Techniques and benefits of incorporating Safety and Security analysis into a Model Based System Engineering Environment

Gavin Arthurs P.E
Solution Architect – Systems Engineering
IBM Software, Rational
Common Safety Terminology

_Reliability_ - The probability that a system component will perform its intended function, for a prescribed time and under prescribed conditions.

_Fault_ - Is the inability to perform – (i.e. _Unreliability_ is the probability of fault).

- _Failure_ – is a random fault in which a properly functioning component becomes dysfunctional (event)
- _Error_ – is systematic fault in requirements, design, implementation, or installation (condition or state)

_Accident_ – An unplanned event that that results in some specified loss

_Hazard_ – is a system condition and a set real world conditions or events that will lead to an accident – (driven by context and system boundaries)

_Risk_ – is a combination of the likelihood of an accident and its severity

_Safety_ – is freedom from accidents

Source: various sources (see references on the last slide)
Safety and Security

Safety and Security are both *system properties* that are closely related.

Both involve:
- dealing with risk
- trading constrained behavior with important system goals
- protection from loss
- aspects of a system that are regulated by government agencies or licensing bodies

Source: various sources (see references on the last slide)
Traditional Hazard Analysis Techniques – Fault Tree Analysis

Overview
• Developed in 1961 – Bell Labs
• Top down search of selected event (must assume initial conditions)
• Uses Boolean logic to describe combinations of individual faults that can lead to a hazard

Use in MBSE
• Benefits
  • Graphical representation – can be used in modeling
  • Mitigation identification
  • Promotes focus and understanding of the safety aspects of the system
• Concerns/Limitations
  • Doesn’t handle time ordering of events well
  • Most effective when applied to a completed design – requires system understanding
  • Focuses on causes of hazards not on identification

Source: various sources (see references on the last slide)
Traditional Hazard Analysis Techniques – Event Tree Analysis

Overview
- Developed in the 70s by the Nuclear industry
- Forward search of selected event to assess possible outcomes
- Depends on understanding of the application – that is, previous experience

- Similar to FTA – Requires prior system understanding

Other analysis techniques
- CCA – Cause Consequence Analysis
- FMEA – Failure Modes and Effects Analysis
- FMECA – Failure Modes, Effects and Criticality Analysis

Source: various sources (see references on the last slide)
The Effect of System Complexity on Safety

- Behavior is driven by the interaction of system components – including un-safe behavior
- Enabled by the ever increasing use of software to implement functionality – software does not “fail”
- Provides a coupling/dependence mechanism that is difficult to understand

Traditional analysis methods based on a reliability and failure models are not effective in dealing with these kinds of faults
Example: System Interaction Accident (no failure)

1. Computer detected a low oil signal from the gearbox
2. Computer sounded alarm and “held” control variables as per requirement
3. At the time, catalyst was added to the reactor but only a small amount of water flow was flowing to the condenser
4. The reactor overheated and vented toxic vapor.

NOTE: No components failed, everything worked as specified, including the software.

Any effort to increase the reliability of the components would not have prevented this accident

Adapted from Kletz, Trevor, Human problems with computer control. Plant/Operations Progress, Oct 1982
System oriented Hazard Analysis Techniques - HAZOP

Overview - HAZOP (Hazards and Operability Analysis)
- Developed in the 60’s by the chemical industry
- Considers design or operation deviations
- Uses “guide words” applied to system variables to illicit possible hazards

Use in MBSE
- Benefits
  - Focuses/encourages hazard identification – deviations in system parameters
  - Provides guidance - *more than, less than* etc.
  - Simple to apply
- Concerns/Limitations
  - Generally focused around process systems
  - Does require a representation of the system
  - Not inherently a graphical depiction

<table>
<thead>
<tr>
<th>Guide Word</th>
<th>Deviation</th>
<th>Possible Cause</th>
<th>Possible Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>NONE</td>
<td>No Flow</td>
<td>1. Pump Failure</td>
<td>1. Over heating in heat exchanger</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Pump suction filter blocked</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Pump isolation valve closed</td>
<td>2. Loss of feed to reactor</td>
</tr>
</tbody>
</table>

Guide Words
- NO, NOT, NONE
- MORE
- LESS
- AS WELL AS
- PART OF
- REVERSE
- OTHER THAN
System oriented Hazard Analysis Techniques - STPA

Overview STPA – System-Theoretic Process Analysis
• Developed by Professor Nancy Leveson – MIT 2011
• Rooted in an Systems Engineering approach
• Views safety as inadequate control vs failure of components
• Addresses issues presented with complex systems

Use in MBSE
• Benefits
  • Can be applied early in the development phase – Uses a “systems” perspective
  • Explicitly maps to system hierarchy decomposition
  • Provides guidance with keywords and functional control model
• Concerns/Limitations
  • New – relatively unproven
  • Maximum benefit achieved with effective traceability management
Goals

• Leverage the graphical representations and semantic meaning of SysML
• Provide a framework for incorporating the appropriate analysis technique in the right context
• Provide a mechanism to create traceability between artifacts/analyses
• Work with and complement current MBSE development approaches
FTA and MBSE

Using a UML/SysML profile to extend the modeling language to support safety concepts:
- FTA diagrams
- Logical operators
- Structural elements – Hazard, Fault etc.
- Metadata – probability,
- Associations and dependencies
“Systems” based Hazard Analysis and MBSE

Level 0

L0 System Behavior

<<satisfy>>

<<mitigate>>

<<trace>>

<<allocate>>

L0 SDC

Constraint description

Level 0 Hazard

Hazard description...

Level 1

L1 System Behavior

<<satisfy>>

<<mitigate>>

<<derivedHazard>>

<<allocate>>

L1 SDC

Rationale

Level 1 Hazard

Hazard description...
Example
Load and Unload Passengers

«Requirement»
SK0000
The APM will be configured as dual lane shuttle with four stations (two terminals and two intermediate stations). The trains will be self propelled and the stations will be configured with triple platforms - with flow through movement.

«Requirement»
SK1000
Station platforms will be configured with adequate loading and unloading sides

«Requirement»
SK1001
The trains will have automatic doors on either side for loading and unloading of passengers

«Requirement»
SK1002
The station will incorporate barriers to operate safe passage for the train’s movement. The barriers will have automatic doors to allow passengers safely load and unload the trains.
Single-Lane Shuttle  Single-Lane Shuttle with Bypass  Dual-Lane Shuttle  Dual-Lane Shuttle with Bypass

Source: Lea+Elliott, Inc.
**H1**
Exposure of station passengers and personnel to moving trains, exposed power sources of the guideway, heat and noise and physical drop offs

**H2**
Exposure of train passengers or personnel to impact of fixed guideway or station structures during train motion, drop offs and exposed guideway power sources

**H3**
Exposure to impact while passengers transfer in and out of the train

**Load and Unload Passengers**
Summary

• The complexity exhibited in many of today’s “systems” has limited the effectiveness of the traditional safety analysis techniques that are based in a “failure” perspective.

• New approaches are being developed to analyze safety concerns early in the early design phases – these take a “systems” perspective

• Model based approaches to systems engineering can incorporate both of these Safety analysis approaches and can provide context and a framework for their appropriate use.

• To be most effective, traceability has to be implement effectively both in scope and efficiency
References


*ACRP report 37, Guidebook for Planning and Implementing Automated People Mover Systems at Airports*, TRB 2010

Thank You

www.ibm.com/software/rational