

Human Factors in Automatic Risk Assessment for Systems of Systems

Jonathan Aitken
University of York



Introduction

- Dynamic Risk Assessment in NEC SoS
 - A live safety case
- SSEI Task 19 - Overview and Objectives
- Decision Making and Risk
- Impact of Complexity and Future Systems

NEC SoS

■ System of Systems

“A DSoS (Dependable System of Systems) is a dependable system composed of independent autonomous systems. The purpose of a SoS is to provide a set of enhanced or improved ‘emergent’ services, based on some or all of the services provided by the participating component systems. The provision of these emergent services requires cooperation between the systems” [1]

- A collection of systems capable of acting together
- Improved service of individual components

[1] P. Periorelis, and J. Dobson, “Organisational Failures in Dependable Collaborative Enterprise Systems,” *Journal of Object Technology*, vol. 1, no. 3, pp. 107-117, 2002.



NEC SoS

- Network Enabled Capability
 - Used to facilitate communication amongst separate nodes within the SoS
 - Operation of the SoS relies on the complex network setup
 - Decision taken about connectivity directly reflect risk within the SoS

Objectives of Task 19

- Aid with safety concerns in NEC SoS
- Development of a technique for dynamic risk assessment
 - How to develop a reliable a risk model for a NEC SoS
 - How to build a dependability model of an NEC network infrastructure
- Human factors and interaction with personnel
 - How can an automated tool justify the risk assessments and communicate them effectively to the field commander?

Decision Making and Risk

- Recognition-Primed Decision Making ^[1]
 - “Decisions” not taken
 - Familiarity with a situation provides all of the identifiers required
- What if the situation is unknown?
 - Mental simulation playing out possible scenarios

[1] G. Klein – Sources of Power, MIT Press

Presenting Information

*“I used to listen to the sounds the boiler makes and know just how it was running. I could look at the fire in the furnace and tell by its colour how it was burning. I knew what kinds of adjustments were needed by the shades of the colour I saw. A lot of the men also said there were smells that told you different things about how it was running. **I feel uncomfortable being away from these sights and smells ... I feel that I should be closer to it in order to control it**” – A worker in a paper mill [1]*

[1] S. Zuboff – In the Age of the Smart Machine: The Future of Work and Power



Presenting Information

- Mechanical systems understood by operators
- Direct operation – useful in obtaining feedback about the system
 - Provides information and subconscious cues
 - Physical separation presents a potential issue
- Our concern is primarily with Network-Enabled Capability Systems-of-Systems
 - Potentially little information or subconscious cues
 - Operators physically separated from equipment



Growing Network Complexity

- An increase in complexity causes a breakdown in technical assistance
 - Disuse of automatic systems under pressured conditions [1][2][3]
 - Unfamiliarity with technology
 - Uncertainty over capabilities

[1] Dzindolet, M.T., et al., *Predicting Misuse and Disuse of Combat Identification Systems*. *Military Psychology*, 2001. **13**: p. 147-164.

[2] Salmon, P.M., et al. *Decisions, Decisions... and Even More Decisions: The Impact of Digitisation in the Land Warfare Domain*. in *9th International Conference on Naturalistic Decision Making*. 2009. London, UK: British Computer Society.

[3] Personal Communication



Concern Over Future Systems

- Increased complexity of systems puts additional pressure on personnel ^[1]
- Significant challenge to the user's situational awareness
- User's very competent in solving problems ^[1]
 - "I know what happened last time..."
- Increasing complexity puts more pressure on the user
 - Necessitates an increase and reliance on *trustable* automatic tools
 - Complex interactions make the implications of an event difficult to understand

[1] Personal Communication



Developing Trustable Techniques

- Our technique will be built upon within existing models
- The Ministry of Defence Architectural Framework (MODAF)
 - Advantage – Common language
 - Disadvantages – No representation of safety

MODAF As a Modelling Tool

- MODAF – Ministry of Defence Architectural Framework
- Standard approach to Enterprise Architectures
- Multiple views of networks
 - All (scope, ownership and timeframe)
 - Strategic (analysing and optimising capability)
 - Operational (behavioural and information aspects)
 - System (resources realising capability)
 - Technical (standards, rules, policy and guidance)
 - Acquisition (dependencies and integration)
 - Service Orientated (Services in an SOA)



Hazard Representation in MODAF

- No explicit representation of a hazard
 - Traceability of risk and hazards presents a problem
 - Views deal with operational circumstances
- MODAF provides the information
 - The hazard is in the context

Definitions

- System-of-Systems Caused Loss
 - Injury or death to non-combatants (white)
 - Injury or death to blue personnel
 - Damage or destruction to blue equipment
 - Damage or destruction to white buildings or possessions
 - Damage to blue equipment or personnel caused by undetected-enemy action
- Providing loss caused by an SoS Hazard



Definitions

- System-of-Systems Accident
 - Combined behaviour of two or more nodes
 - Hazardous state combination (SoS Hazard)
- Four Classes
 - Blue-on-Self SoS Accidents
 - Blue-on-Blue SoS Accidents
 - Blue-on-White SoS Accidents
 - Red-on-Blue SoS Accidents

Definitions

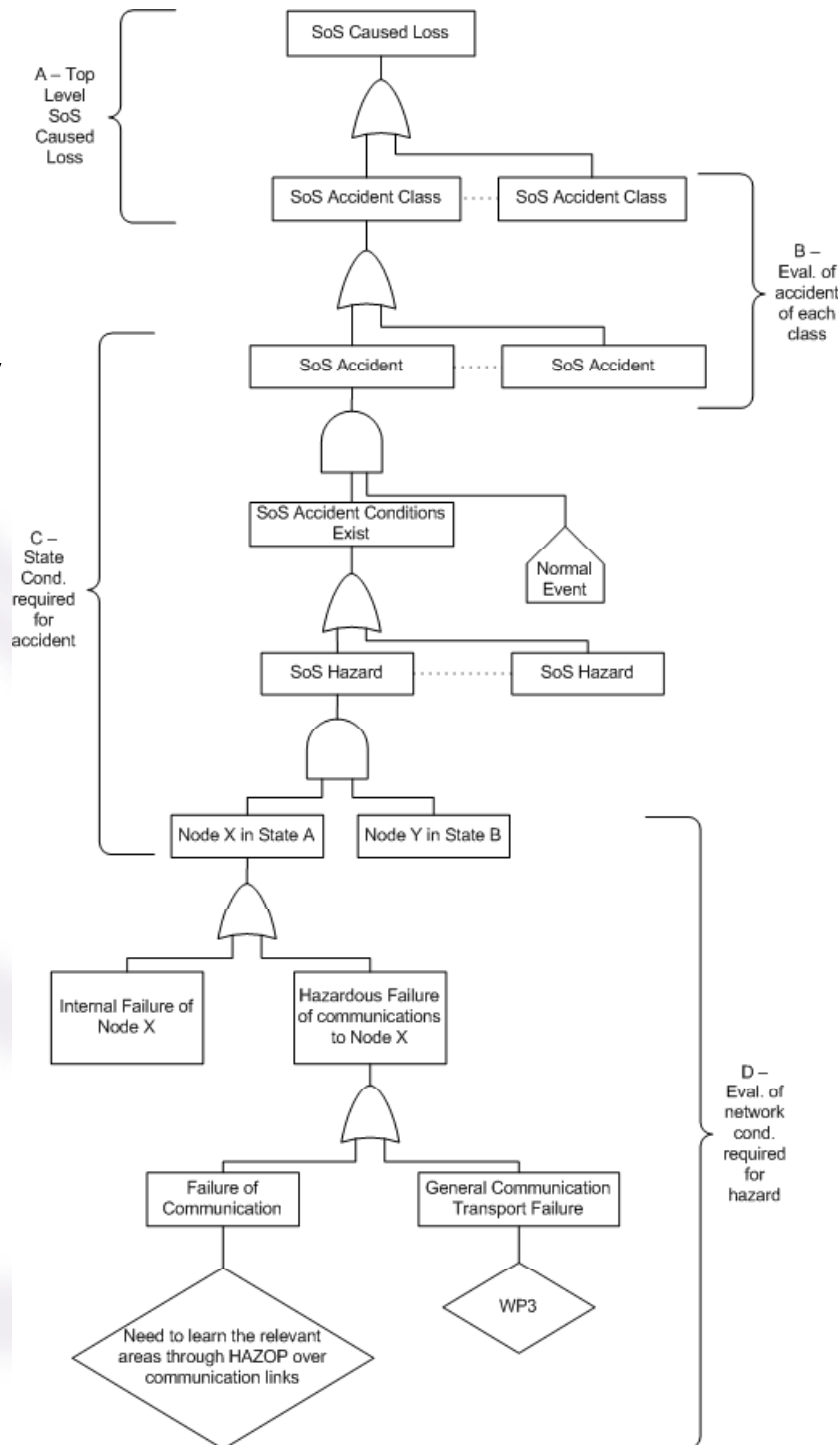
- System-of-Systems Hazards
 - A SoS Hazard is a state of a SoS such that: no further abnormal events need to occur for an accident to occur, **AND** it can be described as a set of state combinations across at least two nodes.

Risk Modelling

- Risk model formed from a fault tree, extended during analysis
 - Linked to operational views in MODAF
- The Fault tree is broken down into four separate regions
 - Accumulation of SoS Accident Classes
 - Assignment of SoS Accident to SoS Accident Class
 - Linking individual node states, hazards and accidents
 - Identifying causes of the individual node states

Order of SoS Analysis

- Region C - Opportunity for potential accidents
- Region B – Group accidents to accident classes
- Region D – Exploring local conditions for causing hazards
- Region A – Bringing together the accident classes



Future Work

- Potential impact of the network
 - Direct impact on end-to-end service (e.g. Bandwidth limitations)
 - Applications of issues highlighted in IEC-61508 (repetition, delay, deletion, insertion etc...)
 - Impact of these factors on higher levels of the SoS

Conclusions

- Separation from equipment leads to operator dissociation
- Trust in information is a serious
- Risk modelling techniques must be built upon common products such as MODAF
- Common model provided to be extended for each individual example

Software Systems Engineering Initiative

www.ssei.org.uk



Überlingen – A Practical Example

- Collision between Boeing 737 and Tupolev Tu-154 at FL350
- Collection of errors or failures in practice present
 - Single-man operating procedures (late-night)
 - Downgraded radar (no short-term conflict alert)
 - Multiple responsibility (dual screens)
 - Phone system errors (diversion of attention)
 - TCAS (information to pilots only)
 - Corporate culture (Europe versus Russian pilots)

Überlingen – Asking Questions On-Line?

- Cause and Effect
 - Equipment going offline
 - Operational procedure change
- Each incident has a minor impact on the system
 - Can an operator keep track of all minor problems and predict cumulative effects?
- Automatic risk detection can provide warning providing adequate information ahead of time