Model Based Systems Engineering & Hazard Logs

Hazard logs are at the core of any system safety argument or safety case. This article explores some of the challenges with the standard tabular, textual hazard logs and whether these challenges can be addressed with support from Model Based System Engineering (MBSE).

In this article we will:

- Identify several challenges faced by system safety engineers with existing hazard logs.
- Look at several existing methods used to overcome these challenges.
- Consider how MBSE using Systems Modelling Language (SysML) tools may be able address those challenges.

The Challenges Of Using Hazard Logs

The standard hazard log, following industry standards such as EN50126-1 [1], captures hazards in a tabular, textual form using a large spreadsheet or assurance database (e.g. IBM DOORS Next). These spreadsheets and databases are often customised in a format to comply with relevant standards and/or a stakeholder's templates for on-going safety risk management. Although this approach is widely used, it does create a few notable challenges:

Challenge 1: It takes specialist knowledge to understand them. Text-based formats do not intuitively demonstrate the causal relationships between hazards, causes and controls to those who are unfamiliar with system hazard analysis and risk assessment processes in general.

Challenge 2: It takes a significant amount of time from specialist safety engineers and other stakeholders to prepare, manage, maintain these hazard logs at a high level of quality and prepare explanations to stakeholders.

Challenge 3: It is difficult to demonstrate the completeness of the hazard log (required for a solid SFAIRP argument) showing that all safety related functions/data flows between different sub-systems have been analysed.

How Can We Resolve These Challenges?

There are several methods commonly used that attempt to resolve these challenges. These are examined below.

Illustrate Hazard Analysis with Diagrams

Visualisation of the hazard, causes, controls and other architectural relationships as shown in

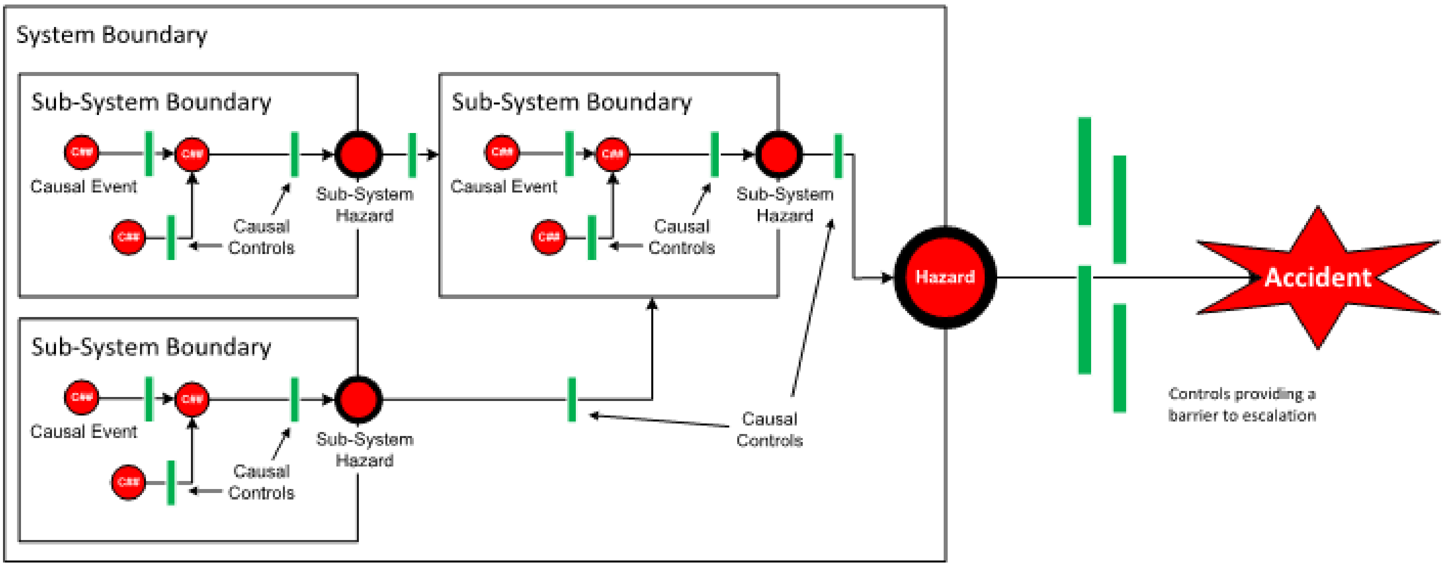

Fig. 1 - Illustration of Hazards with Respect to the System Boundary

Figure 1 enables non subject matter experts to understand the hazards intuitively and in part solves the issues identified in Challenge 1. This approach is appropriate when the quantity of information is limited; however, might not be cost-effective when attempting to illustrate a wider scope due to the amount of time and effort required to produce such diagrams (Challenge 2).

As the complexity of a system increases, a diagram of this type can become very costly to create and manage using conventional drawing tools, such as Microsoft Visio. Tools such as Visio lack integration (or have limited integration) between the diagram and data analysis tools such as a spreadsheet or a database.

Safety engineers are subsequently required to expend effort processing information in the diagrams and transferring it to a spreadsheet or database which can be prone to error. As a result of these deficiencies, such diagrams are not commonly produced unless required by very specific project requirements or to illustrate a specific, novel risk assessment.

Systematic Analyses and Subject Matter Expert Reviews

Current best practice is to execute techniques and methods for safety analyses such as those defined in Table F.2 of EN50126-2:2017 [2]. These techniques and methods are coupled with cross-functional reviews by subject matter experts, systems engineers, human factors specialists, safety engineers or field engineers. These cross-functional reviews help to ensure that all possible hazards, causes and controls have been identified and documented in the hazard log.

This method is a plausible solution for Challenge 3. However, as the size and complexity of the system increases, so too does the quantity of information covered in the safety analyses. This results in a proportional increase in time spent by reviewers (Challenge 2).

How can MBSE Help?

Concept

MBSE allows systems engineers to define the system under analysis in a model that defines the physical and functional blocks of the system and the interactions between those blocks and other systems. A well-modelled system then provides all the information required by a safety engineer to perform their traditional safety analysis techniques.

The concept considered here is to enhance the traditional model-based diagrams with hazard, causal, and control information to provide a view that overlay the hazards, causal links, and controls on the system model as shown conceptually in Figure 2.

By linking the hazard analysis and results to the complete model it can then be easily shown that the hazard analysis is complete (Challenge 3).

The pictorial view of the hazard flow with causal linking and identified controls can enhance the readability and understanding of the analysis for stakeholders (Challenge 1) reducing review time (Challenge 2).

The MBSE tooling will provide the safety engineer a single model to work in and coupled with automated report generation will reduce the time it takes to perform the model and increases the potential for re-use (Challenge 2). This concept has attracted the attention of industry experts and researchers who have made great efforts to standardise the process of integrating safety analysis into MBSE and extend the capability of the MBSE toolbox to support this process [3].

Implementation

This concept was explored using the MBSE tool* "MagicDraw" to create a model for a simple axle counter system. The activity found that while promising there is still more work required in improving the tool set to fully realise the advantages envisioned in the concept.

This implementation is captured in the series of diagrams (Figures 3-8) featured below.

*There are a number of MBSE tools available, including IBM Engineering Systems Design Rhapsody Architect, Cameo Systems Modeller (MagicDraw) and Capella.

Fig. 2 - Concept

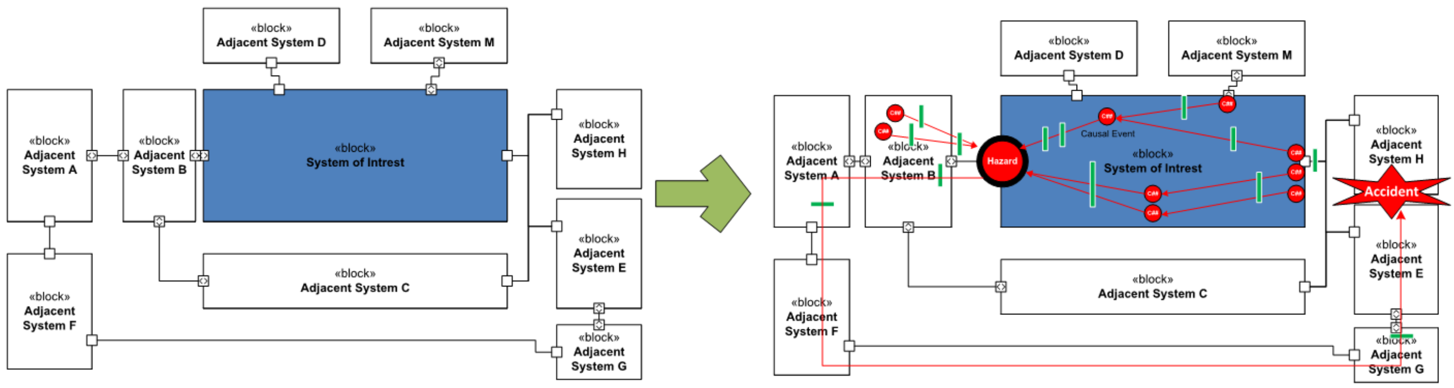

Fig. 3 - System Context of the Axle Counter

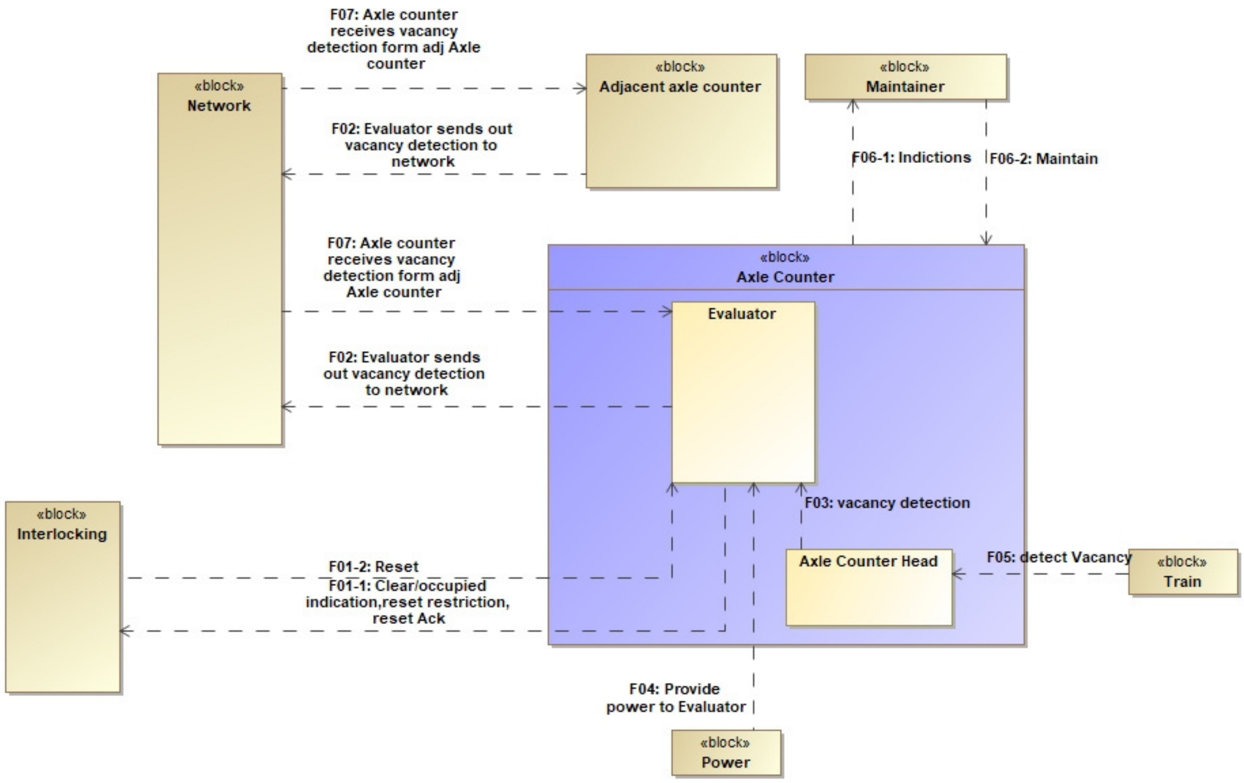

Fig. 4 - Establish Risk Reference Relationship Between Item Flow and Hazard

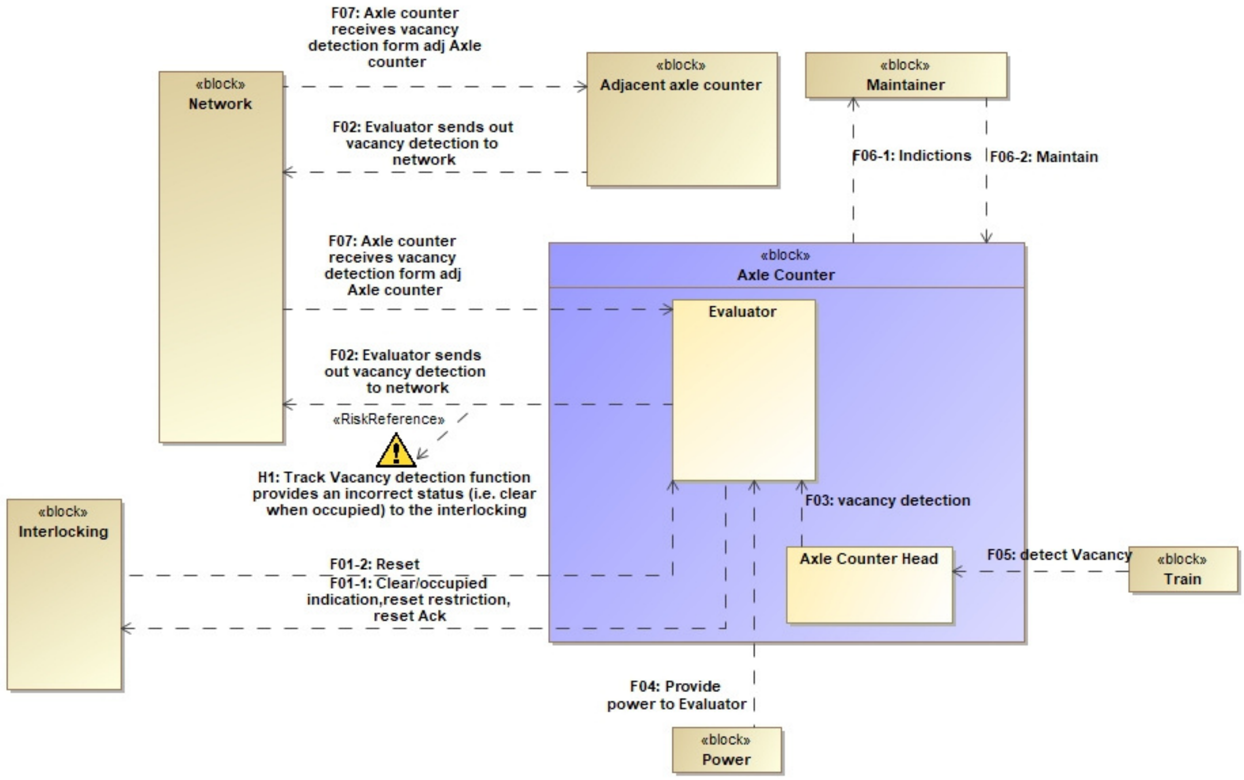

Fig 5 - Hazard Diagram

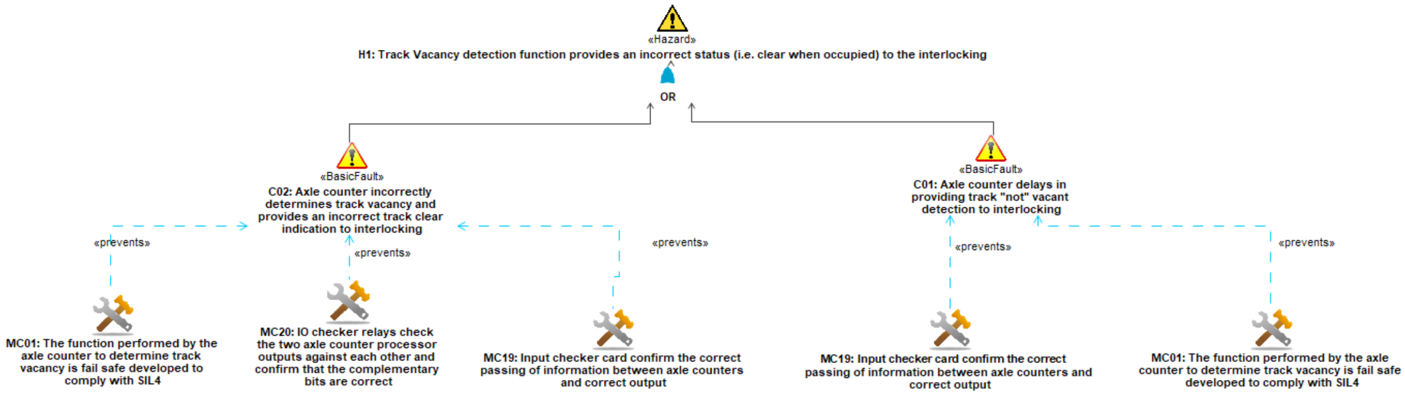

Fig 6 - Hazard Analysis Coverage Report

Criteria

Element Type: Item Flow ... Scope (optional): Design ... Filter:

#	Source	Target	Design Element	Conveyed	Client Dependency
1	Axle Counter	Maintainer	Item Flow[Axle Counter -> Maintainer]	F06-1: Indictions	
2	Evaluator	Interlocking	Item Flow[Evaluator -> Interlocking]	F01-1: Clear/occupied indication,reset restriction, reset Ack	
3	Evaluator	Network	Item Flow[Evaluator -> Network]	F02: Evaluator sends out vacancy detection to network	Risk Reference[-> H1: Track Vacancy detection function p
4	Interlocking	Evaluator	Item Flow[Interlocking -> Evaluator]	F01-2: Reset	
5	Maintainer	Axle Counter	Item Flow[Maintainer -> Axle Counter]	F06-2: Maintain	
6	Network	Adjacent axle coun...	Item Flow[Network -> Adjacent axle counter]	F07: Axle counter receives vacancy detection form adj Axle counter	
7	Power	Evaluator	Item Flow[Power -> Evaluator]	F04: Provide power to Evaluator	
8	Train	Axle Counter Head	Item Flow[Train -> Axle Counter Head]	F05: detect Vacancy	
9	Axle Counter Head	Evaluator	Item Flow[Axle Counter Head -> Evaluator]	F03: vacancy detection	
10	Adjacent axle coun...	Network	Item Flow[Adjacent axle counter -> Network]	F02: Evaluator sends out vacancy detection to network	
11	Network	Evaluator	Item Flow[Network -> Evaluator]	F07: Axle counter receives vacancy detection form adj Axle counter	

Fig 7 - Hazard Log

Criteria

Element Type: Hazard ... Scope (optional): Hazards ... Filter:

#	Name	Applied Stereotype	Nested Classifier	Owned Behavior	Probability
1	H1: Track Vacancy detection function provic	Hazard [Class]	C01: Axle counter delays in providing track "not" vacant detection to interlocking Association[C01: Axle counter delays in providing track "not" vacant detection to i C02: Axle counter incorrectly determines track vacancy and provides an incorrect Association[C02: Axle counter incorrectly determines track vacancy and provides	MC01: The function performed by the axle counter to determin MC19: Input checker card confirm the correct passing of inform MC20: IO checker relays check the two axle counter processor	
2	H2: The Axle Counter inherent design poses	Hazard [Class]			
3	H3: The Axle Counter is inadequately maint	Hazard [Class]			
4	H4: The track vacancy detection function fai	Hazard [Class]			
5	H5: The Power supplied to the Axle Counter	Hazard [Class]	H4: The track vacancy detection function fails to detect the presence of a track ve		

Fig 8 - Cause to Control Traceability Report

Criteria

Element Type: BasicFault ... Scope (optional): Hazards ... Filter:

#	△ Name	Supplier Dependency
1	C01: Axle counter delays in providing track "not" vacant detection to interloc	Dependency[MC01: The function performed by the axle counter to determine track vacancy is fail safe developed to comply with SIL4 -> C01: Axle counter delays in providing track "not" vacant detection to interlocking] Dependency[MC19: Input checker card confirm the correct passing of information between axle counters and correct output -> C01: Axle counter delays in providing track "not" vacant detection to interlocking]
2	C02: Axle counter incorrectly determines track vacancy and provides an inco	Dependency[MC01: The function performed by the axle counter to determine track vacancy is fail safe developed to comply with SIL4 -> C02: Axle counter incorrectly determines track vacancy and provides an incorrect track clear indic Dependency[MC19: Input checker card confirm the correct passing of information between axle counters and correct output -> C02: Axle counter incorrectly determines track vacancy and provides an incorrect track clear indication to i Dependency[MC20: IO checker relays check the two axle counter processor outputs against each other and confirm that the complementary bits are correct -> C02: Axle counter incorrectly determines track vacancy and provides an inc

Conclusion

There are a number of challenges faced by safety engineers in communicating hazard logs to stakeholders (Challenge 1), improve efficiency of preparation and maintenance of hazard logs (Challenge 2), and demonstrating completeness of the hazard log (Challenge 3). It has been shown that MBSE has a significant potential to aid safety engineers in collaboration with systems engineers, overcome these challenges; however, there still exists some challenges to fully realise this.

Acmena will continue to research how to better use the tools made available through MBSE to improve the efficiency and strength of their safety arguments.

Andrew Gabler, Dan Munoz & Yanan Li

References

1. EN50126-1:2017 Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS process

2. EN50126-2:2017 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety

3. Biggs, G., Juknevicius, T., Armonas, A., Post, K.: Integrating safety and reliability analysis into MBSE: overview of the new proposed OMG standard. INCOSE International Symposium, vol. 28, pp. 1322–1336, July 2018.

Acmena

CONTACT US

+61 (0) 478 814 324
enquiries@acmena.com.au
www.acmena.com.au

Acmena Group Pty Ltd
PO BOX 220
Ashgrove West
Brisbane, QLD 4060
ABN: 37 158 514955
ACN: 158 514 955