Safety & Reliability
Model-Based Safety Engineering
Fran Thom & James Towers
Hello from Fran & James!
Overview

• The Problem
  – Do we want to:
    a) Design the system today and check it is safe tomorrow?
    b) Design a safe system today?
  – How is safety analysis efficiently integrated with MBSE?

• A Solution
  – Scope – the context of safety
  – Ontology – the rule-set for capturing information
  – Viewpoints & Views – communicating the information
  – Constraints:
    • Must be integrated into the System Specification (model)
    • Must be simple and easy to use
Safety in Industry

- Lots of safety standards out there
  - Some general standards e.g. ISO-61508
  - Most are tailored for different industries
    - Aerospace – DO-178C, DO-254, ARP4754A
    - Automotive – ISO-26262, WVTA
    - Rail – CENELEC
    - Nuclear – ONR, IAEA
    - Marine – LR, SOLAS, IMSBC, MARPOL
- General widening of scope of safety standards to encompass all technologies integrated in the system
  - Human, mechanical, hydro-mechanical, pneumatic, electrical, electronic, software...
- Evolving standards
  - From prescriptive – *do what we were told*
  - To objective – *keep risk as low as reasonably practicable* (ALARP)
  - More options and complexity requires an increase in visibility of safety analysis and design choices
Thought...

The actual hazards, consequences, risks, failures etc. may differ between industries however, can the approach to safety engineering be the same?
What else to consider?
Shifting Landscapes

• *Left-shifting* the engineering process (*Faster...*)
  – address system safety as early as possible

• Project Management (*Faster...*)
  – agile, lean (Incremental and Iterative)
  – multi-functional teams including safety

• Economics (*Better and Cheaper...*)
  – feature-rich products with value-adding services cheaper, or at no extra cost... 😌
Common Problems

• **Textual** Requirements used to
  • Design the System AND
  • Analyse the Safety & Reliability of the System
    - Different teams with different interpretation of the requirements
    + The model contains the system AND safety requirements
• Communicating in different languages (often different tools)
  + MBSE facilitates agreement between Systems Engineers, Design Engineers and Safety Engineers
• **Independent** Assessment & Certification
  + System Engineers create the system specification including safety with Independent Assessment
  + The model provides visualisation and traceability to support Independent Assessment
Requirements for A Solution

• Must use our agreed system modelling approach

• Must use our agreed framework approach

• Minimise any duplication of effort
  – Safety to be an integral part of the System Specification – *easy to use*

• Integrate with static and dynamic safety analysis techniques
  – *left-shift safety engineering*
A Solution

Scope: The system (products + services) in context throughout its life-cycle

Methodology

Views  Define and Refine  Viewpoints

Ontology
Methodology - Hazards

- It is a consequence of previous system failures that we know some hazards:
  - The system (or sub-system):
    - Failed to stop when commanded and crashed
    - Started when not commanded, produced an arc flash and killed the operator
    - Exploded causing fire damage to its environment
  - The system (or sub-system) produced uncontrollable [energy | material | force]* flows which resulted in:
    - Too much * flow causing another system (or sub-system) to catch fire
    - Too little * flow resulting another system (or sub-system) over-heating and releasing poisonous gas into the environment
    - None at all * flow causing the system (or sub-system) to stop when not commanded causing injury to the operator and passengers
    - Oscillating * flow leading to the system (or sub-system) mechanically disintegrating releasing radiation into the environment
    - ...

BUT WAIT...
Methodology – Hazards & Effects

- It is a consequence of previous system failures that we know some hazards:
  - The system (or sub-system):
    - Failed to stop when commanded and crashed
    - Started when not commanded, produced an arc flash and killed the operator
    - Exploded causing fire damage to its environment
  - The system (or sub-system) produced un-controllable [energy | material | force]* flows which resulted in:
    - Too much * flow causing another system (or sub-system) to catch fire
    - Too little * flow causing another system (or sub-system) over-heating and releasing poisonous gas into the environment
    - No * flow causing the system (or sub-system) to stop when not commanded causing injury to the operator and passengers
    - Oscillating * flow leading to the system (or sub-system) mechanically disintegrating releasing radiation into the environment
    - ...
This Ontology is modelled using UML Classes
(We will see why later...)
The Ontology

Agreeing the terms and their relationships provides the common language for communication.
Safety Viewpoint

• Views to support:
  – Functional Hazard Analysis (FHA) to determine the Safety Integrity or Design Assurance Levels (SIL/DAL)
FHA View - Hazards

Drag and drop the term (onto a UML Object Diagram) to create Instances of Hazards
FHA View – Hazards & Effects

Instances of Effects tracing to the Hazards they cause

The ontology enforces the permissible relationship

Only Effects can cause a Hazard (that’s what we agreed...)

The ontology also allows us to have many Effects causing the same Hazard
FHA View – Hazards, Effects to SIL

Instances of Safety Mechanisms (and SIL) to mitigate the Effects
Viewpoint Organisation

System-Level Hazards exist at the system level

The same pattern of Viewpoint organisation (package structure) can appear for Sub-System or at any Part of the System Specification
Safety Viewpoint

• Views to support:
  – Functional Hazard Analysis (FHA) to determine the Safety Integrity or Design Assurance Levels (SIL/DAL)
  – Hazard End-to-End Thread (“The Red Thread”) to determine all the components involved in leading to an effect
Interrogating the System Design

• The System Specification is composed of multiple sub-system hierarchies of parts, it is not easy to see the complete, end-to-end set of interacting parts that lead to a hazard.

• We will use the “as specified” (SysML) blocks and parts to create the red thread
  - Describe the “as desired” behaviour
  - Interrogate the red thread to determine how the safety mechanism is integrated
First the System as specified
The Sub-Systems as specified

**Sub-System 1**
- **B**: Battery
- **P**: Pump
- **W**: Water
  - **POut**: Water
  - **PIn**: Water
- **W**: Water Tank

**Sub-System 2**
- **CWIn**: Water
- **CE**: Core Enclosure
- **CJ**: Cooling Jacket
- **RC**: Reactor Core
  - **CWIn**: Water
  - **CJ**: Water
  - **RC**: Thermal Energy
A Sequence Diagram (named by the Hazard) is used to bring all the parts involved in producing the Effect.

The red thread cuts across different sub-systems and references their parts.

The part references do not affect the System Specification.

We know the Hazard and the Effect and need to address the Safety Mechanism...
Interrogating the red thread:

- Battery Power not stable causing pump to generate oscillating flow
- Battery not suitable for nuclear installation
- Pump faulty
- Water Tank generating oscillating flow
- Cooling Jacket not mounted correctly and amplifying oscillating flow
- ...

Description

Sub-System 1.B: Battery
Sub-System 1.P: Pump
Sub-System 1.W: Water Tank
Sub-System 2.CE.CJ: Cooling Jacket

E Power

Water

Water
Updating the System Specification

• The System Specification (model) is updated to introduce new functionality and/or new physical parts to address the Safety Mechanism

• The red thread is updated with new the parts and acts as evidence of how the System Specification mitigated the Effect that could lead to the hazard
System Re-Specification
The newly introduced parts are integrated into the end-to-end sequence.
Updated FHA

References are made to the parts implementing the Safety Mechanism
Summary

• Safety is a separate but integral part of the System Specification
• Uses ‘out of the box’ SysML and UML with the addition of only one stereotype – easy to adopt
• Does not duplicate effort – the system specification is referenced, updated and re-referenced
• Provides traceability between systems and safety engineering
• Can be integrated with more detailed safety analysis (e.g. FTA, Markov, etc.)
Questions?
Further reading
Coming soon...

- Training courses:
  - 28\textsuperscript{th} April 2020: Introduction to MBSE
- Free events every Thursday:
  - 1000 – 1045 – a free talk and presentation
  - 1100 – 1145 – the Model-Based Social Event

Visit: www.scarecrowconsultants.co.uk for more details