 60 times per second.
Syntactic	The pixels are set using low-level instructions that are composed by two parameters: location (x,y) and colour.
Semantics	The displayed objects represent the synthetic vision (obstacles are omitted such as fog, clouds and rain) within the horizon line. The symbols help the user indicating the directions and some flight parameters (speed, altitude).
Pragmatics	All the representations intend to enable the user to have situational awareness knowing the flight route and observing objects that cause route deviation.
Social world	Providing better situation awareness, the user feels safe during the flight.

The instantiated FMC allows the critical system to be designed in the perspective of communication; the designer can think about the components regarding a specific role (or goal) related to communication. The information about the intention, reason, limitation, format, structure and either the social impact of this role is always specified due to the SL. Therefore, the SL provides information focusing on the specific context of the channel.

The FMC´s communication structure covers two views: the organizational view (stakeholder's context) and technical view (software-centred agents and channels). It means that we have the connection between the business and the technical views under the perspective of communication.

If a communication channel fails, it means that at least one SL layer had failed propagating this failure to the upper layers. There are two possible solutions for this problem:

> (i) Provide a specific mechanism to detect the problem and to handle this failure inside a layer;
>
> (ii) An agent can detect the failure of a channel, invalidate it and switch to one or more alternative ways through another communication channel represented in FMC model.

The artefacts SL and FMC can be used for analysing potential communication failures considering solutions (i) and (ii). In case of Table 5.2, one of the potential failures can be originated by the physical world layer. If a hardware component of a display fails, the designers should investigate what would the best solution for this problem. If the best solution is to use a redundant display, therefore, the option (ii) could be used.

Another point to observe is that the instantiation procedure also helps in the identification of new communication connections between the technical and the organizational world.

5.4 Conclusions

Communication is a factor to be addressed in critical systems, especially in the avionics and aviation domains. Semiotics as a discipline focused on communication may provide a good foundation to inform the modelling of communication in these systems. This paper proposed an analysis based on artefacts of Organisational Semiotics allied to a framework for designing communication: the Fractal Model of Communication (FMC). The approach was illustrated with the modelling of the communication structure for designing critical systems regarding the user interface of Personal Air Vehicles.

The FMC represents agents and channels of communication within different fractal dimensions and domains. The communication model presents an overview as well as a detailed view of each channel, with the six layers of communication of the Semiotic Ladder (SL). The FMC and the SL taken together provide support for representing the structure of communication with information regarding the physic, empirics, syntactic, semantics, pragmatics and social aspects of each channel. Therefore, this artefact allows modelling the structure of communication joining both its organisational and technical aspects. This tool is valuable for defining redundancy points, obtaining alternative ways (channels and agents) to maintain communication in a failure situation.

The presented FMC model provides strong contribution for socio-technical systems as this model and the instantiation procedure may reveal new communication connections, new solutions and challenges due to connections and dependencies between technical and organizational worlds.

Nevertheless, reading may become difficult when the model grows in complexity, presenting many agents and channels. Some visualization tools may offer the presentation of the FMC model with a configurable filter to allow visualizing each fractal dimension separately, zooming in and out to show only the agents and channels needed for a specific consideration. Moreover, part of this communication based modelling may be automated.

Capítulo 6

A Communication based Process Model in Critical Systems Design

6.1 Introduction

We have experienced a growing demand on hardware and software systems to support the work on critical areas that used to be managed mostly by human beings. The concept of a critical system has been discussed by several authors, encompassing from conceptual to technical issues. The safety-critical category of critical systems is the one whose failure would provoke catastrophic or unacceptable consequences for human life (Paulson, 1997). Recently, the ReSIST project (ReSIST, 2008) created a new field of study, Resilience Systems, which includes safety-critical systems.

Usability is considered one of the most important aspects to consider in critical systems; gaps and challenges are still being identified in the ReSIST project. Literature on critical systems has long shown dramatic cases of human-system failures that resulted in people's deaths. Therac-25 is a typical case: an X-ray used to obtain bone images (through x-ray emission) or to treat tumors (through radiation emission). The message "Malfunction 54" had no meanings for the operators, who just ignored it (Mackie and Sommerville, 2000) although, for the software developer, the message intended to inform that the radiation dosage was above normal values. Due to this human-computer communication problem reflected in the user interface, the consequence of this episode was disastrous leading to several deaths because of the extreme radiation injected to patients. More dramatically, as the effect of over dosage was not instantaneous, it took several years for the problem to be identified.

In aviation systems, many incidents (unexpected events that may or may not lead to accidents that may lead to deaths) have reasons originated from failures during user-system interaction. Harrison (2004b) shows some statistics with 34 total incidents (1979-1992); 4% of the deaths were due to physical causes; 3%, software error; 92%, problems related to human-computer interaction. According to ATC (Air Traffic Control), 90% of the air traffic incidents were consequences of faults attributed to pilots or controllers. These reports show the role that a reliable user interface (better human-computer interaction) has in enabling the correct use of critical artifacts and supporting decision making mainly during emergency situations when the users are in panic.

As discussed by Carver and Turoff (2007), one of the challenges for obtaining better human-computer interaction is the significant technical evolution that has happened regarding the cockpits of aircrafts. Nowadays, the flight decks (or cockpits) have multifunction computer displays where huge amounts of information are presented. This new concept of modern cockpit, named “glass cockpit”, provides rich amount of information using graphical elements through diagrams and symbolic information. In parallel with this evolution, sophisticated automation systems may produce conflicting data from different sources forcing decisions about which information to act upon. The pilot needs to navigate through layers and layers of information becoming more a system engineer than a pilot.

As space systems have evolved technically, there are demands for new fundamentals, theoretical and methodological backgrounds to understand the interaction and communication issues between the human and the technical system. We understand that the Human-Computer Interaction (HCI) field has a role to play and responsibilities to assume in this particular domain. HCI field of study draws on knowledge on both the machine and the human sides. On the machine side, computer graphics, operating systems, programming languages, and development environments are relevant areas. For the human side, communication theory, graphic and industrial design, linguistics, social sciences, cognitive psychology, and ergonomics are some important disciplines. Moreover, engineering and design methods are naturally relevant (Hewett et. al., 2007).

Regarding engineering and design methods, the requirement analysis is a known problem in the development of a critical system (Johnson, 2003). Communication is a crucial factor among stakeholders during the elicitation process and also in the communication among internal components of a critical system.

The study of signs and rules operating upon them and upon their use, form the core of the human communication study. As there is no communication without a system of signs, Semiotics, as a discipline concerned with the analysis of signs or the study of the functioning of sign systems, may offer an appropriate foundation for this study. Organizational Semiotics (OS) is one of the branches of Semiotics particularly related to business and organizations (Liu, 2000). The study in OS is based on the fundamental observation that all organized behavior is made effective through the communication and interpretation of signs by people, individually or in groups. The aim of OS studies is to find new and insightful ways of analyzing, describing and explaining the structure and behavior of organizations, including their inner workings, and the interactions with the environment and with one another.

This work brings communication to the discussion of safety-critical systems by proposing a communication based process model, including procedures and artifacts, for designing interaction in these systems based on a semiotic-informed theoretical and methodological background. As instance of this process model, we will illustrate the proposed approach with a case study on the Scientific Satellite Payload Support System (SAPOP), a system designed to support research investigators, sub-systems operator and operation coordinator to program the satellite for executing experiments during the flight (Francisco and Sagukawa, 2006).

The paper is organized in the following way: The next section presents literature contributions regarding interaction in safety-critical systems. The third section presents the proposed communication-based model. Section four presents the case study illustrating the application of this communication process model. The conclusion section summarizes the contribution and points out to new challenges.

6.2 Literature Background

Several works have been proposed in literature for improving the quality of human-computer interaction in critical systems. Most of them involve the areas of human factors and cognitive theories, software design and usability, and socio-technical theories (Guimarães et. al., 2007b) as briefly summarized:

1. Human Factors and Cognitive-related Theories (Baxter and Besnard, 2004; Douk and Leverson, 2006; Galliers and Minocha, 2000; Harrison, 2004a; Harrison, 2004b; Hollnagel, 1993; Smith and Harrison, 2002a; Smith and Harrison, 2002b; Vicente, 2002; Vicente et. al., 1995; Vicente et. al., 1998; Vicente and Rasmussen, 1992) – Papers in this field have contributed especially to understanding of human errors and the human cognition within critical systems. The main findings in this area have been used to explain human reaction when dealing with critical situations.

2. Software Design and Usability (Barboni et. al., 2007; Basnyat and Palanque, 2006; Carver and Turoff, 2007; Connely et. al., 2001; Fields, 2001; Fields et al., 2000; Navarre et. al., 2008; Palanque et. al., 2006; Palanque and Schyn, 2003; Palanque et. al., 1997; Pap and Petri, 2001; Paternò et. al., 2005; Reeder and Maxion, 2005) – Contributions in this field have focused on improvements in parts of the software development process that can have impact on the user interface component. Some

additional or modified steps in the software development process have been proposed to improve the quality of the user interface regarding critical systems.

3. Socio-Technical Approaches (Felici, 2006; Felipe et. al., 2003; Gurr, 2008; Gurr and Hardstone, 2001) – Many critical systems depend on the interaction among a group of people. Socio-technical approaches have been used to understand the interaction among team members using a critical system.

Although some safety-critical systems have a socio-technical nature (Hopkin, 1995), the amount of work related to socio-technical aspects of safety-critical systems is not as expressive as in the other categories of contributions. The studies are multidisciplinary by nature as, for example, Filipe's team work (Filipe et. al., 2003) which also extends it to some aspects regarding user interface design.

The main contributions, grouped by their approaches, can be mapped in the "organizational onion": an Organizational Semiotics (OS) artifact (Liu, 2000;Stamper, 1973) as illustrated by Figure 6.1. The "semiotic onion" metaphorically represents any information system in a group of information layers constituted by informal, formal and technical systems. Any information system, including the critical ones, is situated in a society, in which several layers of information cause direct or indirect influences in the automated artifact. In the informal level, there is a sub-culture where meanings are established, intentions are understood, beliefs are formed and commitments with responsibilities are made, altered and discharged. At a formal system level, form and rule replace meaning and intention, and finally, in the technical level, part of the formal system is automated by a computer-based system. The informal level embodies the formal level which in turn embodies the technical level, meaning that changes in any level may influence the other levels.

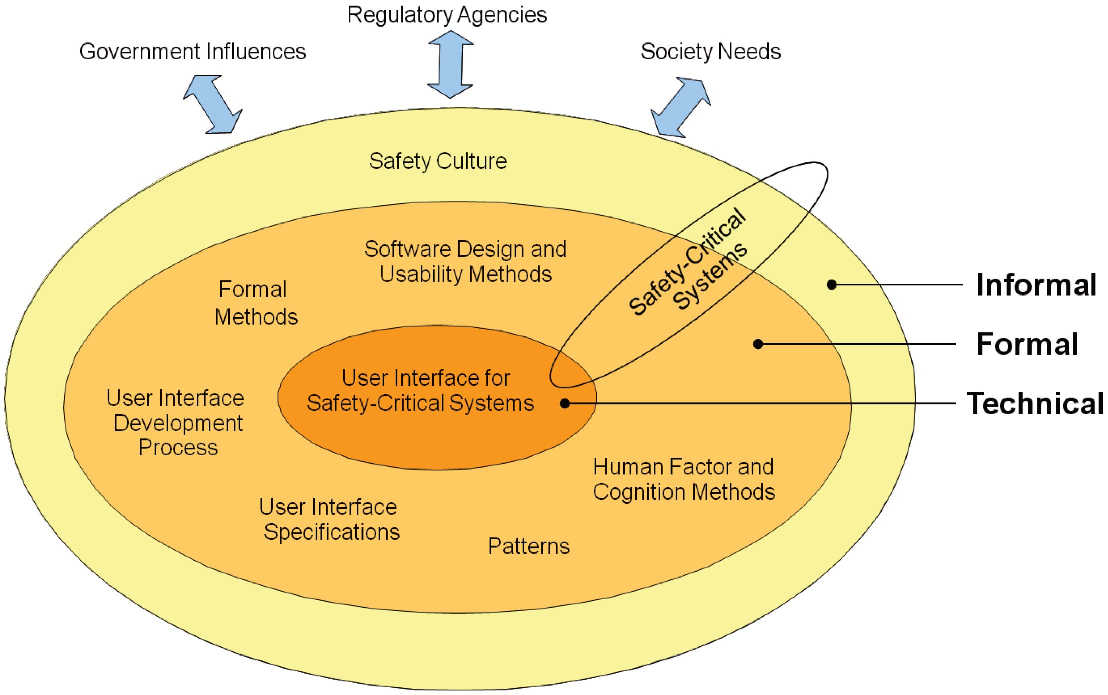

Regulatory Agencies
Government Influences
Society Needs
Safety Culture
Software Design and Usability Methods
Formal Methods
Safety-Critical Systems
Informal
Formal
Technical
User Interface for Safety-Critical Systems
User Interface Development Process
Human Factor and Cognition Methods
User Interface Specifications
Patterns

Figure 6.1: The "onion" model instantiated

As Figure 6.1 illustrates, literature contributions in the field so far are mostly situated in the formal layer, with methods, processes and patterns related to the formal aspects of developing critical systems (Guimarães et. al., 2007b). Not much is found regarding the informal systems layer. Johnson (2003) acknowledges the need of safety culture knowledge within an organization for improvement in safety. Therefore, studies related to informal information systems may bring important contributions to safety-critical systems in general through improvements in their interaction design.

We argue that safety-critical systems have to address the three layers as they are also subject to Governmental influences, Regulatory agencies and Society needs. Communication is present in the three layers of information: informal, formal and technical, because it involves a comprehensive variety of technical, empirical, syntactical, semantical, pragmatical and social aspects. Filipe et. al. (2003) have discussed communication motivated by a real case - an air collision of two aircrafts which may have been caused by failure in communication.

As there is no communication without a system of signs, this work considers Semiotics as theoretical and methodological backgrounds. Guimarães et. al. (2007a) draw on Semiotics (Liu, 2000) to focus on the communicational aspects involved in the requirements elicitation. The proposed approach guides analysts in eliciting requirements regarding communication and its possible failures. The work of Guimarães et. al. (2008) extends the previous work (Guimarães et. al., 2007a) by focusing on modeling and inspection of safety-critical systems using Semiotics as the theoretical and methodological background. This work goes further to propose a design process model under a communication perspective.

6.3 A Communication Process Model

The proposed communication process model uses Semiotics as theoretical and methodological background to deal with the communication perspective in safety-critical systems design.

6.3.1 Semiotics as a Basis

Semiotics is a discipline concerned with the use of signs, their function in communicating meanings and intentions, and their social consequences. Organizational Semiotics (OS), one of the branches of Semiotics, understands that any organized behavior is governed by a system of social norms which are communicated through signs. OS methods and artifacts provide a better understanding of the interested parties of a focal problem, their requirements, as well as the restrictions not only regarding the information system, but the software system as well (Bonacin et. al., 2006). Methods for Eliciting, Analyzing and Specifying Users' Requirements (MEASUR), which resulted from Stamper's research work in the late 70´s (Stamper, 1993), constitute a set of methods to deal with all aspects of information system design. The relevant methods for the specific scope of this work are Stakeholder Analysis, Evaluation Framing and Semiotic Ladder that are briefly described as follows:

1. The Stakeholder Analysis allows investigation of the interested parties (stakeholders) that directly or indirectly exert influences on or are influenced by the information system under analysis. In the stakeholders analysis all interested parties are categorized into different groups: Operation, Actors/Responsible, Clients/Providers, Partners/Competitors and Spectators /Legislators (Liu, 2001).

2. The Evaluation Framing is an extension of the Stakeholder Analysis (Baranauskas et. al., 2005), which allows identifying, for each stakeholder category, their questions and problems, in order to discuss possible solutions.

3. The Semiotic Ladder (SL) is an artifact primarily used to clarify different levels of communication. Stamper (1973) extended the traditional semiotic divisions of syntactics, semantics and pragmatics by adding three other layers: social world, physical world and empirics as depicted in Figure 6.2, which, all together, form the SL.

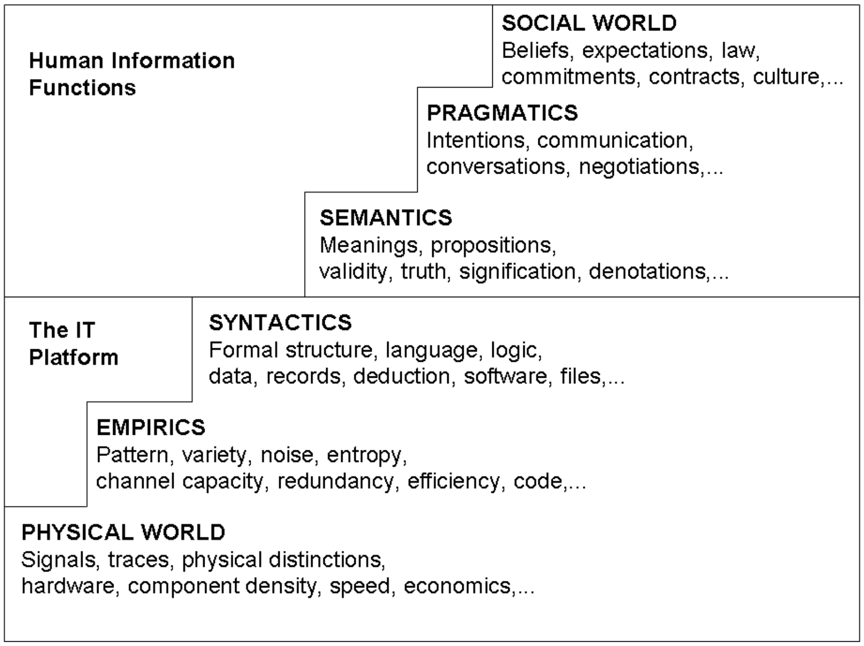

SOCIAL WORLD
Beliefs, expectations, law, commitments, contracts, culture,...
Human Information Functions
PRAGMATICS
Intentions, communication, conversations, negotiations,...
SEMANTICS
Meanings, propositions, validity, truth, signification, denotations,...
The IT Platform
SYNTACTICS
Formal structure, language, logic, data, records, deduction, software, files,...
EMPIRICS
Pattern, variety, noise, entropy, channel capacity, redundancy, efficiency, code,...
PHYSICAL WORLD
Signals, traces, physical distinctions, hardware, component density, speed, economics,...

Figure 6.2: Semiotic Ladder, adapted from Stamper (1973)

A communication is considered successful if all these six levels of the SL are successfully accomplished. The communication in the upper levels depends on the result of the communication on lower levels. These levels provide different views for analysis of different aspects of signs. The Physical World deals with the physical aspects of signs. In telecommunication, for example, there are some physical signs such as those transported by cable or radio waves. The Empirics deals with the statistical properties of signs such as channel capacity, patterns, efficiency. In the Syntactic level, the signs and their relations to other signs form a structure, language, data and records. The Semantics deals with signs and their relations to meanings that users perceive. In the Pragmatic level, the signs and their intention and effect on users are identified. Finally, in the Social World, the signs and their relation to social implications are considered. Therefore, the SL links technology, human factors and social issues.

In the communication perspective, we can categorize some hazards according to the SL as follows:

1. Physical world hazard – hazard regarding physical components such as hardware components, damaged cable, burnt fuse, memory fault.

2. Empirical hazard – problems or limitations on the channel capacity or information flow (e.g. transmission rate decreasing, noise rate increasing).

3. Syntactic hazard – structure-related problems or any violation of the structural standard (e.g. network communication protocol violation).

4. Semantic hazard – problems related to meanings or misinterpretation of information (e.g. misinterpretation of the meaning of an interaction channel, error messages).

5. Pragmatic hazard – problems related to intentions, negotiations and conversations (e.g. usability problem when the user does not understand the intention behind a specific icon).

6. Social world hazard - problems related to social and cultural issues, beliefs, expectations, contracts, commitments (e.g. when a system executes a specific task that is different from the user expectations, contract or user beliefs).

As the communication on the upper layers of the SL depends on the lower layers, having a physical fault means that all layers above the physical one will have problems and consequently, the communication fails. Therefore, communication is critical as it is accomplished successfully only if all layers do not present failure.

To capture the structure of the communication involved in the application domain we use the Fractal Model of Communication (FMC) (Salles, 2000; Salles et. al., 2001). The FMC stresses the fact that, in order to design the primary message (the system's interface), other fractionated messages must be carefully designed and appropriate channels must be chosen to convey them.

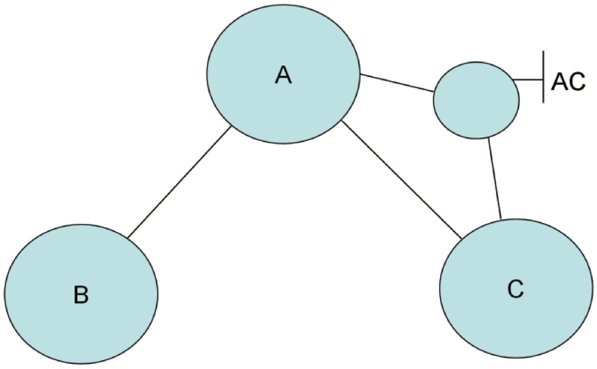


Figure 6.3: The Fractal Model of Communication (Salles et. al., 2001).

The FMC models agents communicating through channels. An agent shares information with others through channels. Figure 6.3 represents this concept of communication in which, in one level, agents B and C communicate through channel A. In another dimension, A assumes the role of an agent in communication with C through channel AC.

6.3.2 An Overview of the Proposed Communication Model

The proposed process model involves multi-disciplinary issues and artifacts coming from different fields: Semiotics, Software Engineering and Human-Computer Interaction. Figure 6.4 illustrates the relation among these fields. The solid arrows represent the semiotics-related artifacts, which provide the communication perspective of a system, and are used as inputs for a communication-based process which is composed of two phases: requirements analysis and design. The dashed arrows indicate the target contributions of each part of the communication-based process for a critical system development process.

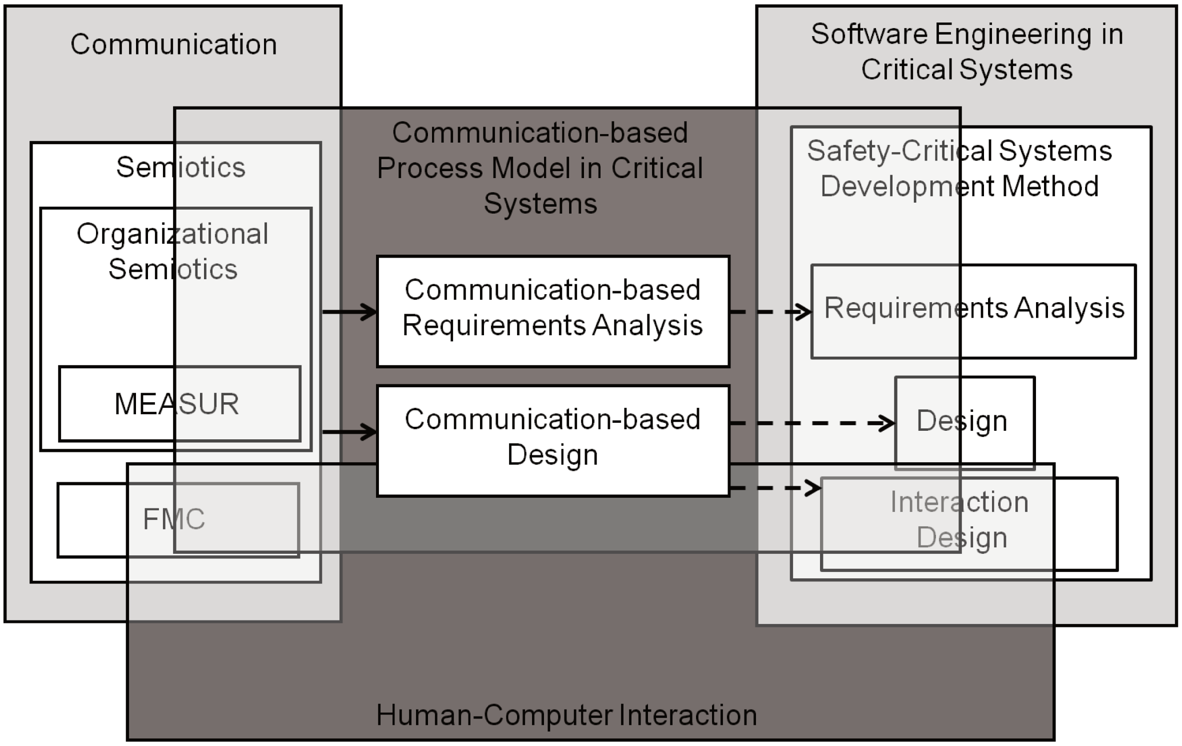
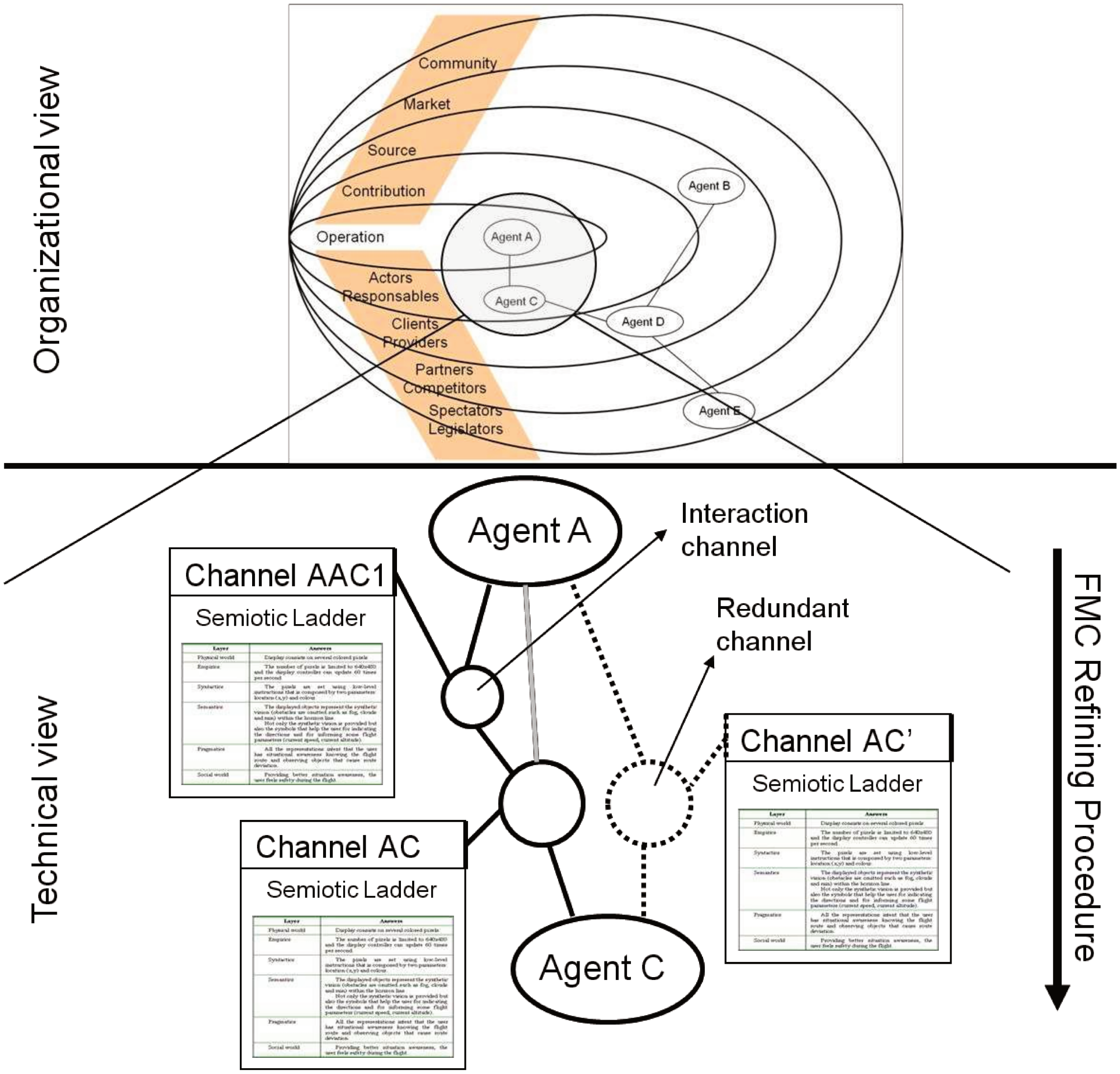

Communication
Semiotics
Organizational Semiotics
MEASUR
FMC
Communication-based Process Model in Critical Systems
Communication-based Requirements Analysis
Communication-based Design
Software Engineering in Critical Systems
Safety-Critical Systems Development Method
Requirements Analysis
Design
Interaction Design
Human-Computer Interaction

Figure 6.4: Relations among different fields.

During requirement analysis we work on the problem articulation using some MEASUR methods: Problem Articulation Methods (PAM), Evaluation Framing, Semiotic Diagnosis and Norm Analysis Methods (NAM). The FMC is developed based on the artifacts produced. With these artifacts and the FMC, the communication-based requirements are modeled. Guimarães et. al. (2007a) describe this process in detail.

During communication design, the FMC is refined becoming a fine-grained model representing the communication structure in conjunction with the Semiotic Ladder artifact which complements a detailed specification. The Stakeholder Analysis and the Evaluation Framing artifacts are considered inputs for the definition of agents and channels of the FMC. The Evaluation Framing identifies channels that provide the communication between agents. The communication inspection is accomplished by analyzing all the six levels of the SL for each channel. The Physical, Empiric and Syntactic levels focus on information technology and the Semantic, Pragmatic and Social World levels focus on the human context as Figure 6.2 illustrates. The SL also allows defining hazards and actions for each level. An action is directed to a specific hazard which consists of a procedure that is executed when a hazard occurs for solving or diminishing the problem caused by a hazard. Moreover, the designer may add information about how to detect the hazard.

Figure 6.5 depicts a conceptual communication model with artifacts and procedures representing the communication structure of an interactive system. In the organizational view, PAM model represents the stakeholders categorized by groups. A FMC model is represented over this PAM model considering stakeholders as agents. If there is a communication between two stakeholders, they are connected by a line as represented in the FMC model. The resulting model is a detailed FMC model composed of channels which may have interaction channels (channels to the user, e.g. channel AAC1) or redundant channels (e.g. channel AC´ is a redundant channel for AC).



Layer	Answers
Physical world	Display consists on several colored pixels
Empirics	The number of pixels is limited to 640x480 and the display controller can update 60 times per second.
Syntactics	The pixels are set using low-level instructions that is composed by two parameters: location (x,y) and colour.
Semantics	The displayed objects represent the synthetic vision (obstacles are omitted such as fog, clouds and rain) within the horizon line. Not only the synthetic vision is provided but also the symbols that help the user for indicating the directions and for informing some flight parameters (current speed, current altitude).
Pragmatics	All the representations intent that the user has situational awareness knowing the flight route and observing objects that cause route deviation.
Social world	Providing better situation awareness, the user feels safety during the flight.

Figure 6.5: Communication Structure in Safety-Critical Systems after Refinement.

The refinement procedure is executed for obtaining the expanded FMC model extending the organizational view to a technical view. In the first iterations of the refining procedure, the channel identification may be guided by information extracted from the Resources column of the Evaluation Framing table which represents resources or media that a stakeholder needs for obtaining solutions. According to Guimarães and Baranauskas (2009), the refinement allows more detailed views of the critical system under the communication perspective. The refinement starts considering stakeholders in the Operation and Contribution groups of the PAM artifact (Figure 6.5) and the more detailed FMC model which extends the organizational domain to the technical domain. Figure 6.6 depicts one iteration of the refining procedure.

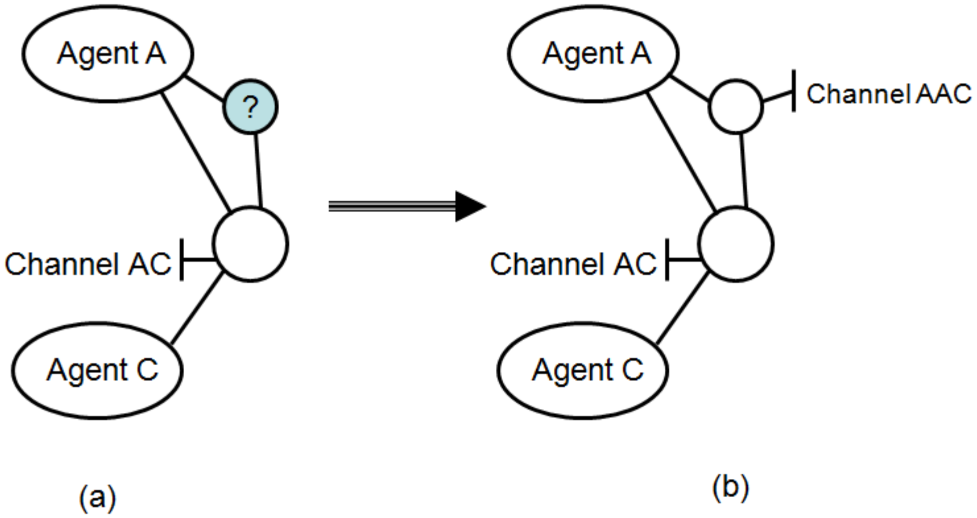


Figure 6.6: The FMC refining procedure for a specific domain (Guimarães et. al., 2008)

Figure 6.6a shows the FMC with the agents “Agent A” and “Agent C”. To refine the context between Agent A and channel AC for obtaining more details regarding the communication between these agents (the designer is who takes refinement decision during the system design), the channels need to be identified by answering the question: “Who is intermediating Agent A and Channel AC communication?” The answer to this question identifies the new channel that should be considered. The next step involves defining the correspondent SL for these new channels with information regarding this communication. Figure 6.6b represents the generic structure after inserting the new channel AAC and its correspondent SL. Therefore, the refining procedure can be repeated for obtaining more detailed (fine-grained) view of the communication with all necessary channels and agents for analyzing the critical aspects of a system design.

According to Sommerville (2003), using redundancy is a typical strategy to design solutions for critical systems. The proposed communication model enables to represent redundancy for some critical channels, indicated as dashed representations in Figure 6.5. If any of these channels is damaged or inactive, the redundant one must be activated.

In interactive safety-critical system, after the refining procedure, we will have the interaction channels for user communication. All interaction channels must communicate with the user, at least, suggesting they are interactive. If this communication fails, the user won’t act and this may lead to unexpected critical consequences.

During the interaction design, the part of the communication model composed of interaction channels, is considered. Interaction design focuses on how the interaction channels should be displayed and available for communicating with the user. The FMC model contributes to identifying how the information content should be obtained, which information content should be displayed for the user and also how the interaction channel(s) should be displayed. When the user interacts with some objects, information is generated and propagated in this communication structure. This information is interpreted and stored by agents or channels. This dynamics of the communication structure (that includes the interaction channels) is functional only if the six levels of the SL for each channel are well connected (with coherent information in all levels of SL) to the others. Each channel must be capable of interpreting the information and knowing how to handle it.

Therefore, during the interaction design, all communication with the user through interaction channels must be consistent with the communication structure considering all six levels of SL (Physical world, Empiric, Syntactic, Semantic, Pragmatic and Social world).Besides information about how the communication is accomplished in six levels of communication, in the hazard handling scope, the SL also provides information about hazards and correspondent actions for handling these hazards or failures regarding communication. The hazards can be categorized into each layer of the SL. Defining action for hazards may provoke discussions; in the case of a display failure, for example, the need for displaying more information in one display may be a challenge for designers.

Therefore, the communication is comprehensive enough to cover the organizational and technical aspects focusing the six levels of the SL defined for each channel. Basically, the FMC helps to have design solutions in the communication perspective by:

1. Providing mechanisms that handle the hazard located at each SL layer avoiding the communication fault of a specific layer. For example, when a transmission rate is not enough, a mechanism located in the empiric layer may send an event for a new connection requesting another free transmission band.

2. Providing an additional channel that handles the hazard. These new channels may be directed to solve a specific hazard or just switch to another connected channel, when a channel is not functional (e.g. redundant channels management). For example, a channel may switch to a redundant display once detected that the display is damaged. The mechanism of switching procedure will depend on the context. It should be discussed by designers about what the design solution will be provided. The switch may be handled automatically or it may require a user intervention. If user intervention is required, the detected problem should be clear enough for notifying the problem to user leading to a concise user feedback. Designers may discuss how to provide a good situational awareness which help users to take better decisions. The SL will guide discussion on the six communication levels in the context of a specific channel.

By using the redundancy strategy in design solutions, it is necessary to have also another redundant agent that would have this information for assuring that the problem can be handled.

There are several ways to have solutions based on redundancy channels. According to Sommerville (2003), in critical system architecture, Triple-Modular Redundancy (TMR) in hardware systems consists of three redundant components replicated for handling faults if one of these components fails. In software systems, the same analogy of TMR is applied as N-versions Programming which consists of developing at least three versions of software systems (two versions should be consistent if one version fails) based on the same specification and functionality.

In the communication perspective, the same analogy of TRM and N-versions Programming can be applied to the FMC model creating new communication paths providing at least three alternative ways of communication between two or more critical agents or channels.

6.4 A Case Study in a Space System

This section presents the design model regarding communication for Scientific Satellite Payload Operation Support System (SAPOP), described in Francisco and Sagukawa (2006).

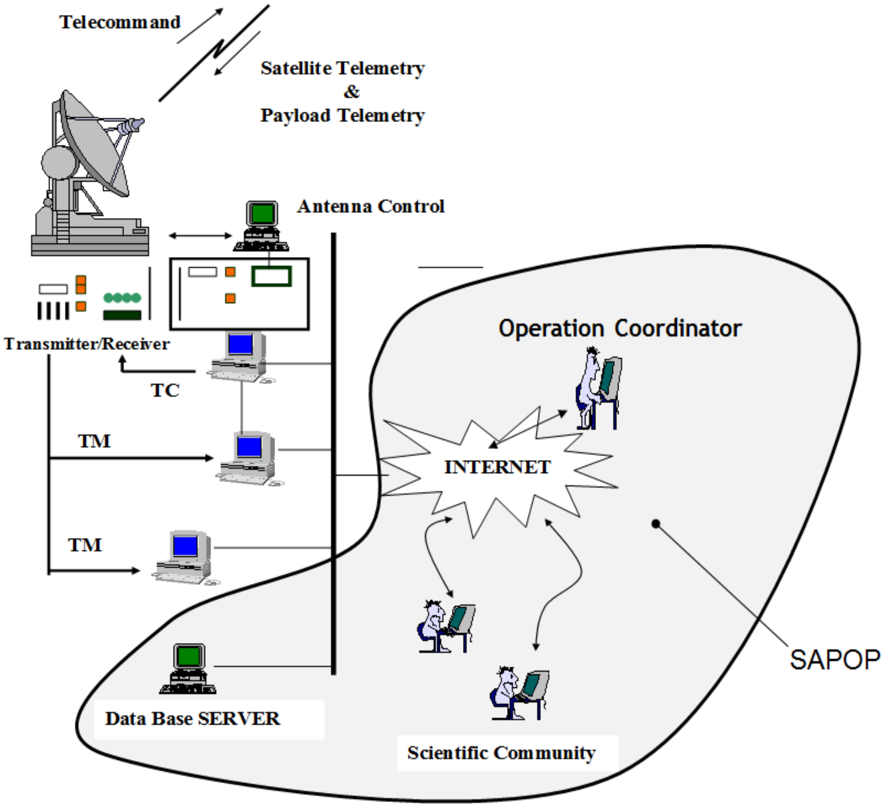


Figure 6.7: SAPOP system, adapted from Francisco and Sagukawa (2006)

To execute a specific missions (e.g., atmospheric phenomena analysis), satellites have a payload which consists of a set of instruments with specific sensors. The satellite on-board computer collects, processes data from sensors and sends packets to ground system through telemetry, as Figure 6.7 depicts. The telemetry has information about collected data regarding internal satellite system (internal temperature, internal components status, battery power and so on) and also payload data (information collected by the payload system which has specific purpose sensors for scientific studies). These data are analyzed by investigators (researchers who have the direct access to this payload information) for a specific research purpose.

During the satellite-ground system communication, some satellites receive sequences of telecommands (TCs) which are a set of commands to be executed immediately or in programmed time in the on-board satellite. Payload team (or investigators in the Scientific Community) uses SAPOP for defining TCs regarding payload system, and the sub-system operators use it for defining TCs of internal satellite sub-system through Internet network as Figure 6.7 illustrates. The Operation Coordinator (OC) is the user who authorizes transmission of some TCs sequences stored at a data base server to the satellite.

The safety-critical issue of the SAPOP is the sequence of the TCs that may lead to a total or partial loss of mission (Francisco and Sagukawa, 2006). As SAPOP is an interactive system, the human error (e.g. Operation Coordinator mistake) may lead to a total loss of the mission with high cost for the project. In the next section, this critical aspect will be analyzed under the communication perspective focusing on the interaction between the Operation Coordinator (OC) and SAPOP.

6.4.1 Organizational View

Before defining the requirements for SAPOP, the PAM artifact is produced defining the target system and the stakeholders as Figure 6.8 depicts. The Stakeholder Analysis (Liu, 2001) shows stakeholders categorized in groups with several knowledge and responsibility areas. For each stakeholder, an Evaluation Framing (Baranauskas et. al., 2005) provides more information regarding conditions (or effects), problems that they may have, proposed solutions and resources needed for the solution.

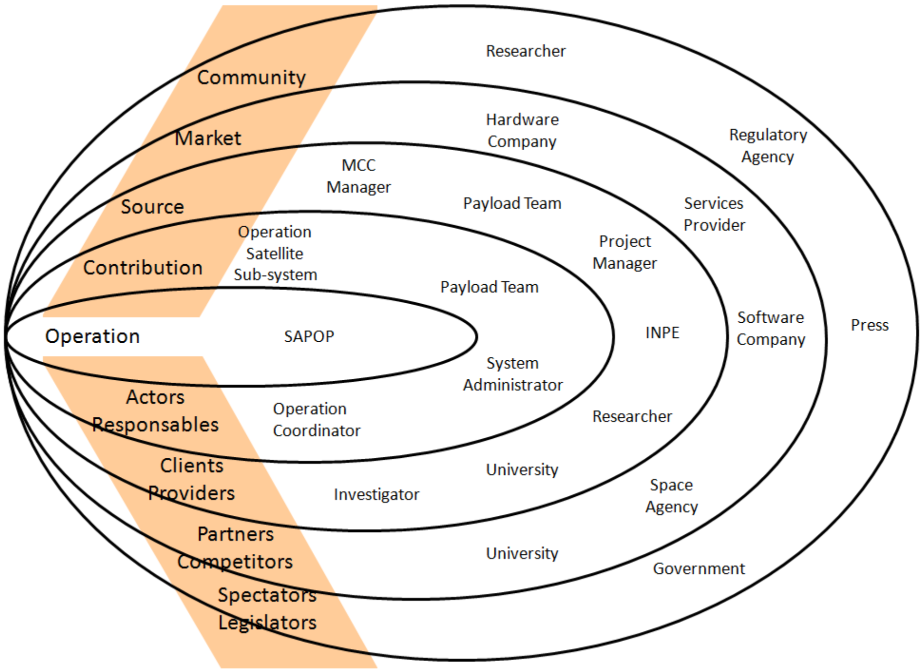


Figure 6.8: SAPOP Stakeholder Analysis Model

6.4.2 Technical View

The refining procedure is started with the stakeholders categorized in the Operation and Contribution groups because, typically, the Contribution group represents the users and the Operation group, the target system. The SAPOP interacts with four types of users:

1. System Administrator – user who manages and controls the access of users accounts;

2. Payload team – researchers who need the data collected from the space for investigation; they also define the telecommand sequences regarding the payload system;

3. Operation Coordinator – user who authorizes telecommands to be sent to satellite;

4. Sub-system Operator – user who defines the telecommand sequences regarding the satellite sub-system (satellite system excluding the payload system).

Figure 6.9 is a part of the PAM and FMC models with the agents and channels generated after the refining procedure. This procedure starts with the SAPOP agent who belongs to the Operation category and agents in the Contribution category of the Stakeholder Analysis model, producing not only new channels but also connections with stakeholders which belong to any group of PAM model. Figure 6.9 shows that the stakeholder Operation Coordinator, who belongs to the Contribution category, connects to other stakeholders outside of this category, the Project Manager (agent that belongs to the Source category in the Stakeholder Analysis model). Figure 6.9 also shows that there are several new channels produced by refining procedure execution (e.g. the Operation Manual channel).

One of the identified channels is the User Interface (UI), by observing the column Resource in the Evaluation Framing corresponding to the System Administrator, Payload Team, Operation Coordinator and Sub-system Operator stakeholders. The UI is the part of SAPOP which allows the users-system interaction and communication.

Figure 6.9 also shows the interaction channels (Flight Plan Generation Window and Flight Plan Checking Window). These channels represent a communication means used by the User Interface channel. More interaction objects inside of these windows will appear if the refinement procedure is executed more times. Therefore, through this procedure, FMC connects to interaction design domain.

These connections produced by executing the refinement procedure may extend beyond Stakeholder Analysis domain resulting in a complex and huge model with a high number of agents and channels involving other domains in organizational and technical context. For example, if this procedure is applied in the communication between SAPOP and Operation Coordinator, as UI is a communication channel between users and SAPOP, a more detailed view may be obtained with UI interaction channels.

Another example, if the refining procedure is applied to the communication between INPE (National Institute for Space Research) and the SAPOP, new agents and channels may be in the domain of development process because software development process is one of the communication means between organization (INPE) and its employees involving to SAPOP development.

6.4.3 Identifying Redundancy

The FMC for SAPOP current version was modeled as Figure 6.9 illustrates. The Operation Coordinator agent has critical information which leads to the satellite loss because he/she has the knowledge about which telecommand sequences are hazardous. One problem identified in this refined model is that the Operation Coordinator is the agent with critical information who communicates with SAPOP through critical interactions by the channel User Interface. If this unique agent fails, the consequences may be catastrophic.

Using N-versions Programming with 3 versions (three redundant channels), if the Coordinator Operator fails, two new paths are added for obtaining three paths between Operation Manual and User Interface channels. Figure 6.9 shows redundancy as dashed representations and the grayed representation means that the domain is outside interaction design. The first redundant path is the insertion of a new user called Flight Plan Reviewer who reviews the flight plan produced by the Operation Coordinator. The second redundant path represented by the Telecommand Hazard Detection channel is an internal software component of SAPOP system which has knowledge about the critical telecommand sequences which can be implemented based on Operation Manual used by Operation Coordinator. These three channels (Operation Coordinator, Flight Plan Reviewer and Telecommand Hazard Detection) have the output decided by comparing the information of these channels. The final result consists of the highest occurrence of outputs of these channels.

Figure 6.9 also shows interaction design affected by redundancy. The Flight Plan Checking Window channel, which is the interaction channel, also appears as a redundant channel towards safety improvements.

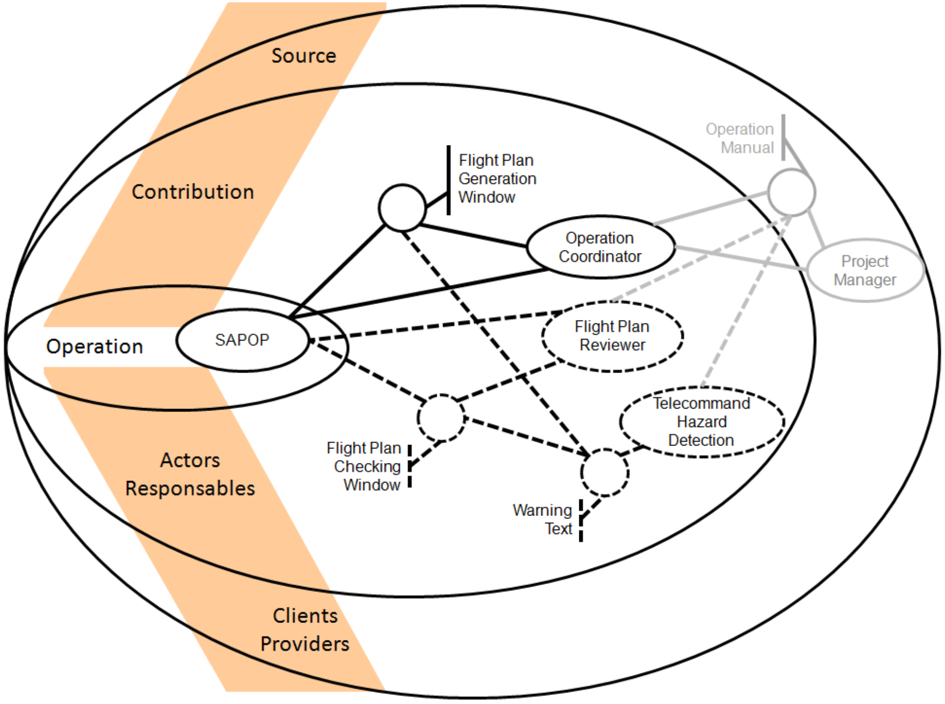


Figure 6.9: Triple-Modular Redundancy Solution for SAPOP

Without redundant channels, if the operation coordinator commits an error defining a sequence which leads to a mission loss, the consequence cannot be avoided because there is no way for handling this problem. If this scenario happens in the proposed SAPOP, the possibility of a mission loss is lower due to redundancy system.

On the other hand, the proposed SAPOP demands considerable higher cost because redundancy demands some additional resources such as: human resource for reviewing the flight plan (channel Flight Plan Reviewer) and the software of SAPOP (channel Telecommand Hazard Detection) including more robust UI. Therefore, this solution is addressed to organizations where safety culture is considered important where there is a strong demand on safety improvements being aware of higher financial expenses.

Table 6.1 represents SL for three channels: Flight Plan Generation Window, Flight Plan Checking Window and Warning Text. The designer has clear and detailed information on how the communication is accomplished in six aspects of channels communication. Therefore, SL should be considered for defining design (including interaction design) solutions for critical systems. If more detailed investigation is necessary, it is possible to execute the refining procedure for obtaining more specific channels and consequently, SL for these specific channels can be developed.

Table 6.1: Semiotic Ladder for some channels

Layer	**Flight Plan Generation Window**	**Flight Plan Checking Window**	**Warning Text**
Physical World	Liquid Crystal Display (LCD)	Liquid Crystal Display (LCD)	Liquid Crystal Display (LCD)
Physical world hazard	Hazard: Display is damaged Action: User can be recommended to have a redundant display.	Hazard: Display is damaged Action: User can be recommended to have a redundant display.	Hazard: Display is damaged Action: User can be recommended to have a redundant display.
Empirics	Resolution is limited to 1024x768	Resolution is limited to 1024x768	Resolution is limited to 1024x768 String size is limited to 110 characters.
Empirical hazard	Hazard: Complex graphical representation demanding on more display resolution. Font size is too small	Hazard: Complex graphical representation demanding on more display resolution. Font size is too small Action: UI Designer must evaluate the objects fonts for avoiding this problem.	Hazard: Complex graphical representation demanding on more display resolution. Font size is too small Action: UI Designer must evaluate the objects fonts for avoiding this problem.

	Action: UI Designer must evaluate the fonts, objects for avoiding this problem.		Hazard 2: String is larger than 110 chars. Action 2: Interaction object should become multiline object. Hazard 2.1: If there is no space for resizing this object. Action 2.1: Provide tooltip using all screen for showing the message. User just put the cursor on this object and a tooltip is shown only in case of big message.
Syntactics	This window is defined as a Web browser standard window with the following components: - Event handler for interaction objects - Interaction objects managements - See details in software specification	This window is defined as a Web browser standard window with the following components: - Event handler for interaction objects - Interaction objects managements - See details in software specification	This window is defined as a Web browser standard window with the following components: - Event handler for interaction objects - Interaction objects managements - Maintain the list of interaction objects - See details in software specification
Syntactic hazard	Hazard: All these problems related to object structure should be detected by software testers Action Software test is required! Develop tests and apply fixes.	Hazard: All these problems related to object structure should be detected by software testers Action: Software test is required! Develop tests and apply fixes.	Hazard: All these problems related to object structure should be detected by software testers Action: Software test is required! Develop tests and apply fixes.
Semantics	This object represents the	This object represents the application as a whole	All text messages for warning the user is

	application as a whole grouping all interaction objects of the main window for user Operation Coordinator.	grouping all interaction objects of the main window for user Flight Plan Reviewer.	displayed through this object.
Semantic hazard	Hazard: The grouping representation is not clear Action: Usability test is required. - The window should be redesigned. - Provide window customizations.	Hazard: The grouping representation is not clear Action: Usability test is required. - The window should be redesigned. - Provide window customizations.	Hazard: User can´t understand the message Action: All possible messages should be analyzed with user(s) for evaluating if the message is clear. Hazard 2: Message is shown improperly. Message is truncated. Action 2: See Empirical layer.
Pragmatics	The intention of this window is identifying which interaction elements belong to the main application for user Operation Coordinator. There is no other way which could substitute a window.	The intention of this window is identifying which interaction elements belong to the main application for user Flight Plan Reviewer. There is no other way which could substitute a window.	The intention is providing a way to communicate with the user through a text without interrupting user´s work. In general case, it is recommended when a user is waiting for a system response, as a warning. The other way is using a pop-up window but it may annoy the user forcing his/her work interruption unless the message is very important.
Pragmatic hazard	Hazard: User can’t understand the intention of the window, the reason	Hazard: User can’t understand the intention of the window, the reason of the window.	Hazard: User can’t understand the intention of the warning text, the reason of the text

	of the window. Action: This problem is detectable during usability test. Is the user waiting for maximized window? Is the user familiarized with window system?	Action: This problem is detectable during usability test. Is the user waiting for maximized window? Is the user familiarized with window system?	warning object. Action: This problem is detectable during usability test. Is the user waiting another way of response? Is the user familiarized with this interaction object? Hazard 2: User disagrees with the usage of this interaction object. Action 2: Evaluate and provide other solutions: pop-up dialogs?
Social world	Window indicates the presence of the application for meeting users' needs for showing the group of information and the option for submitting telecommands of a specific mission.	Window indicates the presence of the application for meeting users' needs for showing the group of information and the option for submitting telecommands of a specific mission.	Warning Text indicates a component of the application for meeting the user's needs for obtaining information about what happened after submitting telecommands of a specific mission.
Social world hazard	Hazard: The system doesn´t meet the user´s needs leading to finish the contract Action: Renegotiate with the client.	Hazard: The system doesn´t meet the user´s needs leading to finish the contract Action: Renegotiate with the client.	Hazard: The system doesn´t meet the user´s needs leading to finish the contract Action: Renegotiate with the client.

FMC also allows having one structure connecting the organizational (with several interconnected segments) and the technical views, and interaction channels belong to this same structure. Therefore, the conceptual communication model allows seeing the connections from interaction channels to stakeholders in an organization in a multiple view.

In critical systems, it is important to consider that some agents/channels may fail, blocking some communication paths. The communication structure can be useful for defining communication-related fault tolerant systems. When a fault occurs, the channels/agents should have functionality for seeking other communication path(s).

The drawback of this communication perspective is that the FMC model may be huge and complex because of the high complexity of the communication structure, since the number of agents and channels may be very extensive and, consequently, developing all SLs is also costly. In the case of SAPOP, after refining the communication between SAPOP and all type of users, the total number of channels is 142. Therefore, it has about 142 SLs and each SL has six levels of communication to be specified.This complexity leads to the visualization of FMC model with high quantity of channels and connections. A tool with filtering functionalities is the solution for this visualization complexity.

The communication perspective puts the focus on the critical information content. With the FMC model that is centered in the information content, the UI designer can define the channels that provide critical information. In the SL of these critical channels, we have the information regarding how this critical information is communicated to users. It may help designers to conduct a better analysis contributing to situational awareness and avoiding hazardous consequences. A further work involves quantifying how much this approach might improve on the situational awareness and safety issues.

6.5 Conclusions

The communication perspective provided by Semiotics as theoretical and methodological background allows a new view on critical systems development. This paper proposed a conceptual communication model with related procedures based on artifacts of Organizational Semiotics combined with the Fractal Model of Communication (FMC). FMC provides communication design with agents and channels allowing to have unlimited fractal dimensions presenting overview and detailed information of each channel. The Semiotic Ladder (SL), which defines the six layers (or levels) of communication, merged with FMC, led to a richer communication-based modeling for designing critical systems; the structure of communication contains information regarding physical world, empiric, syntactic, semantic, pragmatic and social aspects with potential hazard and the correspondent actions. The conceptual communication model allows representing communication in organizational (with several interconnected segments) and technical levels (including interaction channels) in a connected way. Visualization tools may allow the presentation of the FMC model with a configurable filter to allow visualizing each fractal dimension separately, zooming in and out to show only the agents and channels needed for a specific consideration. The proposal was applied to a case study with SAPOP - a space software system which provides support for defining a safe sequence of commands for transmission to a scientific satellite. If it fails, satellite missions can be lost leading to high financial loss.

As future work, a tool to support this method should be developed. The FMC uses to grow and a tool should provide facilities for viewing and for searching for a specific agent or channel, visualizing several degrees of FMC detailed views and identifying alternative paths for critical agents/channels.

In this work, the redundancy strategy was used in conjunction with the communication based method but other strategies can be used and analyzed to demonstrate advantages and disadvantages of using it in conjunction.

Capítulo 7

Interaction Design and Redundancy Strategy in Critical Systems

7.1 Introduction

A growing demand on hardware and software systems is also expanding into critical areas that used to be managed mostly by human beings. The concept of a critical system has been discussed by several authors encompassing from conceptual to technical issues. The safety-critical category of system is defined as a system whose failure would provoke catastrophic or unacceptable consequences for human life (Paulson, 1997).

Literature on critical systems has long shown dramatic cases of human-system failures that resulted in people's deaths. Therac-25 is a typical case: an X-ray used to obtain bone images (through x-ray emission) or to treat tumours (through radiation emission). The message "Malfunction 54" had no meanings for operators, who just ignored it (Mackie and Sommerville, 2000), although, for the software developer, the message intended to inform that the radiation dosage was above normal values. Due to this human-computer communication problem reflected in the user interface (UI), the consequence of this episode was disastrous leading to several deaths because of the extreme radiation injected to patients. More dramatically, as the effect of over dosage was not instantaneous, it took several years for the problem to be identified.

In aviation systems, many incidents (unexpected events that may or may not lead to accidents that may lead to deaths) have reasons originated from failures occurring during user-system interaction. Harrison shows some statistics: from 34 total incidents (1979-1992); 4% of the deaths were due to physical causes; 3% of the deaths were due to software error; 92% of the deaths were due to problems related to human-computer interaction

(Harrison, 2004b). Moreover, according to ATC (Air Traffic Control), 90% of the air traffic incidents were due to faults attributed to pilots or controllers. Nowadays, the flight decks (or cockpits) have multifunction computer displays where huge amounts of information are presented (Carver and Turoff, 2007). This new concept of modern cockpit, named "glass cockpit", provides rich amount of information presented as graphical elements through diagrams and symbolic information. In parallel with this evolution, sophisticated automation systems may produce conflicting data from different sources forcing decisions about which information to act upon. The pilot needs to navigate through layers and layers of information becoming more a system engineer than a pilot.

The ReSIST project (ReSIST, 2008) created a new field of study, Resilience Systems, which includes safety-critical systems. Several gaps and challenges regarding resilience-building technology are discussed in terms of architecture, algorithms, socio-technical factors, verification and evaluation aspects. The resilience needs encompass several aspects including the usability of systems, particularly the ubiquitous ones. Helping users interaction with ubiquitous systems aims at understanding the potential effects of their actions as well as preventing them from taking actions with unwanted and difficult to anticipate system-level effects. Usability is considered one of the most important aspects to consider in critical systems; gaps and challenges are still being identified in the ReSIST project.

The study of signs and rules operating upon them and upon their use, form the core of the human communication study. As there is no communication without a system of signs, Semiotics, as a discipline concerned with the analysis of signs or the study of the functioning of sign systems, may offer an appropriate foundation for this study. Organizational Semiotics (OS) is one of the branches of Semiotics particularly related to business and organizations (Liu, 2000). The study in OS is based on the fundamental observation that all organized behaviour is made effective through the communication and interpretation of signs by people, individually or in groups. The aim of OS studies is to find new and insightful ways of analyzing, describing and explaining the structure and behaviour of organizations, including their inner workings, and the interactions with the environment and with one another.

The goal of this work is to bring communication to the discussion of safety-critical systems by proposing an interaction design procedure in these systems based on a semiotic-informed theoretical and methodological background. This procedure allows to obtain a UI structure (wireframe) using semiotic artefacts. The proposed approach is presented with a case study on the Scientific Satellite Payload Support System (SAPOP), a system to help research investigators, sub-system operator and operation coordinator to program the satellite for executing experiments during the flight using Web services (Francisco and Sagukawa, 2006).

The paper is organized in the following way: the next section presents the theoretical and technical background of this work. The third section presents the proposed design procedure with some semiotic artefacts considered as income and a UI wireframe as outcome. Section four presents the SAPOP case study with this proposed interaction design. Section five has the analysis of the produced UI wireframe. This work finishes with the conclusion section summarizing the contribution and pointing out to new challenges.

7.2 Theoretical Background

Semiotics is a discipline concerned with the use of signs, their function in communicating meanings and intentions, and their social consequences.

Organizational Semiotics (OS), one of the branches of Semiotics, understands that any organized behaviour is governed by a system of social norms which are communicated through signs. OS methods and artefacts provide a better understanding of the interested parties of a focal problem, their requirements, as well as the restrictions not only regarding the information system, but the software system as well (Bonacin et. al., 2006). Methods for Eliciting, Analyzing and Specifying Users' Requirements (MEASUR), which resulted from Stamper's research work in the late 70´s (Stamper, 1993), constitute a set of methods to deal with all aspects of information system design. The Semiotic Ladder (SL) is an artefact primarily used to clarify some important Information System notions such as information, meaning and communication (Cordeiro and Filipe, 2004). Stamper extended the traditional semiotic divisions of syntactics, semantics and pragmatics by adding three other layers: social world, physical world and empirics as depicted in Figure 7.1, which, all together, form the SL.

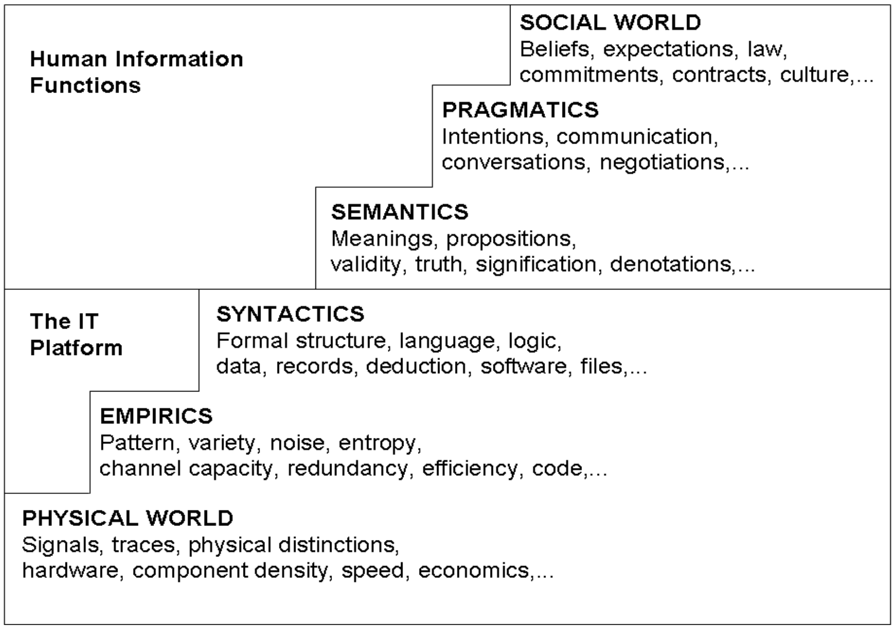

Human Information Functions
SOCIAL WORLD
Beliefs, expectations, law, commitments, contracts, culture,...
PRAGMATICS
Intentions, communication, conversations, negotiations,...
SEMANTICS
Meanings, propositions, validity, truth, signification, denotations,...
The IT Platform
SYNTACTICS
Formal structure, language, logic, data, records, deduction, software, files,...
EMPIRICS
Pattern, variety, noise, entropy, channel capacity, redundancy, efficiency, code,...
PHYSICAL WORLD
Signals, traces, physical distinctions, hardware, component density, speed, economics,...

Figure 7.1: Semiotic Ladder (Stamper, 1973).

A communication is considered successful if all these six levels of the SL are successfully accomplished. The communication in the upper levels depends on the result of the communication on the lower levels. These levels provide different views for analysis of different aspects of signs. The Physical World deals with the physical aspects of signs (Stamper, 1973). In telecommunication, for example, there are some physical signs such as those transported by cable or radio waves. The Empirics deals with the statistical properties of signs such as channel capacity, patterns, efficiency. In the Syntactic level, the signs and their relations to other signs form a structure, language, data and records. The Semantics deals with signs and their relations to meanings that users perceive. In the Pragmatic level, the signs and their intention and effect on users are identified. Finally, in the Social World, the signs and their relation to social implications are considered. Therefore, the SL links technology, human factors and social issues.

The Fractal Model of Communication (FMC) (Salles et al., 2001; Salles, 2000) is used to capture the structure of the communication involved in the application domain. FMC stresses the fact that, in order to design the primary message (the system's interface), other fractionated messages must be carefully designed and appropriate channels must be chosen to convey them. The FMC models agents in communication through channels. Figure 7.2 represents this concept of communication in which, in one level, agents B and C communicate through channel A. In another level, A assumes the role of an agent in communication with C through channel AC.

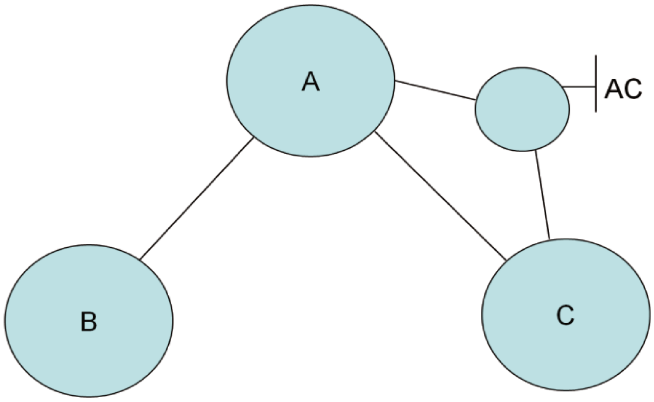


Figure 7.2: The Fractal Model of Communication (Salles, 2000).

The FMC is appropriate for representing the communication structure in critical systems as it makes explicit information about the agents (physical and human) and all the media used in their communication. It allows capturing potential communication failures and to provide redundancy that would be extremely useful for designing the interaction in critical systems. While the FMC provides a structure for analysing agents in communication, the SL allows a deeper analysis into the channels they use to communicate.

7.3 Communication-based Interaction Design

The use of Semiotics (Liu, 2000) to focus on the communicational aspects involved in the requirements elicitation for critical systems is discussed in Guimarães et. al. (2007). In a critical system design, the FMC with SL artefacts were proposed in previous work for modelling communication in critical systems (Guimarães and Baranauskas, 2009; Guimarães et. al., 2008). This work extends this modelling focusing exclusively on the interaction design.

The first step is obtaining the FMC model in the interaction design context through a filtering procedure. Initially, the model has user(s) and agent(s) which can also be interaction channels. Interaction agents or interaction channels consist on agents or channels which interact directly with the user (direct connection to user). All agents and channels which don't have direct connection with any user (called non-interactive agents and channels) are just removed and, consequently, all connections are propagated to an interaction channel or agent. Figure 7.3 illustrates this filtering procedure with the connection propagation where the grey representations are interaction channels and the white ones are non-interactive agents and channels which are removed and the connections are transported to a nearest interaction channel.

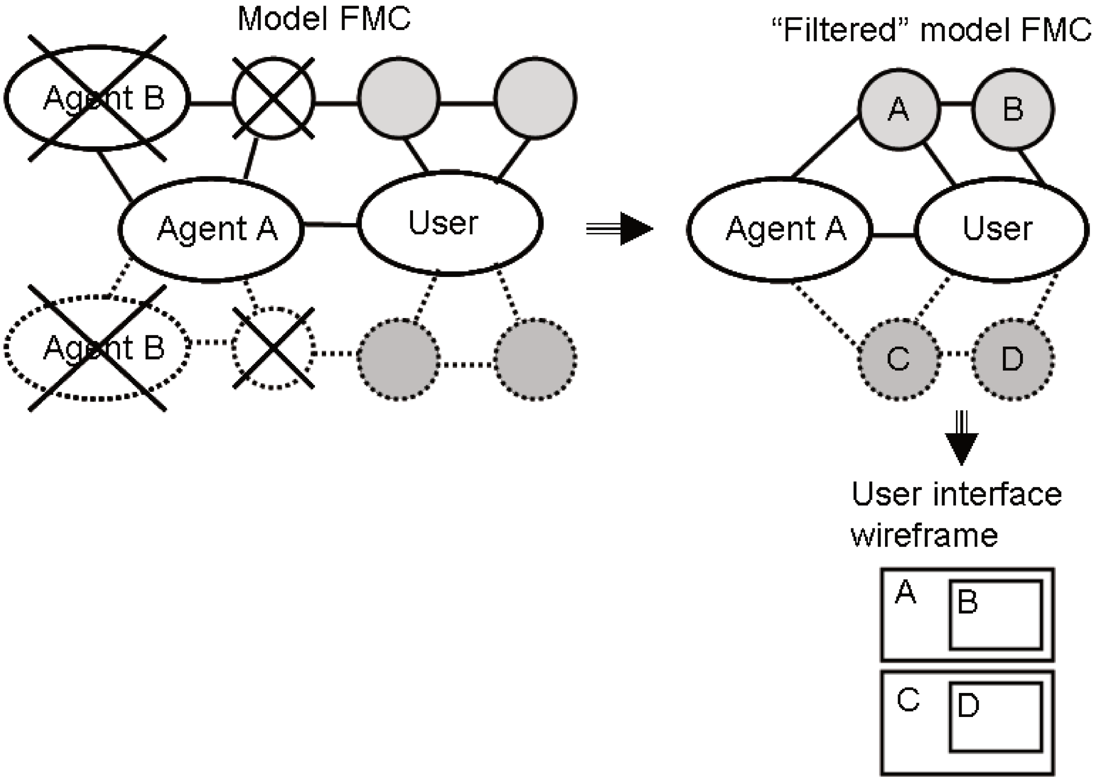


Figure 7.3: Designing User Interface Wireframe.

The next step is the definition of the UI structure. As Figure 7.3 depicts, channels may use other channels for communicating with user, if a channel A uses channel B, then B is an interaction object inside A. For example, the channel A could be a window that uses a channel B that could be a button. In the UI wireframe, the user will have a window with a button as internal interaction object.

By the SL definition, as the communication on the upper layers depend on the lower layers, having a physical fault means that all layers above this level will fail and consequently, the overall communication will fail. In critical systems, the mechanism for handling this failure may use a barrier approach that can be defined for the lower layers. Barrier consists on any mechanism that reacts handling the fault if a hazard is detected. This approach can be applied to represent the diverse physical and organisational decisions that are taken to prevent a target from being affected by a potential hazard (Basnyat et. al., 2007).

The characteristics of each interaction channel are specified in the SL which consists of six communication levels with respective hazards as follows in Table 7.1.

Table 7.1: Semiotic Ladder.

Layer	Description
Physical world	Information about the positioning, size, colours, label and description of the object interaction appearance. For example, the button OK is placed at (12, 56), size = 10 x 5 pixels.
Physical world hazard	Hazard regarding physical world such as invalid positioning, size, label of interaction object. For example, these problems may happen when the resolution display is changed or when the screen is resized.
Empirics	Information about limitations on the channel capacity or information flow (e.g. transmission rate decreasing, noise rate increasing). For example, the button OK can’t handle the double click.
Empirical hazard	Hazards which may handle due to these limitations and problems. For example, what to do, if a button is double clicked.
Syntactic	Information about the sequence of interaction is needed for an interaction object. It consists on interaction behaviour of the interaction channel with the definition about the actions and reactions. For example, when the object is drop-down list, it should appear to user that at first, a button should be clicked and after an option can be listed and then an option can be selected.

Syntactic hazard	Information about the structure of the interaction object and its behaviour. For example, how to inform to user that the drop-down list is empty dispensing with the button click.
Semantics	Information regarding the meaning of an interaction channel for the user. For example, the button should appear clickable.
Semantic hazard	Problems related to meanings or misinterpretation of information, interaction channel or error messages. For example, the user can't recognize that an object is clickable.
Pragmatics	Information about the intention behind the presence of an interaction channel. For example, the button OK is placed at the dialog Confirm Remove File for obtaining the user confirmation before removing the requested file.
Pragmatic hazard	Problems related to intentions of the interaction object. For example, usability problem when the user does not understand the intention behind a specific icon.
Social world	Information about the user expectations, contract, beliefs, and culture related to interaction channels. For example, the expectation of the UI designer must correspond to the user expectation following a specific "contract" (e. g. conventions, culture).
Social world hazard	Problems related to social and cultural issues, beliefs, expectations, contracts, commitments. For example, if the UI behaves differently from what the user was expecting, what it should be done according to the contract.

These SL layers are useful for specifying the communication of each interaction channel and also how to handle communication faults in the six communicational contexts.

7.4 A Case Study in Space System

This section presents the interaction design regarding communication for the Scientific Satellite Payload Operation Support System (SAPOP), developed by National Space Research Institute (INPE) (Francisco and Sagukawa, 2006).

7.4.1 SAPOP Overview

Each satellite has specific missions (e.g., atmospheric phenomena analysis) and contains a payload which consists on a set of instruments with specific sensors. Each instrument collects and processes specific data from sensors and sends them to the satellite on-board computer. This computer, by its turn, sends data to the ground system through telemetry; these data are useful for investigators (researchers who have the direct access to this payload information) for a specific research purpose.

During the satellite - ground system communication, some satellites receive sequences of telecommands (TCs) and send sequences of telemetry in over-the-air transmission as Figure 7.4 depicts. The telemetry has information about the internal satellite system (internal temperature, internal components status, battery power and so on) and payload data (information collected by the payload system which has specific purpose sensors for scientific studies).

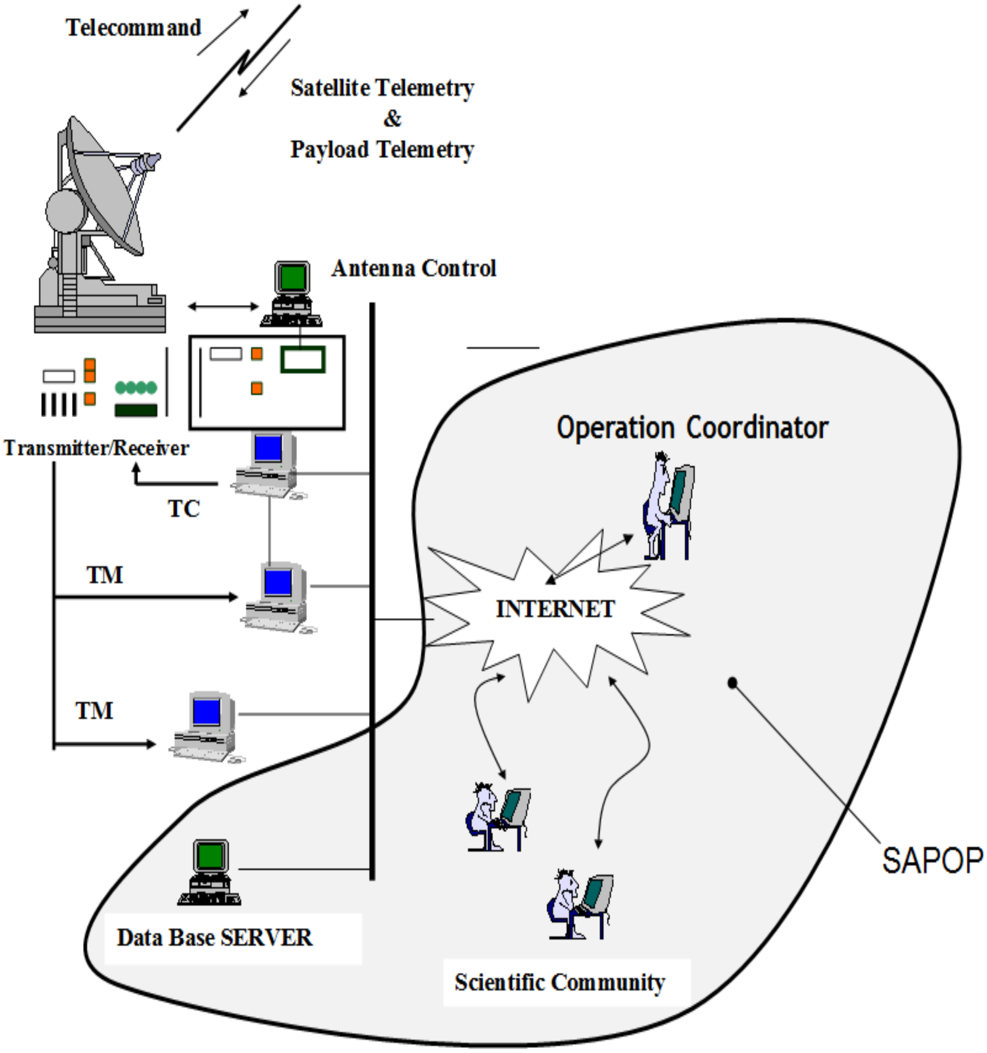


Figure 7.4: SAPOP system (Francisco and Sagukawa, 2006).

The Payload team (or investigator) uses SAPOP for defining TCs of the payload system and the sub-system operators, uses SAPOP for defining TCs of internal satellite sub-system. Figure 7.4 illustrates SAPOP with the TCs as income, which are defined by investigators (represented as Scientific Community) and sub-system operators through Internet network. The Operation Coordinator (OC) is the user who authorizes or not the transmitting of TCs sequences to the satellite through the flight plan that is stored in a data base server.

The safety-critical aspect of the SAPOP is the sequence of the TCs that may lead to total or partial loss of mission (Francisco and Sagukawa, 2006). As SAPOP is an interactive system, the human error (e.g. Operation Coordinator mistake) may lead to total loss of the mission with high cost for the project. This critical aspect will be analysed under the communication perspective focusing on the interaction between the Operation Coordinator (OC) and SAPOP.

SAPOP is an already existent and functional system; its UI was already developed. In this work, the existent UI will be analyzed under the communication perspective for identifying communication problems using one of the strategies known in critical system design: redundancy.

7.4.2 Designing UI Wireframe

After executing the refining procedure resulting in a detailed FMC model, the designer not only defines agents and channels but also all new redundant channels specifying how the communication is accomplished in SL six communication levels (Guimarães and Baranauskas, 2009). The UI designer executes the filtering procedure to focus on the interaction channels only, the resulting FMC model (Figure 7.5 depicts only a part of this model) will be useful for defining the UI wireframe. All channels related to the Flight Plan Generation Window agent are considered interaction objects and are located inside the Flight Plan Generation Window. The Passage Selection channel is an interaction object inside the Table View interaction object. The specification of interaction objects is defined at SL for these channels. Therefore, the outcome of this procedure is the wireframe as Figure 7.6 illustrates.

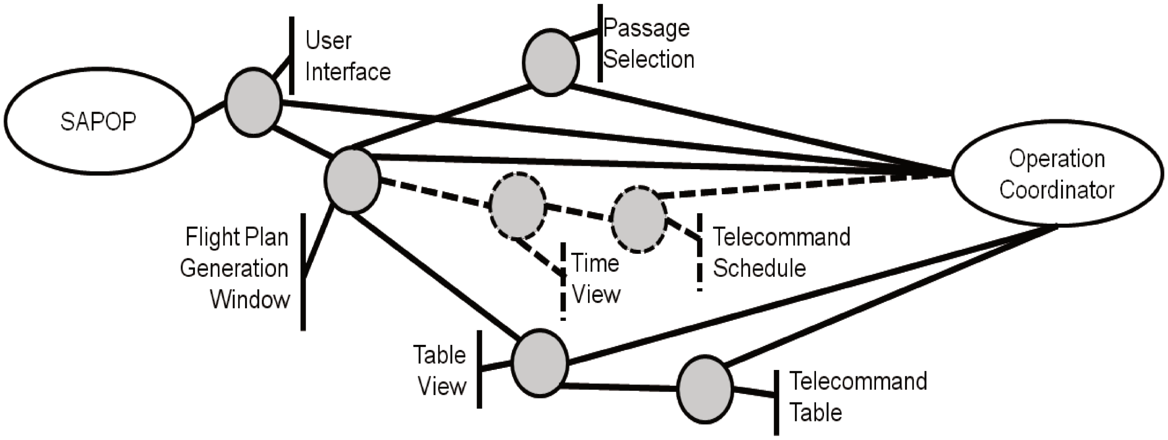


Figure 7.5: Fractal Model of Communication in Interaction Design Domain.

Table View consists on visualising the TCs in a table which is presented in the UI wireframe of SAPOP original version. The proposed wireframe provides also a Time View and tabs (as Figure 7.5 depicts) allowing changing the Table View to Time View, which represents another channel for the same information. If the user doesn't feel safe editing TCs in the Table View, the redundant channel Time View becomes active replacing the first channel.

In the SL, there is information about how to detect a hazard and also how to handle it in all six levels. As the SL applies to a specific channel, a hazard can be detected by a more generic channel. For example, if the user makes a mistake inverting the interaction order pressing button Up before selecting a checkbox in the Telecommands table, the SL for this button and for this checkbox don't have the information about how to detect this interaction error because each interaction object can just handle events in its region; events of other interaction objects can't be handled by this button. This interaction error is only detectable by the channel Flight Plan Generation Window because the scope of this channel, encompasses these two interaction objects (button Up and checkbox), allowing to detect this interaction error in the syntactic level.

Figure 7.6 depicts the window Flight Plan Generation with two views that the OC can switch by clicking on tabs Table View and Time View. To edit TCs in Table view, OC has a table with the TCs list, the start time, the experiment name and the user identification who added the TC. OC can use a checkbox for selecting a TC and can just change the order of selected TCs in the table (by clicking on the buttons Up and Down) or remove selected TCs (by clicking on button Remove).

In the Time View, which is a new view provided by the proposed SAPOP UI, OC has the chronology of TCs (a sequence of time is represented) with start time and end time. The TCs are placed according to the time that corresponds to Start Time column in Table View.

OC can change the order and remove hazardous TC selecting a line and after it, clicking a buttons Up, Down or Remove.

When OC finishes the work, to submit the edited TC sequence, OC clicks on button OK or cancels it by clicking on the Cancel button.

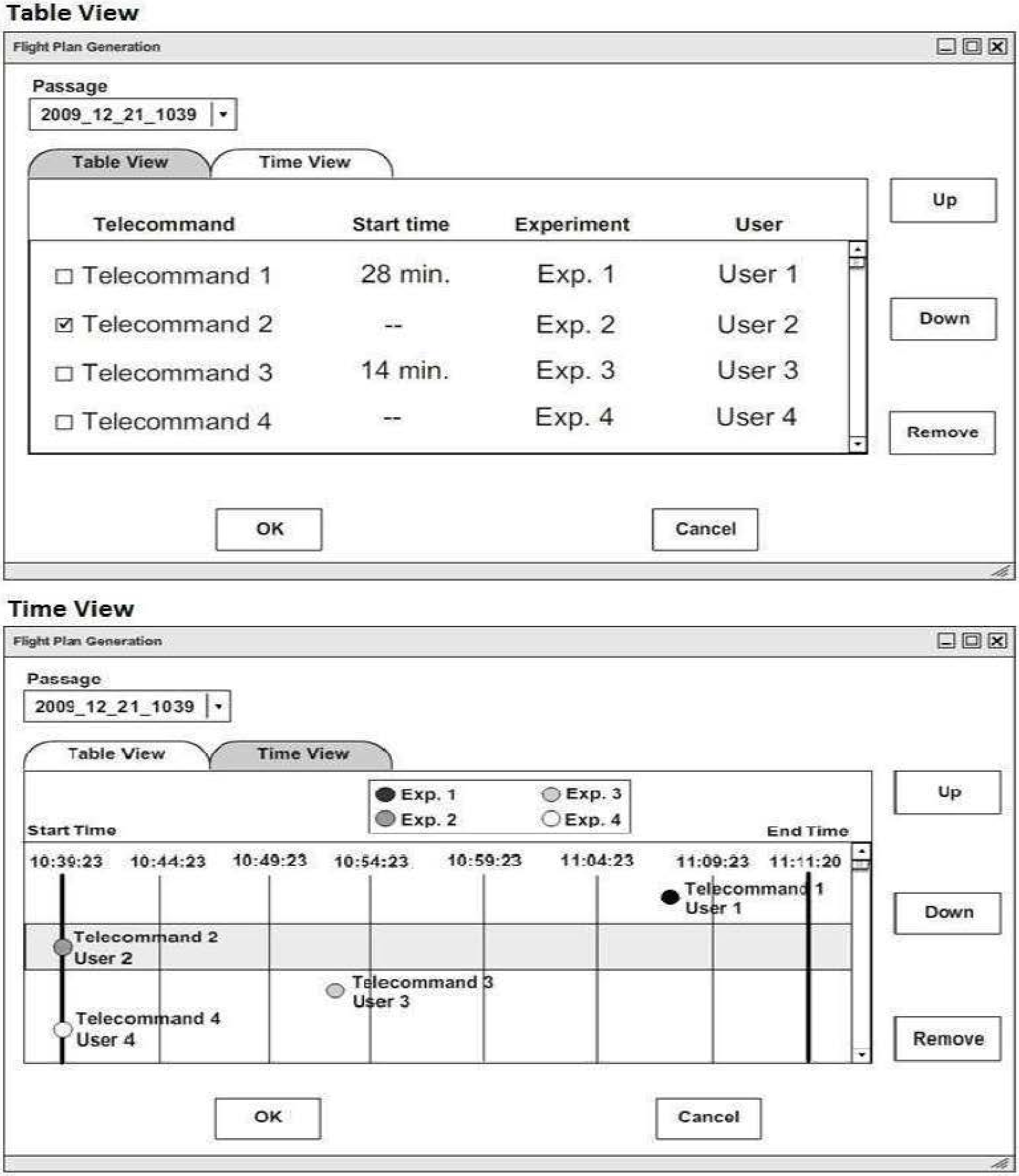


Table View

Flight Plan Generation

Passage: 2009_12_21_1039

Telecommand	Start time	Experiment	User
□ Telecommand 1	28 min.	Exp. 1	User 1
☑ Telecommand 2	--	Exp. 2	User 2
□ Telecommand 3	14 min.	Exp. 3	User 3
□ Telecommand 4	--	Exp. 4	User 4

Time View

Flight Plan Generation

Passage: 2009_12_21_1039

Figure 7.6: Wireframe for the Flight Plan Generation window.

After developing the FMC model and the SL artefacts, the UI designer should analyse all interaction channels verifying all SL layers. . The result is a verification whether a specific SL layer may fail. For example, if the user can´t understand the meaning of the Table View in the window Flight Plan Generation, it means that the Semantic layer of channel Telecommand Table failed. According to the SL definition, all upper levels are compromised by that failure. In the FMC model as Figure 7.5 depicts, the channel Telecommand Table considered as failed means all paths which passes through this channel are obstructed. Due to the redundancy strategy, there is another path through channel Time View. Therefore, in the case of Semantic layer failure of channel Table View, the Time View can be used.

SL artefacts are useful for determining if more redundancy is needed, verifying for all SL artefacts of all interaction channels whether they cover all possible user profiles defined for SAPOP. Although this analysis is time consuming for UI designers, it provides a complete analysis for the UI wireframes covering from technical contexts (physical world, empirical and syntactics) to human information contexts (semantics, pragmatics and social world). This broad view is necessary mainly for critical systems that need to be meticulously analysed.

7.5 Evaluating Safety with The Proposed Wireframe

Focusing on the scenario when OC is editing TC in the window illustrated by Figure 7.6, the proposed SAPOP UI has two representations (Time and Table views), with tabs for switching these views while the original UI has only the table view. This difference can be analysed based on concepts of the FMC model and the SL artefact. If the Table View fails by any reason related to the communication aspect (any SL layer, e.g. semantically, user cannot understand the meaning of information), the original UI doesn't provide any alternative solution for users because there is no other path to communicate from SAPOP to user. The proposed UI provides another path of communication for users through the channel Time View as Figure 7.5 depicts. In the concepts of the SL, the difference in the channels Table View and Time View are located at Semantic and Social layers because the signs were changed. The choice of other type of view provided by the redundant strategy is related to the user safety in choosing the communication channel involving the SL six levels. Moreover, this strategy doesn't impact users who prefer the table view (or any interaction objects of the original version) because it remains present on the proposed SAPOP UI. The redundancy allows the minimum impact for expert users (users who are already adapted to table view) or users with table familiarity and extends UI to a new category of users. The redundancy is not limited to the two options; it can be extended to include more users with different abilities.

The communication perspective with the redundancy strategy contributes for inclusive design underlying the FMC model. The UI designer can define safety strategies for the channels which involve critical information. The SL helps to define how this critical information is communicated to the users providing better situational awareness and either avoiding hazardous consequences.

The drawback of this communication perspective is the growing of the FMC model, which may be huge and complex because of the high complexity of the communicational structure. Developing all the artefacts is considered hard work because the number of agents and channels may be very extensive and, consequently, developing all SLs is also expensive. Visualization tools may allow the presentation of the model with a configurable filter to allow visualizing each fractal dimension separately, zooming in and out to show only the agents and channels needed for a specific consideration.

7.6 Conclusions

Communication is a fundamental factor to be addressed in critical systems. Semiotics provides a good foundation for analysis and design regarding communication. This paper proposed a procedure for focusing on interaction design based on artefacts of Organisational Semiotics combined with the Fractal Model of Communication (FMC). The case study involved the space system SAPOP, which provides support for scientific satellite payload operation. If it fails, satellite missions can be lost leading to high financial loss. This work presented a communication-based solution for interaction design, which uses redundancy as strategy to cope with the critical aspects of interaction with this system.

The FMC represents agents and channels of communication with unlimited fractal dimensions. In this way, the communication model can be presented in several granularity levels, including detailed information for each channel, with the six layers of communication analysis of the Semiotic Ladder (SL). The FMC and the SL provide support for designing the structure of communication containing information regarding the physical world, the empiric, syntactic, semantic, pragmatic and social aspects with potential hazards and correspondent actions. The procedure reaches the goal leading the FMC to the interaction design and to the identification of UI design problems of the SAPOP system. Due to communication perspective, the challenge for applying the redundancy strategy for interaction design was accomplished. Nevertheless, it may grow in complexity presenting many agents and channels making the reading difficult and demanding knowledge in several domain contexts.

The communication perspective may provide contributions to usability itself, because it is not only related to "easy to use", but also to "easy to communicate" providing users with better situational awareness and, consequently, diminishing the hazard possibilities related to “human (interaction) error”.

As further work, the UI proposed as a wireframe needs to be evaluated qualitative and quantitatively using other methodologies including those specialized in the critical system field.

Capítulo 8

Conclusão e Trabalhos Futuros

Sistemas críticos têm sido definidos como sistemas cuja falha provoca conseqüências inaceitáveis para a vida humana. A literatura tem relatado vários casos reais de falhas relacionadas à interação e comunicação entre pessoas e sistemas computacionais que levaram a perdas de vidas humanas. Com base na literatura, este trabalho apresentou vários problemas relacionados à interação e comunicação em sistemas críticos. Do ponto de vista metodológico, foram identificadas lacunas sobre a consideração de aspectos informais no desenvolvimento de sistemas de informação; é nessa camada de informação que são consideradas as crenças, sub-culturas, ou seja, os significados são definidos, as intenções são compreendidas, crenças são formadas e os compromissos com responsabilidades são estabelecidos. Foi visto também que a área de sistemas críticos demanda a inclusão desta camada além das camadas formais e técnicas, como a Figura 2.1 mostra.

Como a Semiótica é uma disciplina que permite foco na comunicação de forma explícita e, em particular a Semiótica Organizacional cobre todos os aspectos do design de sistemas de informação, esta foi considerada a base teórica e metodológica do trabalho.

A solução investigada para os problemas apontados na literatura envolveu a proposta de um modelo de processo baseado na Semiótica com foco principal em interação e comunicação. Este modelo de processo foi apresentado e discutido de forma situada no desenvolvimento de sistemas críticos nas fases de análise de requisitos, design e design de interação. O objetivo deste modelo de processo não foi substituir outros modelos de processos de desenvolvimento de software, mas sim, propor atividades que permitissem uma nova perspectiva ao desenvolvimento de sistemas de software (incluindo sistemas críticos): a da comunicação.

Estudos de caso acompanharam a apresentação do modelo nas várias fases. Na análise de requisitos, o estudo de caso considerado envolveu o projeto PAV focando especificamente uma parte de sistemas aviônicos de uma aeronave que oferece facilidades ao piloto de modo que não precise passar por pesados treinamentos de pilotagem (como ocorre nos dias de hoje). O modelo foi aplicado ilustrando a elicitação de requisitos e também a estrutura de comunicação do sistema auxiliando o analista a obter requisitos de comunicação que é a saída deste modelo nessa fase.

Para as fases de design e design de interação, foi apresentada uma aplicação prática do modelo para um sistema espacial - o SAPOP. SAPOP é um sistema que permite que um conjunto de usuários submeta uma seqüência de comandos a serem enviados para um satélite. Antes do envio, esta deve passar pela análise do usuário Coordenador de Operação que pode autorizar ou não o envio interagindo com a interface de usuário do SAPOP; uma sequência de comandos pode levar à perda da missão do satélite, ou seja, perda do custo financeiro bastante elevado - cerca de milhões de dólares dependendo do porte do projeto. Com o uso deste modelo em conjunto com a estratégia de redundância (bem conhecida em design de sistemas críticos), o modelo mostrou-se útil na detecção de problemas e na proposta de soluções. Na fase de design, problemas e soluções foram propostas no contexto do sistema crítico como um todo e na fase de design de interação, o foco foi somente na interação com o usuário.

Na literatura, não foi encontrado outro modelo de processo com foco em comunicação de forma explícita. Apesar de ser um modelo único, o que inviabiliza comparações, foi possível obter evidências de que essa perspectiva de comunicação é uma visão bastante útil à melhoria da qualidade do sistema crítico. Essa perspectiva permitiu detectar problemas e definir soluções que não foram visualizadas por outros modelos. A seguir apresentamos análises qualitativas nos resultados produzidos.

8.1 Análise do Modelo de Processo nos Resultados Produzidos

No estudo de caso SAPOP, tem-se o SAPOP proposto como resultado da utilização do modelo de processo. Podemos dizer que este apresenta melhor qualidade, pois evita ou diminui os riscos que levam a perigos, através de meios para contornar esses perigos nos aspectos de comunicação, que não foram tratados no SAPOP atual (versão do SAPOP sem a utilização do modelo de processo).

Os estudos de casos apresentados nos capítulos anteriores mostraram que as soluções propostas cobriram os seguintes aspectos:

- Apresentação – a estratégia de redundância é aplicada, ou seja, com o mesmo conteúdo de informação, mas apresentando-o ao usuário de forma diferenciada.

- Conteúdo de informação – para manter o usuário mais bem informado, foi proposta a adição de agentes que automatizam parcialmente algumas atividades do usuário retornando informações adicionais que apóiam as decisões durante operação.

- Organizacional – Adição de uma nova categoria de usuário, que analisa o trabalho feito por outro usuário. No caso do SAPOP, tem-se o usuário que checa os telecomandos autorizados pelo Coordenador de Operação (Operation Coordinator) para verificar se este cometeu algum erro na definição da seqüência de telecomandos a serem enviados.

8.1.1 Análise Baseada nos Artefatos da Semiótica

Utilizando modelos FMC que representam a comunicação do Coordenador de Operação com interfaces de usuário do SAPOP original e proposto, é possível visualizar os pontos críticos, considerá-los no caso de falha e definir caminhos alternativos para contornar essa falha. Por exemplo, no escopo de design de interação, a versão proposta provê maior segurança que a atual como mostra a Figura 8.1 que ilustra os dois modelos FMC onde o primeiro é relativo ao wireframe da interface do SAPOP original e o segundo, ao da interface proposta.

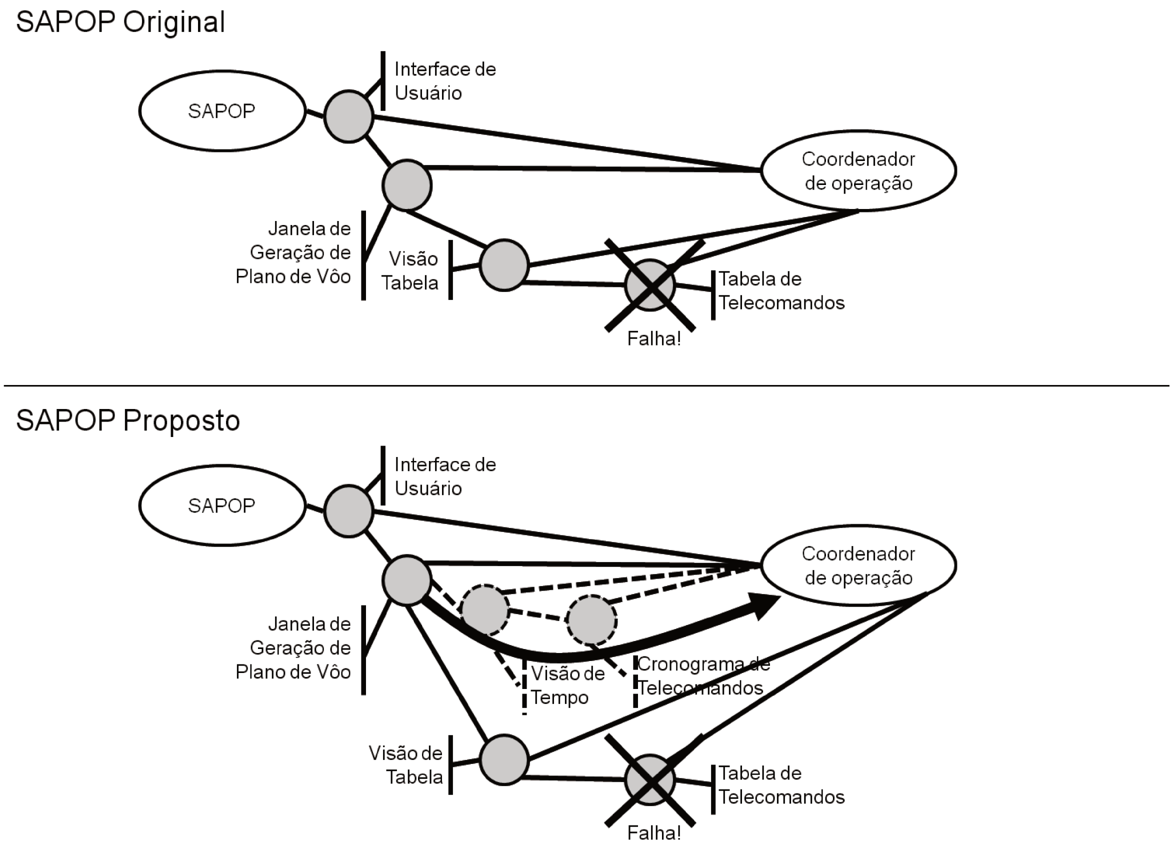


Figura 8.1: Análise Comparativa Entre SAPOP Original e Proposto

A Figura 8.1 mostra uma parte do modelo FMC que define a estrutura de comunicação relacionada à janela de geração de plano de vôo onde o usuário Coordenador de Operação interage. No caso da representação por tabela, representado pelo canal Tabela de Telecomandos, a tabela é um dos objetos de interação mais críticos, pois é o único canal com o qual o usuário interage para definir exatamente a seqüência de telecomandos; se esta comunicação falhar pode-se levar à perda do satélite. A falha de comunicação pode acontecer por razões enquadradas em pelo menos um dos seis degraus da Escada Semiótica; por exemplo, caso o usuário fique com dúvida ou não se lembre o que representa exatamente o valor da coluna Start Time (como mostra a Figura 7.6) no SAPOP original, o usuário não tem recurso alternativo sendo forçado a interpretações subjetivas. No SAPOP proposto, a alternativa é utilizar outra representação que é a visão de Cronograma utilizando o canal alternativo Cronograma de Telecomandos para definição de seqüência de telecomandos ou para, pelo menos, esclarecer dúvidas ocasionais do usuário. Essa mudança de visão é chaveada através de abas e pode ser feita em qualquer momento. Portanto, o SAPOP proposto oferece caminho alternativo de comunicação com o usuário focando exatamente no ponto crítico do SAPOP que é quando o Coordenador de Operação está definindo os telecomandos a serem enviados para o satélite.

8.1.2 Análise Baseada em Máquina de Estados

Para analisar o comportamento da interface do SAPOP, foi feita uma representação paralela em máquina de estados da versão atual e da versão proposta como mostra na Figura 8.2.

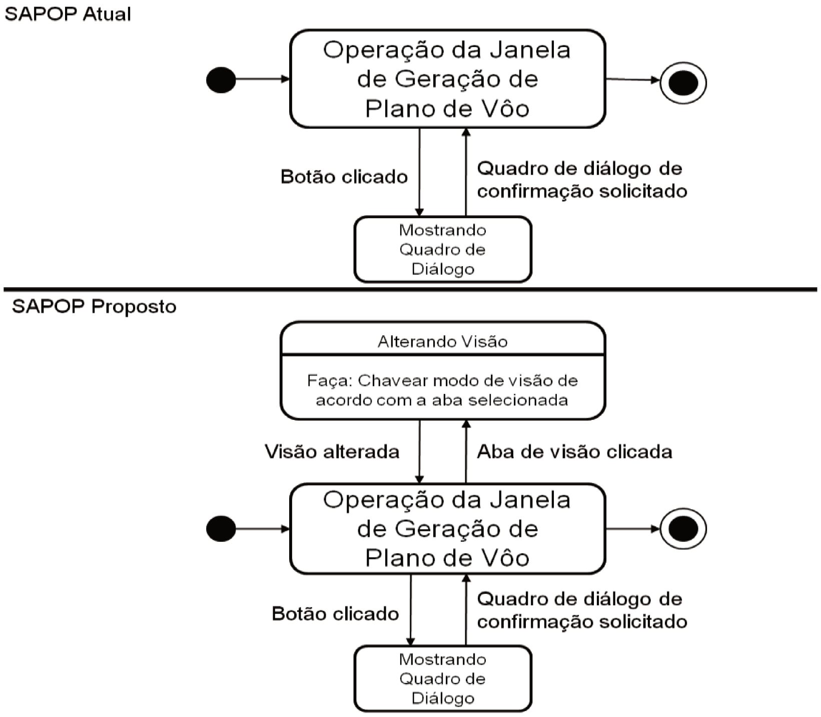

SAPOP Atual
Operação da Janela de Geração de Plano de Vôo
Botão clicado
Quadro de diálogo de confirmação solicitado
Mostrando Quadro de Diálogo
SAPOP Proposto
Alterando Visão
Faça: Chavear modo de visão de acordo com a aba selecionada
Visão alterada
Aba de visão clicada
Operação da Janela de Geração de Plano de Vôo
Botão clicado
Quadro de diálogo de confirmação solicitado
Mostrando Quadro de Diálogo

Figura 8.2: Máquina de Estados das Interfaces do SAPOP atual e proposto

Consideremos o seguinte cenário:

"O Coordenador de Operação, frente à janela de Geração de Plano de Vôo, precisa verificar um conjunto de grande quantidade de telecomandos que está sendo executado em paralelo. Na tabela de telecomandos, vê a coluna Start Time (tempo de início de execução de telecomandos temporizados) e o usuário precisa verificar quais telecomandos estão sendo executados em paralelo em um determinado intervalo de tempo."

No SAPOP original, o usuário precisa verificar linha a linha de uma tabela bastante extensa quais telecomandos estão programados para iniciar no intervalo de tempo sob consideração. No SAPOP proposto, o usuário tem a opção de selecionar a aba de visão para Time View levando para o estado Alterando Visão; lá o usuário poderá notar o tempo de início dos telecomandos na representação gráfica facilitando a visualização sobre tempos de inicio de execução dos telecomandos que estarão a bordo.

Na versão proposta a máquina de estados mostra ligeiramente mais robustez, pois possui “saída” das operações já existentes do SAPOP original (representada pelo super-estado “Operação da Janela de Geração de Plano de Vôo”); o usuário pode escapar do modo de operação atual para um outro estado que permite chavear o modo de visão indo para o estado “Alterando Visão”, que possibilita chavear modos de apresentação entre visão Tabela (Table View) e visão Tempo (Time View), como foi apresentado no capítulo 7. Portanto, se o usuário tiver algum problema na interação com uma visão dos objetos que são críticos, como ilustrado no cenário, no SAPOP proposto, o usuário tem a opção de saída deste modo de visão chaveando para outro modo de visão como não ocorre no SAPOP atual.

8.2 Contribuições

As contribuições apresentadas neste trabalho estão relacionadas a três áreas principais: Sistemas Críticos, Interação Humano-Computador e Semiótica, e estão listadas a seguir:

- Com base na revisão bibliográfica afim, não foram encontrados trabalhos com foco em comunicação de forma explícita na interação em sistemas críticos; também constatamos que há poucas contribuições na camada informal apresentada na cebola semiótica, para visão geral de sistemas de informação.

- Foi proposto o modelo de processo que utiliza Semiótica e Semiótica Organizacional para prover visão de comunicação em sistemas para elicitação e análise de requisitos de comunicação. O estudo de caso é um sistema de cockpit de uma aeronave.

- Foi proposta a modelagem e inspeção de uma interface com o usuário focando nos aspectos de comunicação utilizando a Semiótica como referencial teórico-metodológico. O estudo de caso utilizado foi o projeto Personal Air Vehicle (PAV), mais especificamente no display Synthetic Vision System (SVS).

- Foi proposta a modificação do artefato Quadro de Avaliação, adicionando uma coluna chamada "Recursos" que representa o recurso que um stakeholder deve utilizar ou possuir para resolução de problemas. Este novo artefato foi aplicado no estudo de caso PAV.

- Foi proposto o procedimento para refinamento do Modelo Fractal de Comunicação (MFC) reconhecendo que dimensões fractais levam a níveis de detalhamento da comunicação ilimitados. Estudo de caso foi aplicado no projeto PAV.

- Foi proposto o modelo de processo para a fase de design de sistemas críticos em conjunto com a estratégia de redundância utilizando vários artefatos da Semiótica focando em como a comunicação se realiza em um sistema crítico. Estudo de caso foi aplicado para o sistema espacial do Instituto Nacional de Pesquisas Espaciais (INPE) chamado Sistema de Apoio à Operação de Cargas Úteis de Satélites Científicos (SAPOP).

- Foi proposta a Escada Semiótica modificada para se adequar melhor ao escopo de sistemas críticos adicionando uma camada adicional de informação em cada nível, para obter informações dos perigos e ações contra esses perigos. Estudo de caso: SAPOP.

- Foi proposto o procedimento de filtragem do MFC para obter canais e agentes de interação. Estudo de caso: SAPOP.

- Foi proposto o modelo de processo para fase de design de interação em sistemas críticos utilizando artefatos da Semiótica em conjunto com a estratégia de redundância que permitem gerar um wireframe (estrutura de interface com o usuário) de um sistema crítico. Estudo de caso: SAPOP.

8.3 Considerações Finais e Trabalhos Futuros

A Semiótica mostrou-se um referencial teórico-metodológico fundamental para a perspectiva de comunicação durante as fases de requisitos e design de um sistema crítico como um todo. O modelo de processo apresentado neste trabalho mostrou ser possível também visualizar em um único modelo tanto a estrutura de comunicação no contexto organizacional como no técnico, conectados entre si mostrando dependências entre ambos os contextos, permitindo realizar uma análise de impacto mais abrangente. Em outras palavras, é possível obter informações causais de problemas ocorridos ou previstos do sistema de software percorrendo os modelos e artefatos baseados na Semiótica. Por exemplo, é possível avaliar se uma determinada falha de comunicação numa organização leva a uma falha de interação de sistema crítico.

Na fase de elicitação de requisitos, não se tem conhecimento de outros modelos que considerem aspectos de comunicação no domínio de sistemas de informação de forma tão explicita. Os artefatos e métodos da Semiótica representaram uma contribuição guiando os analistas a obterem os requisitos com cenários que consideram o que o sistema deve fazer se uma determinada comunicação falhar. Essa abordagem possibilita antecipar diferentes falhas de comunicação em vários níveis de detalhamento graças ao recurso que o FMC oferece. O Modelo Fractal de Comunicação pode contribuir inclusive no sistema sócio-técnico revelando novas conexões de comunicação, e conseqüentemente, novas soluções e desafios.

A Figura 6.4 ilustra como o modelo de processo foi desenhado a partir de artefatos da Semiótica e aplicando-os no desenvolvimento de software. Entretanto, vale ressaltar que a Engenharia de Software também sofre influência da implantação do modelo de processo, por exemplo, obtendo mais requisitos (relacionados à comunicação). Para obtenção destes requisitos, o processo de desenvolvimento de software deverá ser alterado e isto contribui a obtenção de novos significados, novas culturas, novas crenças, novas intenções, novas possibilidades que podem realimentar o modelo de processo.

De acordo com o conceito da Escada Semiótica, foi visto que as camadas superiores dependem das inferiores para que se realize a comunicação. Não só as camadas superiores são influenciadas pelas inferiores mas também no sentido oposto, ou seja, as superiores podem influenciar as inferiores. Por exemplo, se no mundo social um compromisso se firmou, novas intenções de comunicação serão estabelecidas (aspecto pragmático), conseqüentemente, novos significados serão construídos e assim por diante até alcançar a camada do mundo físico.

A Escada Semiótica também pode ser estendida para além do seu conceito básico. Por exemplo, a camada Sintática poderia ser sub-dividida em camada Léxica e Gramatical e a camada Semântica, em Sinonímia, Antonímia e Polissemia. A Escada Semiótica poderia ter mais camadas ou menos camadas dependendo do contexto; algumas camadas poderiam ser omitidas e outras detalhadas, com mais sub-divisões adaptando-se melhor ao cenário em análise, quando se necessita de mais ou menos detalhes na definição da comunicação.

Esta pesquisa certamente não se esgota no apresentado; é importante mencionar as limitações do estudo e caminhos de continuidade possíveis. A complexidade inerente à categoria de sistemas tratados – críticos, bem como a dificuldade de experimentação com tais sistemas certamente limitam a verificação do alcance dos resultados. Ainda, a proposição de um modelo de processo para o design da interação em sistemas críticos como proposto, extrapola os aspectos de interface de usuário propriamente dita, forçando à consideração do design do sistema como um todo, como preconiza a Semiótica Organizacional. A perspectiva da comunicação como base desse modelo de processo, que se mostrou factível e útil em estudos de caso pontuais, precisaria ganhar escala e para tal, o modelo não pode prescindir de ferramentas para suporte às atividades, especialmente para uso do FMC. Todos estes aspectos identificam outros trabalhos futuros que poderão estender esta pesquisa:

1. Apesar do modelo de processo ter sido aplicado em dois casos em áreas distintas (espacial e aviação), isto ainda não é suficiente para comprovar que este se aplica para todos os domínios cobertos pelos sistemas críticos. Uma proposta para trabalhos futuros é aplicar para mais casos reais de sistemas críticos em áreas distintas contribuindo no aprimoramento deste modelo de processo.

2. Tipicamente, o modelo FMC quando aplicado a um caso específico se torna um modelo bastante extenso dificultando a sua leitura. O desenvolvimento de ferramentas seria útil oferecendo as seguintes funcionalidades:

   2.1. Prover navegação, filtragens de agentes/canais e visualização de vários níveis de detalhamento resultantes do procedimento de refinamento.

   2.2. Permitir preenchimento de informações da escada semiótica para todos os canais do modelo.

   2.3. Prover integração com técnicas de análise de erros humanos, como, por exemplo, Kletz (1997), que fez um trabalho baseado na técnica Hazard and Operability (HAZOP).

   2.4. Destacar caminhos críticos e caminhos alternativos (redundantes) como mostra a Figura 8.3.

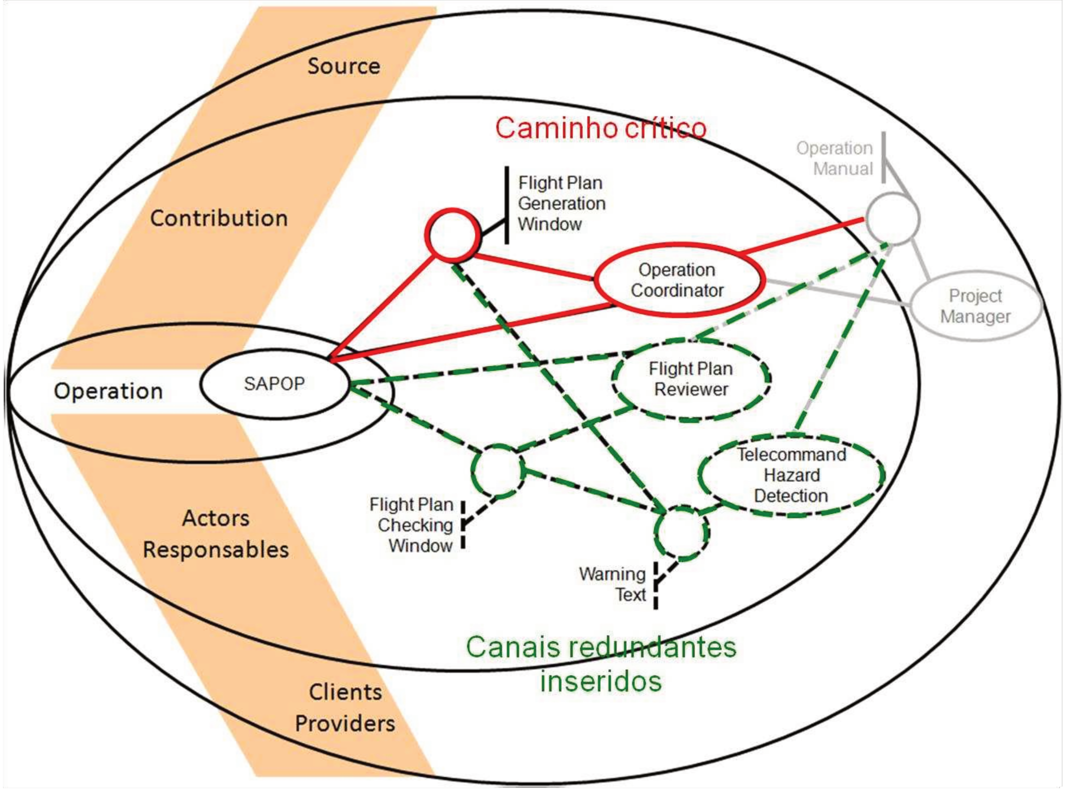


Figura 8.3: Representações de caminhos críticos e redundantes

3. Investigar se o modelo de processo pode atuar em mais fases de desenvolvimento de sistemas incluindo implementação e testes, ou seja, verificar se é possível (e útil) detalhar ainda mais chegando ao ponto de visualizar contextos de implementação (classes, métodos, funções) e, na fase de testes, o modelo poderia fornecer como recursos ferramentais para realização de testes.

4. No design da interação, este trabalho alcançou o desenvolvimento de wireframes de interfaces de usuário. A proposta é estender este estudo para questões de usabilidade, navegabilidade de janelas e até mesmo, a questões de acessibilidade no desenvolvimento dessas interfaces. Em síntese, a perspectiva de comunicação pode contribuir para a usabilidade, porque esta não só está relacionada ao atributo "fácil de usar", mas também "fácil de se comunicar", oferecendo aos usuários uma maior consciência situacional e, potencialmente, diminuindo as possibilidades de riscos relacionados ao "erro humano ou de interação".

5. Aplicar o modelo de processo em todas as fases de desenvolvimento de um sistema crítico. Este trabalho focou na análise de requisitos e modelagem, que foram aplicadas no PAV como estudo de caso e nas fases de design e design de interação,

foram aplicadas no SAPOP. Idealmente, o modelo de processo poderia ser aplicado em um estudo de caso passando por todas as fases de desenvolvimento de software.

APÊNDICES

Apêndice I

Artefatos para Display SVS

Este apêndice apresenta um artefato resultante após a execução do método PAM para o caso de display Synthetic Vision System (SVS) como mostra a Figura I.1.

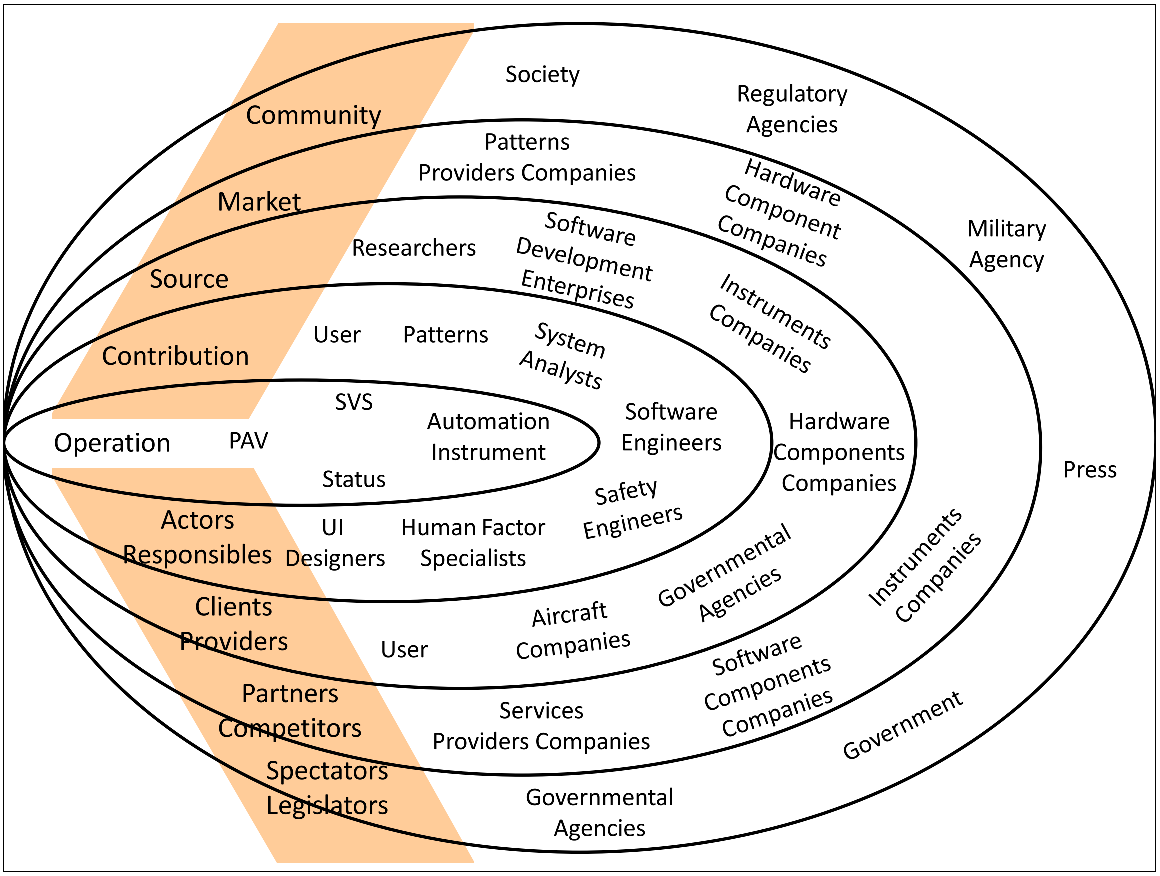


Figura I.1: Modelo PAM de um display SVS

A Figura I.2 mostra o modelo FMC do sistema de display SVS como um todo. Os nós em branco representam os agentes e canais resultantes após da execução do procedimento de refinamento. Os agentes e canais em cinza representam agentes que são stakeholders que foram levantados durante a execução do método PAM.

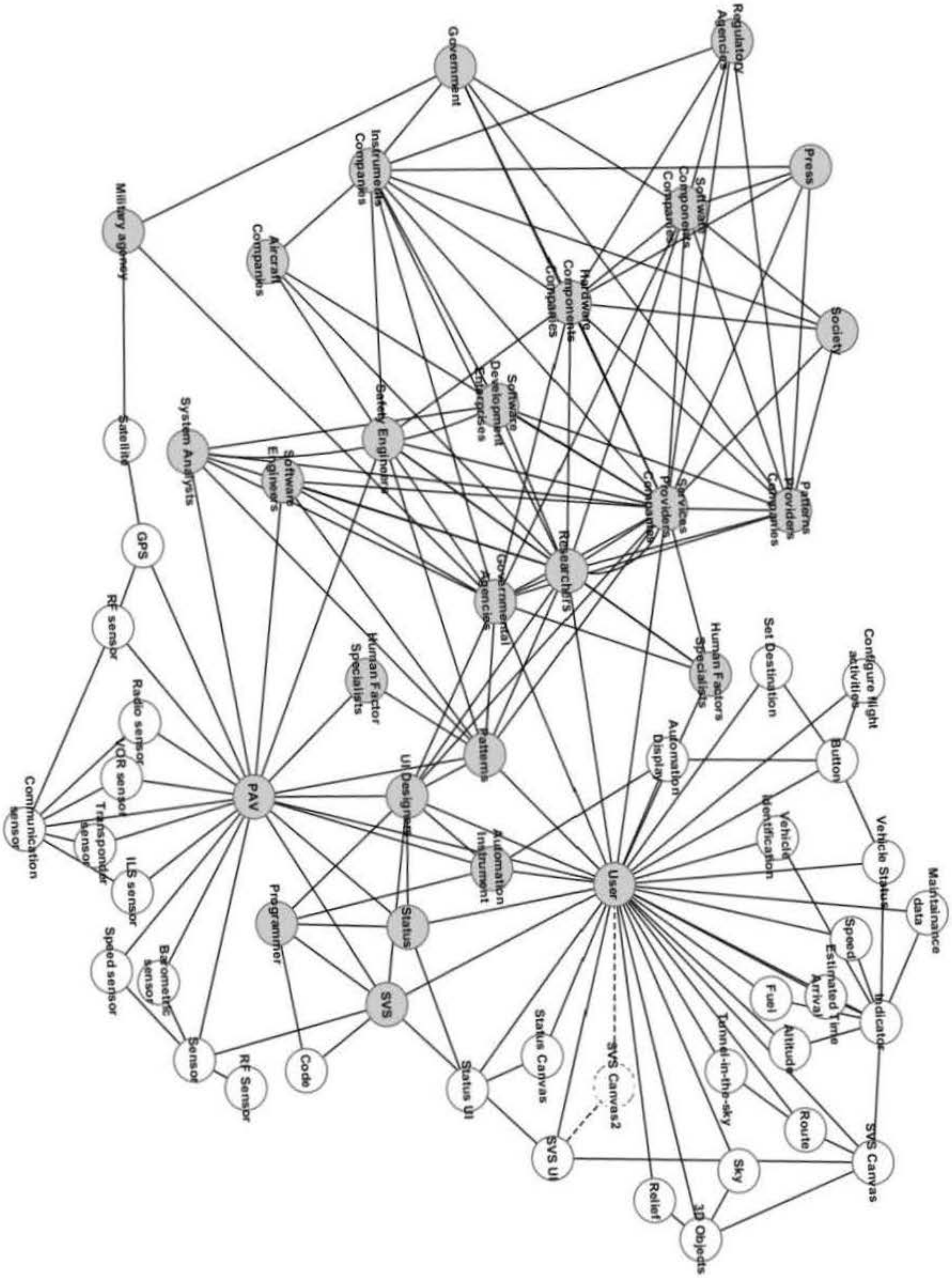


Figura I.2: Modelo FMC de um display SVS

Apêndice II

Artefatos do SAPOP

Neste apêndice, tem-se a estrutura do modelo FMC detalhado gerado após procedimento de refinamento a partir do modelo FMC de alto nível, ou seja, composto por somente agentes como stakeholders. Na Figura II.1, há duas ramificações de refinamento do modelo onde a primeira ramificação consiste na execução do procedimento de refinamento a partir do canal entre SAPOP e o usuário obtendo objetos de interação. A segunda ramificação foi feita a partir do canal entre SAPOP e stakeholders que fazem parte do time de desenvolvimento de software resultando agentes e canais envolvidos no desenvolvimento de software de uma organização. A Figura II.1 ilustra como o modelo FMC do SAPOP se tornou um modelo bastante extenso para representar alguns domínios de um sistema de informação.

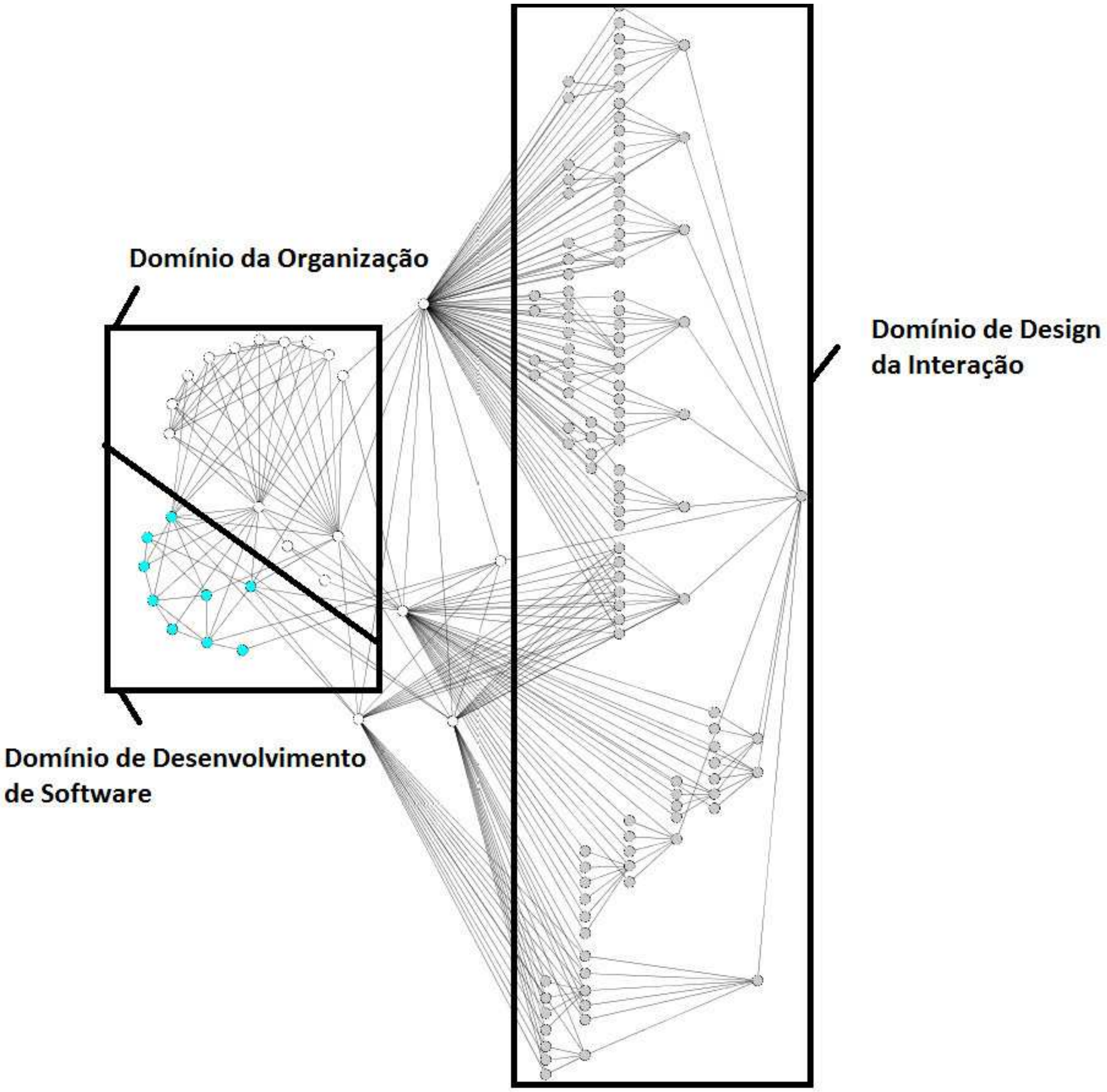

Domínio da Organização
Domínio de Design da Interação
Domínio de Desenvolvimento de Software

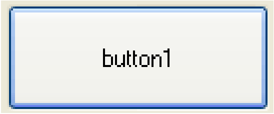
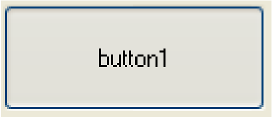
Figura II.1: Modelo FMC do SAPOP

A Figura II.1 também ilustra um único modelo representando elementos do domínio da organização (agentes e canais do nível de stakeholders) conectado ao domínio técnico (agentes do modelo que não pertencem ao grupo de stakeholders).

As Tabelas II.1, II.2 e II.3 representam as Escadas Semióticas de alguns canais de interação que são: Botão, Texto e Tabela de Telecomandos para ilustrar como as Escadas Semióticas podem manter bastante informação sobre a comunicação dos canais.

Tabela II.1: Escada Semiótica do canal Botão

Escada Semiótica	
Canal: Botão	
Camada	Como a comunicação é realizada?
Mundo Físico	O display é o dispositivo físico que exibe o botão como um conjunto de pixels
Perigos no mundo físico	Perigo 1: Display falha com tela preta Ação 1: Sem ação por ser um problema genérico e de difícil detecção. Fora do escopo da aplicação; A aplicação não controla o display no mundo físico, este é controlado somente pelo sistema operacional.
Empírico	Botão atua independentemente podendo ser pressionado mais de uma vez. Resolução do display é 1024x768, o suficiente para exibir botão claramente.
Perigos no Empirico	Perigo 1: Se o botão é pressionado várias vezes e o evento do botão foi tratado várias vezes Ação 1: Implementar um mecanismo para detectar esse perigo. Enquanto o evento não tiver processado, o botão deve aparecer como "pressionado" até que o tratamento finalize e o botão retorne para o estado liberado.
Sintática	O botão é estruturado da seguinte forma: a aparência deve ser uma metáfora de um botão real, possuindo uma borda e uma parte retangular que pode estar um nível acima da borda (quando liberado) ou abaixo da borda (quando pressionado) Favor, veja a figura abaixo a aparência do botão:

	 Botão pressionado  Botão liberado O mecanismo consiste em quando pressionado, o sinal é enviado. Quando liberado, o botão retorna ao estado original. Todos os botões devem possuir um rótulo. Cor do botão tem que ser diferente da cor de fundo tornando visíveis pelo usuário.
Perigo na Sintática	Perigo 1: Alguma parte do botão está faltando Ação 1: Detectar essa anormalidade é difícil por causa da limitação do sistema operacional. Isso pode ser testado em um laboratório de testes. Estudo de viabilidade deve ser realizado. Perigo 2: Se o botão não apresentar como pressionado quando for clicado pelo usuário. Ação 2: Criar um mecanismo que monitora um mecanismo (similar ao watchdog) para detectar este problema (capturar o evento de clique e obter a posição clicada para determinar se o clique ocorreu na região do botão. Se o botão não enviar o evento, então este mecanismo de detecção deve notificar ao sistema o comportamento anormal do botão. Perigo 3: Quando o botão deve ser liberado mas não apresenta ao usuário como um botão liberado. Ação 3: Pode aplicar o mesmo mecanismo da Ação 2.

	Implementar watchdog. Perigo 4: Se o botão foi clicado mas o sinal não for enviado. Ação 4: O mesmo da Ação 2. Implementar watchdog Perigo 5: Não há rótulo no botão Ação 5: Ver comentário da Ação 1 Perigo 6: Se o botão não tiver visível Ação 6: Obter se a cor definido para o botão é a mesma do cor de fundo. Se for igual, mudar a cor do botão.
Semântica	A representação gráfica do botão é uma metáfora do botão real simulando a sua ação através de um sistema de iluminação. Quando liberado, o botão é mais claro porque o nível retangular do botão está iluminado mas quando o botão está pressionado, ele apresenta mais escuro simulado que a parte retangular está na sombra causada pela borda do botão. Todos os botões têm um rótulo que representa uma ação do botão.
Perigos na Semântica	Perigo 1: O usuário pode não interpretar que o objeto é um botão Ação 1: Para detectar este problema, teste de usabilidade deve ser feito. Isso pode até ser detectado computacionalmente quando for possível detectar reações inesperadas do usuário. Ao detectar esse problema, o sistema pode mudar a aparência do botão. Perigo 2: Usuário não pôde interpretar o rótulo do botão. Ação 2: Ver comentário da Ação 1. Ao detectar esse problema, o sistema pode mudar o rótulo do botão quando este for exibido ou apresentar um tooltip para fornecer mais informações para o usuário.
Pragmática	A presença do botão e do seu nome indica a intenção do botão, ou seja, disparar uma ação.
Perigos na Pragmática	Perigo 1: O usuário não entende a razão do aparecimento de um botão específico. Ação 1: O design de interação deve ser analisado. Perigo 2: O usuário não tem noção do que o sistema fará se

	o botão for pressionado. Ação 2: O design de interação deve ser analisado.
Mundo Social	O botão age como botão no mundo real e ele pode ser pressionado usando o clique do mouse. O nome do botão representa o nome da ação ou intenção.
Perigos no Mundo Social	Perigo 1: Usuário não conhece o botão real para interpretar a metáfora. Ação 1: Conhecer mais sobre o mundo real do usuário para encontrar outro objeto de interação que substitua um botão. Perigo 2: De acordo com a cultura do usuário, o nome do botão ofende o usuário. Ação 2: Conhecer mais sobre o mundo real do usuário para encontrar outro nome para o botão. Perigo 3: O usuário pode não ter conhecimento sobre o nome do botão ou de uma intenção. Ação 3: Conhecer mais sobre o mundo real do usuário para encontrar outro nome para o botão.

Tabela II.2: Escada Semiótica do canal Texto

Canal: Texto	
Camada	Como a comunicação é realizada?
Mundo Físico	Display mostra o texto como um conjunto de pixels
Perigos no mundo físico	Perigo 1: Display falha com tela preta Ação 1: Sem ação por ser um problema genérico e de difícil detecção. Fora do escopo da aplicação; A aplicação não controla o display no mundo físico, este é controlado somente pelo sistema operacional.
Empírico	Resolução do display é 1024x768 que é bastante para exibir botão claramente.
Perigos no Empirico	Perigo: Se o display estiver numa resolução abaixo de 1024x728.

	Ação: Recalcular se o texto pode ser truncado e as fontes podem ser redimensionadas. Posição e o tamanho devem ser recalculados.
Sintática	É um texto não interativo. Ele deve comunicar ao usuário informando que este não é interativo. O texto deve utilizar a fonte Arial tamanho 12 como tamanho mínimo.
Perigo na Sintática	Perigo: Se o texto for muito pequeno para usuário (menor que 12) Ação: O sistema deve prover facilidade de definir o tamanho mínimo da fonte. Testador deve detectar esse problema e se tiver problema, solicitar mudança do software.
Semântica	O texto deve ser escrito no vocabulário usado pelos investigadores, coordenador de operação, administradores de sistemas e operador de subsistemas.
Perigos na Semântica	Perigo: O usuário não foi capaz de entender o significado do texto apresentado. Ação: Prover ajuda (glossário) ou prover recursos de tooltip para explicar um termo específico.
Pragmática	Texto é para identificar qualquer objeto de interação (rotular objetos de interação) ou simplesmente transmitir uma informação útil no formato de um texto para usuário.
Perigos na Pragmática	Perigo: Se o texto está adicionado mas não para identificar um objeto de interação e nem para transmitir informações úteis. Ação: Rever a especificação de design de interação para identificar qual a intenção do texto e fazer devidas correções.
Mundo Social	O texto, na cultura do usuário, deve ser interpretado como vocabulário ativo.
Perigos no Mundo Social	Perigo: O usuário não entende ou sente ofendido com a palavra ou sentença apresentada. Ação: Conhecer a cultura do usuário e refazer a sentença ou palavra.

Tabela II.3: Escada Semiótica do canal Tabela de Telecomandos

Canal: Tabela de Telecomandos	
Camada	Como a comunicação é realizada?
Mundo Físico	Display mostra o texto como um conjunto de pixels
Perigos no mundo físico	Perigo 1: Display falha com tela preta Ação 1: Sem ação por ser um problema genérico e de difícil detecção. Fora do escopo da aplicação; A aplicação não controla o display no mundo físico, este é controlado somente pelo sistema operacional.
Empírico	Resolução do display é 1024x768 que é bastante para exibir botão claramente.
Perigos no Empirico	Perigo: Se o display estiver numa resolução abaixo de 1024x728. Ação: Recalcular a tabela para ser apresentada de forma mais legível possível tanto na posição quanto no tamanho.
Sintática	A tabela é composta por 3 colunas: nome do telecomando, parâmetros e tempo. Número de linhas não tem limite.
Perigo na Sintática	Perigo 1: Problemas de layout Ação 1: Recalcular o layout Perigo 2: Dados inconsistentes ou vazios na tabela. Ação 2: A funcionalidade para validar os dados deve ser implementada. Se tiver erro, os procedimentos de preenchimento de tabela devem ser re-executados. Se o problema persistir, exibir erro.
Semântica	As linhas devem ter informações claras e concisas de acordo com as colunas da tabela.
Perigos na Semântica	Perigo: Se o significado dos valores causar problemas de interpretação Ação: Todos os valores da tabela devem ser testados com usuários reais.
Pragmática	A intenção é listar todos os telecomandos entrados pelos

	investigadores e operadores de sub-sistemas.
Perigos na Pragmática	Perigo: A tabela foi usada para uma outra intenção Ação: Análise de especificação de design da interação deve ser analisada e validada.
Mundo Social	A coluna "Tempo" deve ser adaptada para cada país, cultura, pois cada país utiliza padrões diferentes.
Perigos no Mundo Social	Perigo 1: Usuário pode se confundir na leitura de datas no formato diferente do país. Ação 1: O sistema deve verificar a localização do sistema utilizado pelo usuário e se configurar de acordo com o padrão correto. Perigo 2: Por ser um sistema Web, fuso horário pode estar errado Ação 2: Utilizar fuso horário relativo ao horário do Meridiano de Greenwich (GMT).

Apêndice III

Autorizações de Publicação

AUTORIZAÇÃO DOS ARTIGOS DAS CONFERÊNCIAS ICOS E ICISO

De: "Kecheng Liu" <k.liu@henley.reading.ac.uk>

Assunto: RE: Permission to reprint the copyrighted papers in my Ph.D thesis

Data: Seg, Junho 28, 2010 4:24 pm

Para: ra946056@ic.unicamp.br

You are permitted to reprint the papers mentioned provided you make proper references and citations.

All the best

Kecheng Liu

Professor Kecheng Liu, Director,
Informatics Research Centre, University of Reading
Ground Floor, Building 42
Whiteknights
Reading RG6 6WB
United Kingdom
Tel: +44 118 378 8614, Fax: +44 118 378 4421
email: k.liu@henley.reading.ac.uk; k.liu@reading.ac.uk;
IRC website: www.reading.ac.uk/irc

-----Original Message-----

From: ra946056@ic.unicamp.br [mailto:ra946056@ic.unicamp.br]

Sent: Fri 25/06/2010 13:50

To: iciso@reading.ac.uk

Subject: {Spam?} Permission to reprint the copyrighted papers in my Ph.D thesis

Dear Sirs,

In the forthcoming months I will defend my Ph.D. in Computer Science in the Institute of Computing at University of Campinas (IC/UNICAMP). For this reason I send this email in order to request the permission from ICOS/ICISO to incorporate (reprint) papers that were published in proceedings of ICOS 2007, ICISO 2009 and ICISO 2010 conferences in my Ph.D. dissertation. Papers mentioned in this mail are listed below:

"Interaction Design and Redundancy Strategy in Critical Systems"
Marcos Salenko Guimarães, M. Cecilia C. Baranauskas and Eliane Martins
12th International Conference on Informatics and Semiotics in
Organisations, ICISO, 2010.

"A Case Study on Modelling the Communication Structure of Critical Systems"
Marcos Salenko Guimarães and M. Cecilia C. Baranauskas
11th International Conference on Informatics and Semiotics in
Organisations, ICISO, 2009.

"A Communication-based Approach to Requirements Elicitation for
Safety-Critical Systems"
Marcos Salenko Guimarães, M. Cecilia C. Baranauskas and Eliane Martins
10th International Conference on Organisational Semiotics, ICOS, 2007

Sincerely,

Marcos Salenko Guimarães

AUTORIZAÇÃO DOS ARTIGOS DAS CONFERÊNCIAS ICEIS

De: "ICEIS Secretariat" <iceis.secretariat@insticc.org>

Assunto: RE: [Fwd: Permission to reprint the INSTICC copyrighted papers in my Ph.D thesis]

Data: Qua, Julho 28, 2010 7:27 pm

Para: ra946056@ic.unicamp.br

Prezado Marcos Salenko Guimarães,

De facto não recebi o seu primeiro email e espero que a minha resposta não seja tardia.

Relativamente à questão colocada, venho por este meio dar permissão para fazer o "reprint" desses 2 artigos na sua tese de doutoramento.

Cumprimentos,

Vitor Pedrosa

-----Original Message-----

From: ra946056@ic.unicamp.br [mailto:ra946056@ic.unicamp.br]

Sent: segunda-feira, 12 de Julho de 2010 22:13

To: secretariat@iceis.org; iceis.secretariat@insticc.org

Subject: [Fwd: Permission to reprint the INSTICC copyrighted papers in my

Ph.D thesis]

Dear Sirs,

I would like to know if you received this mail below (sent on June, 25th, 2010) because my university requires a written permission (e-mail, letter, or fax) from the publisher. Please, I'd like to kindly ask you to respond to my mail below. If I sent to wrong contact, please indicate me a person to whom I can send this request.

Counting with your support, I thank you in advance.

Sincerely,

Marcos Salenko Guimarães.

-------------------------- Mensagem Original ---------------------------

Assunto: Permission to reprint the INSTICC copyrighted papers in my Ph.D
thesis

De: ra946056@ic.unicamp.br

Data: Sex, Junho 25, 2010 9:28 am

Para: iceis.secretariat@insticc.org

Dear Sirs,

In the forthcoming months I will defend my Ph.D. in Computer Science in the Institute of Computing at University of Campinas (IC/UNICAMP). For this reason I send this email in order to request the permission from INSTICC to incorporate (reprint) papers that were published in proceedings of ICEIS 2007 and ICEIS 2008 conferences into my Ph.D. dissertation.

Papers mentioned in this mail are listed below:

"Interaction in Critical Systems: Conquests and Challenges"

Marcos Salenko Guimarães, M. Cecilia C. Baranauskas and Eliane Martins

9th International Conference on Enterprise Information Systems, INSTICC
Press.

"Communication-Based Modelling and Inspection in Critical Systems"

Marcos Salenko Guimarães, M. Cecilia C. Baranauskas and Eliane Martins

10th International Conference on Enterprise Information Systems, INSTICC
Press.

Sincerely,

Marcos Salenko Guimarães

Referências Bibliográficas

Aith M., Portela F., Duailibi J., 2007. A Tragédia, Segundo as Caixas-Pretas. Revista Veja, Edição número 2019, ano 40, no. 30, Editora Abril.

Allen M. J., 2007. Guidance and Control of an Autonomous Soaring UAV. In *NASA Technical Memorandum*, NASA/TM-2007-214611, NASA.

Avizienis A., Laprie, J., and Randell B., 2001. Fundamental Concepts of Dependability. *Research Report N01145*. http://www.cert.org/research/isw/isw2000/papers/table_of_contents.html, visitado em 16 de Novembro de 2006.

Baker, L., Beyer, H., Holtzblatt, K., 2004. An Agile Customer-Centered Method: Rapid Contextual Design. *Proceedings of XP Agile Universe*, http://www.incontextdesign.com/resource/pdf/XPUniverse2004.pdf, visitado em 10 de Maio de 2006.

Baranauskas, M. C. C., Salles J., Liu K., 2002. Analysing Communication in the Context of a Software Production Organisation. *4th International Conference on Enterprise Information Systems*, 202-209. Kluwer Academic Publishers.

Baranauskas, M. C. C., Schimiguel, J., Simoni, C. A. C., Medeiros C. M. B., 2005. Guiding the Process of Requirements Elicitation with a Semiotic Approach. (3) 100-111. *The 11th International Conference on Human-Computer Interaction*. Lawrence Erlbaum Ass. Inc.

Barboni, E., Navarre D., Palanque P., Basnyat S., 2007. A Formal Description Technique for the Behavioural Description of Interactive Applications Compliant with ARINC Specification 661. *IEEE Second International Symposium on Industrial Embedded Systems - SIES'2007*. Special Session on Behavioural Models for Embedded Systems, Hotel Costa da Caparica, Lisbon, Portugal, 4-6 July.

Basnyat, S., Palanque, P., Schupp, B., Wright, B.P., 2007. Formal Socio-technical Barrier Modelling for Safety-critical Interactive Systems Design. *Safety Science*, Vol 45, Issue 5, June 2007, ISSN: 0925-7535.

Basnyat, S., 2006. A multi-perspective approach for the design of error-tolerant socio-technical safety-critical interactive systems. *Resilience for Survivability in Information Society Technologies (ReSIST) European Network of Excellence Student Seminar*. 5-7 September 2006, Centro Studi "I Cappuccini", Italy.

Basnyat, S., Palanque, P., 2006. A Barrier-based Approach for the Design of Safety Critical Interactive Application. *ESREL 2006 Safety and Reliability for Managing Risk. Safety and Reliability Conference*. Balkema (Taylor & Francis) 18-22 September, Estoril, Portugal.

Baxter, G., Besnard, D., 2004. Cognitive Mismatches in the Cockpit: Will They Ever Be a Thing of the Past? *The Fight deck of the Future: Human Factors in Data links and Free flight conference.* University of Nottingham Press.

Billings C. E., 1996. Human-Centered Aviation Automation: Principles and Guidelines. NASA Technical Memorandum 110381. NASA.

Bonacin, R., Simoni, C.A.C, Melo, A.M., Baranauskas M.C.C., 2006. Organisational Semiotics: Guiding a Service-Oriented Architecture for e-Government. *9th International Conference on Organisational Semiotics*, pp 47-58.

Browne, G., Rogich, M., 2001. An Empirical Investigation of User Requirements Elicitation: Comparing the Effectiveness of Prompting Techniques. *Journal of Management Information Systems*, (4) 223-249.

Card, S. K., Moran, T. P. and Newell, A., 1983. *The Psychology of Human-Computer Interaction*. Hillsdale, NJ: Lawrence Erlbaum Associates.

Cafe, Cafe Foundation, 2007. Personal Air Vehicle. http://cafefoundation.org/v2/pav_home.php, visitado em 27 de Janeiro de 2007.

Cantanhêde E., 2007. Fitas Revelam Erros na Queda de Avião. Folha de São Paulo, ano 86, n^{o}. 28.445.

Carver L. and Turoff M., 2007. Human-Computer Interaction: The Human and Computer as a Team in Emergency Management Information Systems. *Communications of the ACM, Vol. 50. No. 3*. ACM Press.

Connelly, S., Burmeister, J., MacDonald, A., Hussey, A., 2001. Extending and Evaluating a Pattern Language for Safety-Critical User Interfaces. *SCS´01, 6th Australian Workshop on Safety Critical Systems and Software.* Australian Computer Society, Inc.

Cordeiro, J., Filipe, J., 2004. The Semiotic Pentagram Framework - A perspective on the use of Semiotics within Organisational Semiotics. *Proceedings of the 7th International Workshop on Organisational Semiotics*, 249-265.

Daouk, M., Leveson, N. G., 2001. An Approach to Human-Centered Design. *Workshop on Human Error and System Development*. http://web.mit.edu/hfes/www/Research.htm, visitado em 24 de Outubro de 2006.

Dewsbury, G., Clarke, K., Hughes, J., Rounce, M., Sommerville, I., 2003. Designing Dependable Digital Domestic Environments. *HOIT 2003, The Networked Home of the Future Conference*. http://www.crito.uci.edu/noah/HOIT/2003papers.htm, visitado em 17 de Março de 2005.

Domino D. A., 2006. Concept of Operations for the Use of Synthetic Vision System (SVS) Display During Precision Instrument Approach. *Tech paper of MITRE*. http://www.mitre.org/work/tech_papers/ tech_papers_07/06_1230/06_1230.pdf, visitado em 11 de Outubro de 2007.

Fields R., 2001. Analysis of Erroneous Actions in the Design of Critical Systems. *PhD dissertation*. Human Computer, Interaction Group, Department of Computer Science. University of York, 2001.

Fields, R., Paternò, F., Santoro, C., Tahmassebi, S., 2000. Comparing Design Options for Allocating Communication Media in Cooperative Safety-Critical Contexts: A Method and a Case Study. *ACM Transactions on Computer-Human Interaction*, 4, 370-398. ACM Press.

Felciano, R. M., 1997. Human Error: Designing for Error in Medical Information Systems. http://smi-web.stanford.edu/people/felciano/research/humanerror/humanerrortalk.html, visitado em 17 de Março de 2005.

Felici, M., 2006. Capturing Emerging Complex Interactions: Safety Analysis in Air Traffic Management. *Reliability Engineering & System Safety (RESS)*. Volume 91, Issue 12, pp. 1482-1493, Elsevier Ltd.

Filipe, J. K., Felici, M., Anderson, S., 2003. Timed Knowledge-based Modelling and Analysis: On the dependability of Socio-technical Systems. *HAAMAHA 2003, 8th International Conference on Human Aspects of Advanced Manufacturing: Agility and Hybrid Automation*. http://www.dirc.org.uk/publications/inproceedings/abstract.php?id=41, visitado em 9 de Março de 2005.

Francisco, M.F.M, Sagukawa B.M., 2006. Safety in a Web-based Satellite Flight Plan Supporting System. *SpaceOps 2006 Conference*. AIAA 2006-5773. American Institute of Aeronautics and Astronautics Inc.

Freissinet S., 2007. 1001 Crash - The Tenerife Disaster. http://www.1001crash.com/index-page-tenerife-lg-2-numpage-1.html, visitado em 26 de Março de 2007.

Galliers, J., Minocha S., 2000. An Impact Analysis Method for Safety-critical User Interface Design. In *TOCHI, ACM Transactions on Computer-Human Interaction*. ACM Press.

Glaab L. J., Kramer L. J., Arthur T., Parrish R. V., Barry J. S., 2003. Flight Test Comparison of Synthetic Vision Display Concepts at Dallas/Fort Worth International Airport. *NASA Technical Publication NASA/TP-2003-212177*. NASA.

Guimarães, M.S., Baranauskas, M.C.C., 2009. A Case Study on Modelling the Communication Structure of Critical Systems. *Information Systems in the Changing Era: Theory and Practice*, Proceedings of *11th International Conference on Informatics and Semiotics in Organisations*, 465-472, Aussino Academic Publishing House, ISBN: 978-0-9806057-2-3.

Guimarães M. S., Baranauskas M. C. C., Martins E., 2008. Communication-Based Modelling and Inspection in Critical Systems. *10th International Conference on Enterprise Information Systems*, INSTICC Press.

Guimarães M. S., Baranauskas M.C.C., Martins E., 2007a. "A Communication-based Approach to Requirements Elicitation for Safety-Critical Systems". *Complexity in Organizational and Technological Systems*, Proceedings of *10th International Conference on Organisational Semiotics*, 66-75, ISBN 1-87412-15-2/978-1-87412-15-6.

Guimarães M. S., Baranauskas M. C. C., Martins E., 2007b. Interaction in Critical Systems: Conquests and Challenges. *9th International Conference on Enterprise Information Systems*, INSTICC Press.

Gurr, A.C., 2008. Knowledge Engineering in the Communication of Information for Safety Critical Systems. *Cambridge Journals*. http://citeseer.ist.psu.edu/348180.html, visitado em 20 de Novembro de 2008.

Gurr C., Hardstone G., 2001. Implementing Configurable Information Systems: A Combined Social Science and Cognition Science Approach. *CT'2001, 4th International Conference on Cognitive Technology*, 391-404. Springer-Verlag.

Harrison, M., 2004a. Human Error Analysis and Reliability Assessment. *Workshop on Human Computer Interaction and Dependability*. http://www.laas.fr/IFIPWG/Workshops& Meetings/46/05-Harrison.pdf, visitado em 2 de Maio de 2006.

Harrison, M., 2004b. Aspects of Human Error: A brief introduction. *Workshop on Human Computer Interaction and Dependability*. http://www.laas.fr/IFIPWG/Workshops& Meetings/46/03-Harrison.pdf, visitado em 2 de Maio de 2006.

Hewett, T.T, Baecker, R., Card, S.K, Carey, T., Gasen, J.G., Mantei, M.M., Perlman, G., Strong G.W., Verplank, B., 2007. Curricula for Human-Computer Interaction. *ACM SIGCHI Curricula for Human-Computer Interaction*. ACM SIGCHI. http://sigchi.org/cdg/cdg2.html, visitado em 17 de Outubro de 2007.

Hollnagel, E., 1993, The Modelling of Loss of Control. *International Conference on Systems, Man and Cybernetics*, 3, 44-49. IEEE Press.

Hopkin, V. D., 1995. *Human Factors in Air Traffic Control*, Taylor & Francis. London.

Johnson, C. W., 2003. *Failure in Safety-Critical Systems: A Handbook of Incident and Accident Reporting*. Glasgow University Press.

Kletz, T. A., 1997. Hazop – past and future. *Reliability Engineering and System Safety*, 263-266.

Liu, K., 2000. *Semiotics in Information Systems Engineering*. Cambridge University Press. Cambridge.

Liu, X., 2001. Employing MEASUR Methods for Business Process Reengineering in China. *PhD Thesis, University of Twente*. University of Twente, Enschede, the Netherlands.

Knight, J. C., 2004. An Introduction to Computing System Dependability. *ICSE 2004, 26th International Conference on Software Engineering*. IEEE Press.

Mackie, J., Sommerville, I., 2000. Failures of Healthcare Systems. *First Dependability IRC Workshop*, 79-85. Edinburg University Press.

Marhan, A., Paternò, F., Santoro, C., 2003. Improving Dependability through a Deviation Analysis on Distributed Tasks in Safety Critical Systems. *Workshop on Interdisciplinary Approaches to Achieving and Analysing System Dependability, DSN 2004, International Conference on Dependable Systems*. http://homepages.cs.ncl.ac.uk/michael.harrison/dsn/index.html, visitado em 14 de Setembro de 2006.

Navarre, D., Palanque, P., Ladry, L.F., Basnyat, S., 2008. An Architecture and a Formal Description Technique for User Interaction Reconfiguration of Safety Critical

Interactive Systems. *XVth International Workshop on the Design, Verification and Specification of Interactive Systems (DSVIS 2008)*. Kingston, Ontario, Canada. July 16-18.

Nielsen, J. 1993. *Usability Engineering*, Academic Press. San Diego, CA.

Nuseibeh, B., Easterbrook, S., 2000. Requirements Engineering: A Roadmap". *Proceedings of International Conference on Software Engineering (ICSE)*, ACM Press.

Palanque, P., Bernhaupt, R., Navarre, D., Ould, M., Winckler, M., 2006. Supporting Usability Evaluation of Multimodal Man-Machine Interfaces for Space Ground Segment Applications Using Petri net Based Formal Specification. *Ninth International Conference on Space Operations*, Rome, Italy, June 18-22.

Palanque, P., Schyn, A., 2003. A Model-Based Approach for Engineering Multimodal Interactive System. *INTERACT´03*. IFIP.

Palanque, P., Paterno, F., Fields, R., 1998. Designing User Interfaces for Safety Critical Systems. *CHI´98 workshop*. ACM Press.

Palanque, P., Bastide, R., Paternò, F., 1997. Formal Specification as a Tool for Objective Assessment of Safety-Critical Interactive Systems. *INTERACT´97,* 323-330. ACM Press.

Pap Z., Petri, D., 2001. A Design Pattern of the User Interface of Safety Critical Systems. *IWCIT 2001, International Workshop on Control and Information Technology*. http://citeseer.ist.psu.edu/pap01design.html, visitado em 24 de Outubro de 2006.

Paternò, F., Santoro, C., Touzet, D., 2005. Adapting Interface Representations for Mobile Support in Interactive Safety Critical Contexts. *Workshop on Complexity in Design and Engineering*. Glasgow University Press.

Paulson, L. C., 1997. *Software Engineering*, University of Cambridge Press. E.U.A.

PAV (Personal Air Vehicles), 2007. http://cafefoundation.org/v2/pav_home.php, visitado em 15 de Janeiro de 2007.

Reeder, R. W., Maxion, R. A., 2006. User Interface Defect Detection by Hesitation Analysis. *International Conference on Dependable Systems & Networks*. IEEE Press.

ReSIST, European Network of Excellence, 2008. Deliverable D13: From Resilience-Building to Resilience-Scaling Technologies: Directions. http://www.laas.fr/RESIST/index.html, visitado em 10 de Outubro de 2008.

Rong J., Theresa S. and Valasek J., 2005. "Small Aircraft Pilot Assistant: Onboard Decision Support System for SATS Aircraft". *AIAA 5th Aviation, Technology, Integration, and Operations Conference (ATIO)*, 26-28.

Rushby, J., 1994. Critical System Properties: Survey and Taxonomy. *Computer Science Laboratory*. SRI International.

Salles J. P., Baranauskas M. C. C. and Bigonha R. S., 2001. Towards a communication model applied to the interface design process. *Knowledge-Based Systems*, v. 18, n. 8, 455-459.

Salles, J.P., 2000. O Modelo Fractal de Comunicação: Criando um Espaço de Análise para Inspeção do Processo de Design de Software. *Tese de Doutorado*. Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade Federal de Minas Gerais.

Salles, J.P., Baranauskas, M.C.C., Bigonha, R.S., 2000. A Communication Model for the Interface Design Process. *Workshop on Semiotic Approaches to User Interface Design*, CHI 2000, 455-459, Elsevier B.V.

SATS, Small Aircraft Transportation System, 2007. Advanced General Aviation Transport Experiments (AGATE). http://sats.nasa.gov/agate.pdf, visitado em 27 de Janeiro de 2007.

Schnell T., Lemos K., and Etherington T., 2002. "Terrain Sampling Density, Texture, and Shading Requirements for SVIS". *Final Report to the Iowa Space Grant Consortium*.

Smith, S. P., Harrison, M. D., 2002a. Blending Descriptive and Numeric Analysis in Human Reliability Design. *9th International Workshop on Interactive Systems: Design, Specification and Verification,* 2545, 223-237. Springer.

Smith, S. P., Harrison, M. D., 2002b. Augmenting Descriptive Scenario Analysis for Improvements in Human Reliability Design. *SAC '02, Symposium on Applied Computing*. ACM Press.

Sommerville, I., 2003. *Engenharia de Software*. 6a. Edição. Addison Wesley.

Stamper, R.K., 1993. Social Norms in requirements analysis – an outline of MEASUR, in Jirotka, M., Goguen, J. and Bickerton, M. (eds.), *Requirements Engineering, Technical and Social Aspects*. Academic Press, New York.

Stamper, R. K., 1973. *Information in Business and Administrative Systems*, John Wiley and Sons. New York.

Vicente K. J., 2002. Ecological Interface Design: Progress and Challenges. *Human Factors,* 44, 62-78. Human Factors and Ergonomics Society Press.

Vicente K. J., Torenvliet G. L., Jamieson G. A., 1998. Making the Most of Ecological Interface Design: The Role of Cognitive Style. *The Fourth Symposium on Human Interaction with Complex Systems*. IEEE Press.

Vicente K. J., Christoffersen K., Pereklita A., 1995. Supporting Operator Problem Solving Through Ecological Interface Design. *Systems, Man, and Cybernetics*, 25, 529-545. IEEE Press.

Vicente, K. J., Rasmussen, J., 1992. Ecological Interface Design: Theoretical Foundations. *Systems, Man, and Cybernetics*, 22, 589-606. IEEE Press.

Victor C., 2007. Pan Am Accidents. http://www.panamair.org/accidents/victor.htm, visitado em 26 de Março de 2007.

Young S. D. and Quon L., 2006. Aviation Safety Program, Integrated Intelligent Flight Deck. Technical Plan Summary. http://www.hq.nasa.gov/office/aero/nra_pdf/iifd_tech_plan_c1.pdf, visitado em 17 de Outubro de 2007.