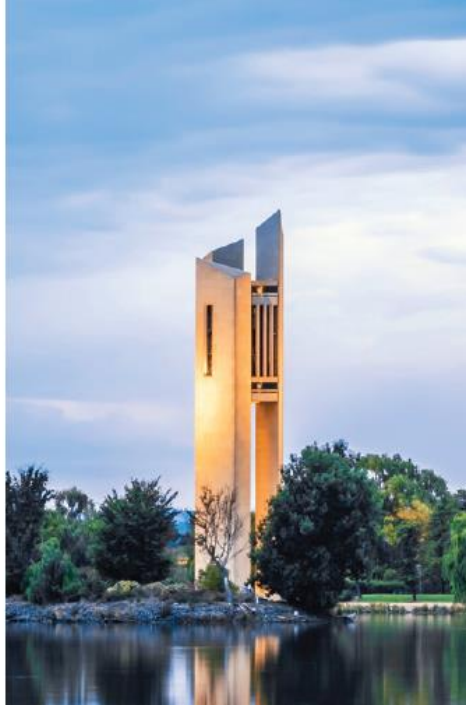
SETE
SYSTEMS ENGINEERING TEST AND EVALUATION CONFERENCE 2019
QT Canberra | Australia
29 April – 1 May 2019



SYSTEMS SCIENCE & ENGINEERING FOR A BETTER AUSTRALIA SETE2019.COM.AU

Enhancement of FMEA Risk Assessment with SysML

William Scott CSEP

Risk and Safety

- New technologies need to be examined when they are introduced to ensure that risk and safety is properly managed
- There are numerous approaches to risk analysis
  - These are used to aid understanding of the risks within the system and subsequently manage the risks to an acceptable level
- FMEA was selected as the SysML tool being tailored already supported capture of FMEA data
  - This reduced effort and allowed the focus on developing the enhancements to the presentation and derivation of the information

Heavy Rail Context

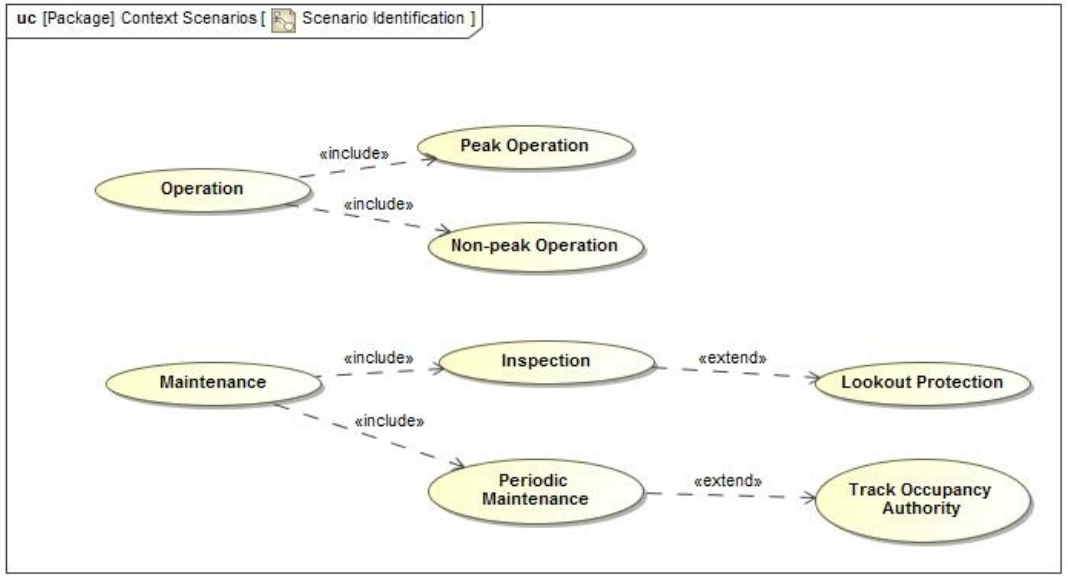
- The work described here has been done as a part of research into how heavy rail systems can benefit from the application of MBSE
  - Work sponsored by the Australasian Centre for Rail Innovation (ACRI)
- Project aims to aid understanding of the impact of the introduction of new technologies on track worker safety
- The approach has been to build a multi-disciplinary MBSE model that aids understanding of the impact of the new technology
  - How the technology integrates into the existing systems
  - Changes to required competencies
  - …
- While the examples provided are based on heavy rail, the approach is designed to be tailorable to other contexts

Improving FMEA Tables in a Visual Language Environment

- Examining how the tool incorporated the FMEA information in tables
  - Table presentation reflects common reporting done in Excel
  - Benefit is that the information is then linkable to other available information
- However several opportunities to improve the tables were identified
  - Tables could be connected of the summary FMEA information to the underlying analyses
    - Retains traceability
  - Automatic table generation for consistency and completeness
  - The ability to create a multi-context analysis

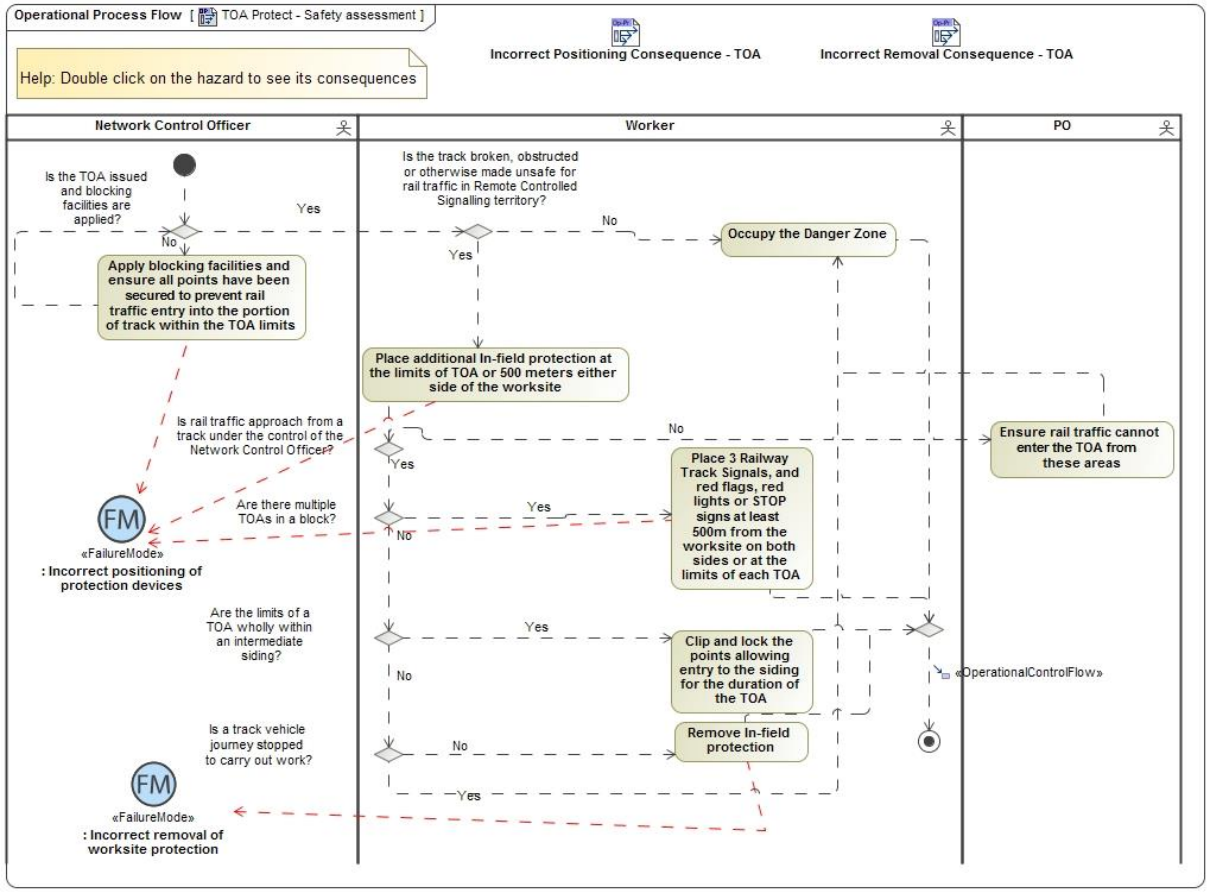
Risk Assessment in Multiple Contexts

- Risk assessment begins with establishing the context to be analysed
- With a complex system such as heavy rail, there are numerous situations that need to be examined
  - Each of these situations will occur in parallel



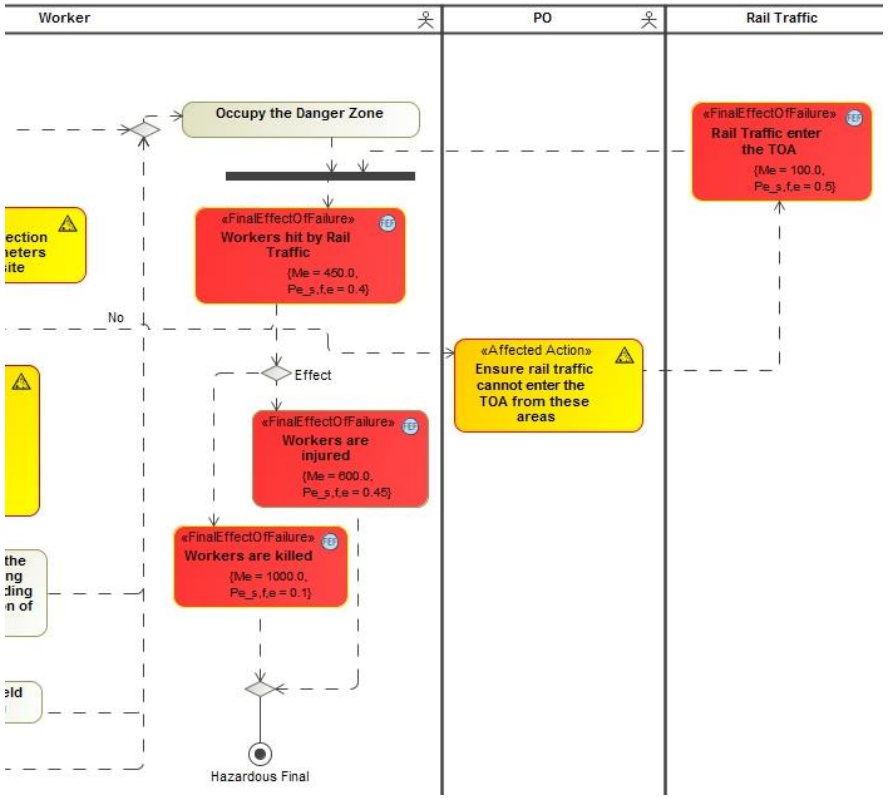
Risk Identification Example for a TOA

- Processes are examined to identify which have failure modes.
  - Diagrams are annotated to identify where failure modes may occur in the process
- These diagrams were created as variantions for many processes
  - When processes were updated, the failure modes needed review



Risk Analysis Example for a TOA

- For each scenario and each failure mode
  - The process diagrams are refined to understand the sequence of events that result in the final effect
- Many process diagrams are often “vanilla” versions
  - i.e. they lack protective gates and actions when adverse events are encountered
- These failure modes capture this important information as well as the consequences for when the protections fail
  - Note that multiple alternative effects can be identified
  - The outcome may be the result of mitigating processes or merely chance



Summary of Effects

- Given the various scenario analyses, it is possible to then report the variety of effects of a particular failure mode
- As the scenario analyses are assumed to be conducted independently, it is important to determine the variety of effects
  - This then helps identify the overall set of possible effects

#	Failure Mode	Final Effects of Failure
1	Incorrect positioning of protection devices	Workers hit by Rail Traffic Rail Traffic enter the TOA Workers are injured Workers are killed
2	Incorrect removal of worksite protection	Damage to the train and protection devices Train hits the protection guards and signs
3	Incorrect identification of worksite location - TOA	Workers hit by Rail Traffic Conduct TOA in wrong location Workers are killed Workers are Injured Understand the Authorized TOA Incorrectly
4	Incorrect identification of worksite location - TWA	Workers hit by Rail Traffic Workers are injured Workers are killed
5	The type of protection being incorrect	Issue wrong Protection Accidents caused by wrong protection Wrong Blocking facilities Wrong briefing of workers

Risk Evaluation and Prioritisation

- So what is the most critical “risk” to address?
- There are two approaches that have been identified:
  - Which scenario contains the highest risk?
  - What failure mode reflects the highest risk?
- The stakeholders can then choose to address a specific failure mode or a scenario/process that contains an unacceptable level of risk.

Measuring Risk over Multiple Contexts

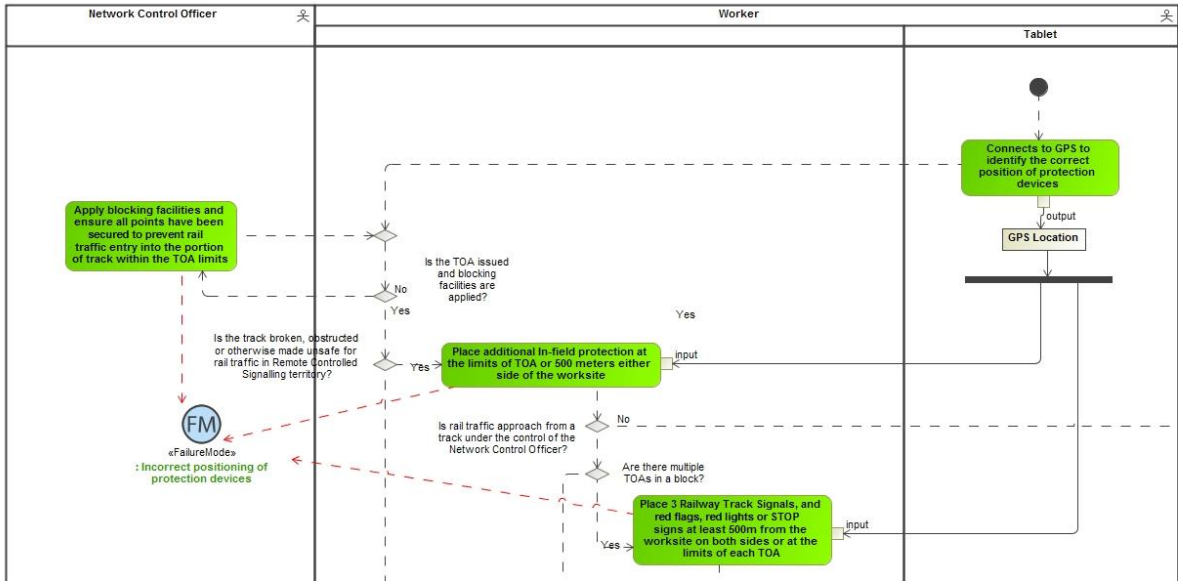
- As a risk is spread over multiple scenarios, it is necessary to modify the risk formula
- A subsequent analysis is also created to rate the failure modes based on the combination of:
  - The likelihood of a scenario occurring
  - The likelihood of the failure mode occurring within the scenario
  - The likelihood of each effect in the event of the failure mode in that scenario
  - The measure of the effect's impact

$$F_i = \sum_s \sum_e P_s P_f(s) P_e(s, f, e) M_e$$

s is the scenario with an associated probability P_s,
e is the effect,
$P_f(s)$ is the probability of the failure mode in scenario s,
$P_e(s, f, e)$ is the probability of effect e given scenario s and failure mode f,
M_e is the measure of the impact of the effect (assumed to be context independent)

Risk Treatment

- Treatments can then be identified to mitigate the various risks
- Further variants of the process diagrams are created that subsequently capture how protections have been put in place to mitigate the risk
- This then results in a flow of diagrams that capture the understanding of how the risk has been analysed and subsequently treated
- A final FMEA table (not pictured) is created that enables the user to see the processes in the various forms and subsequently understand how the risk is being managed



Effectiveness

- Methodology has been well received during the presentations to multiple heavy rail organisations
  - Automation is seen as cost saving
  - SysML adds richness to the previous standard table based representations
  - Traceability and retention of the analysis are also beneficial
- Concerns about availability of the required information
  - Situations in new projects may lack the level of detailed information needed
  - Information is needed earlier in the acquisition process
  - Effort required to keep diagrams aligned
    - Some handled by tools but other algorithms being developed
  - Requires a notification system when underlying changes are made

And… I'm out of time so onto the questions