BowTies for the Digital transformation safety management systems

Coen van Gulijk, Professor, University of Huddersfield, Queensgate HD13DH Huddersfield.

Paul McCulloch, Process Safety & Implementation Consultant, CGE Risk, Vlietweg 17v, 2266 KA, Leidschendam.

The paper shows how the BowTie offers a framework for the digital transformation of safety management systems. The BowTie introduces opportunities for digital transformation on three system levels: barrier system, hazard system and the system management system in its entirety. A concise explanation shows that each of these levels requires different knowledge from safety experts and IT experts alike. The paper includes an insight into the benefits of digital transformation. The case is a transformation on the second level (a hazard system) which is focussed on a railway risk. The work is equally applicable to process safety and all methods are transferrable. This work demonstrates how big-data techniques can add value to chemical safety and paves the way to the widespread introduction of digital safety management systems in the process industries.

Toward digital safety management systems

This paper focuses on the development of a systems approach to digitally-enabled dynamic barrier management. Dynamic barrier management is a key element of safety management that requires the support of digital systems. The approach was developed for the GB railways but it is equally applicable in the chemical industry. The approach is based on the fact that BowTies provide excellent navigation tools for dynamic barrier management. This paper explains how that the digital transformation of dynamic barrier management takes place on three separate transformation levels and demonstrates the suitability of BowTies for the transformation.

The GB railways are exploring the potential for the unremitting ingress of data systems in their industry. One of the areas that much progress was made is in the area of railway safety where the objective is to create a 'safety control centre.' The railway is following the example of the Chemical Industry to monitor the safety condition of the engineering system that is controlled. The UK railway vision was published in RSSB's vision document entitled: 'The Rail Industry's Data and Risk strategy.' This work shows progress toward that vision and the potential use for chemical safety (RSSB, 2017).

With the BowTie it is relatively easy to differentiate between three different transformation processes to support the digital transformation of safety management systems. They are: barriers, hazard systems or BowTies, and the Safety Management System. Without going into the details of the analytics, the paper demonstrates the added value for the hazard system. The work paves the way for the practical introduction of "Big Data" and "Artificial Intelligence" techniques.

Aim

The aim of the IT transformation of safety management systems is to create safety management support systems that deliver safety efficiently, effectively and rapidly. This concept is coined as BDRA or Big Data Risk Analysis. Concisely, it is the application of digital "Big Data" techniques for safety analysis and safety management purposes. Implicitly, this paves the way for the introduction of Artificial Intelligence and Machine Learning into process safety management. The aim of a BDRA Safety Management System is to:

- Extract information from mixed data sources to
- Processes it quickly to infer and present relevant safety management information which
- Combines applications to collectively provide sensible interpretation and
- Uses online interfaces to connect the right people at the right time in order to
- Provide decision support for safety and risk management

This definition guides the development of the IT backbone for Safety Management systems that facilitate AI.

Three levels of transformation

The digital transformation of Safety Management Systems is taking place on three distinct levels. The BowTie provides an excellent platform to explain in what way the levels are different and why they require different methods and expertise.

The first level is the re-engineering of individual barriers based on remote conditioning monitoring; so that is one Threat Barrier or Recovery Measure in figure 2. This approach contains elements of dynamic barrier monitoring and management and allows for the introduction of complex AI algorithms to predict the failure of barriers.

The second level is the re-engineering of a hazard system. In terms of the BowTie that translates into the risk space captured by a single BowTie: all aspects in figure 2. This approach may still be seen as dynamic barrier management but it also captures key elements of the LOPA analysis as it also counts how often hazards and consequence occur and facilitates digital systems to assess barrier efficiency.

The third level is the re-engineering of a Safety Management System in it's entirety: all BowTies capturing all risks in an process plant or perhaps even the entire organization. When that happens, the IT backbone of the Safety Management System has to be re-engineered from the ground up.

The following paragraphs explain the three levels of transformation in some more detail.

Level 1: re-engineering of a barrier system

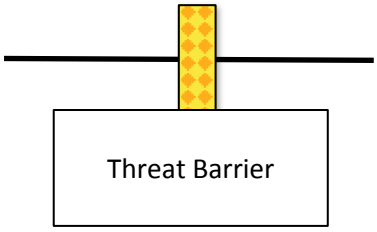

Figure 1: a barrier system in a BowTie.

The first level of digital re-engineering is aimed at individual barriers (see figure 1). This assumes that a barrier is a dedicated safety business process that is designed to control risks, by preventing or mitigating the propagation of threats into consequences.

Let's take an example in the railways: axle box overheating on train wheels. When a bearing on a train malfunctions, it takes more energy to drive the train, it could seize up the wheel and even derail a train. But as bearings wear down they tend to generate more friction and work at higher temperatures. In the distant past, maintenance staff would test the temperature of axle boxes by touching them. However, it was recognized that monitoring the temperature of axle boxes by staff inspection could be inaccurate and unreliable and it was not unheard of that bearings are replaced regardless whether they were at the end of their life service when other bearings appeared worn. As early as 1958 thermal way-side thermal detectors were developed to control this risk. Today Network Rail uses the Hot Axle Box Detection or HABD system that employs 220 thermal detectors across the GB railway network and generates alarms when it detects overheated axle boxes (Huang, 2017). The network that transports data, informs maintenance and stores alarms in a database is what is know as a legacy system: a digital system that was developed in the past.

Even if the HABD system has been around for a while, the technical system is not a simple one. It transports alarm messages from a network of sensors to maintenance staff who follow procedures for the interpretation and follow up of the data which may or may not include visual inspection, further testing and the replacement of the bearing. What complicates this even further is that the system generates false-positives, the identification of the vehicle is not perfect and communication errors occur.

The HABD system as a whole represents a single barrier on a BowTie: a safety control to prevent accidents that could follow from broken bearings. The HABD barrier resides on the left-hand-side of the BowTie: it aims to prevent LoC events by detecting a failure precursor, which lowers the probability for the LoC to materialize. The HABD barrier could be in more than one BowTies: it is in the BowTie that deals with axle failure leading to derailment, but equally it could be on the BowTie that deals with ignition sources leading to fire on a train. Barrier performance for the HABD system can be assessed in terms of dependability: does the barrier always work? It can be assessed in terms of effectively: how often did it prevent reaching the LoC? And it can be assessed in terms of performance: does the safety benefit of the barrier outweigh the cost of the system?

The HABD is also a business process: an ensemble of activities that works aims for safe and reliable trains, utilizes dedicated technical systems, depends on skilled workers, and is embedded in a functional branch of a maintenance organization inside, or working with, the infrastructure manager. Recognizing that the HABD system is a safety barrier in a BowTie and a business process that can be modelled is a key part of the digital re-engineering of safety management systems: ultimately, all barriers are business processes and all barriers record data in one way or another.

The example of the HABD system easily translates into technical systems for process safety control: flare systems collect waste products and products from unplanned and/or accidental leaks and are continuously in operation. They are monitored with dozens, if not hundreds of detectors to assess its operation, they come with their own control and SCADA systems, they are maintained and monitored rigorously and the system may spread to many parts of a plant, in addition to that they are often equipped with complicated flare gas recovery systems. However, from a safety-perspective, the system represents just one barrier system.

From a data perspective, barriers are different in their intensity of data use and the complexity of the analytical functions. For instance, visual inspections yields very little data and usually the data is text based and processed entirely by humans. Vegetation growth detection, CCTV monitoring, or ROV inspection of structural integrity of oil-rigs yield immense amounts of data and requires image analysis.

From a safety perspective all barriers contribute to safety performance, regardless how much data they produce. Both data-heavy and data-light barrier systems have to be taken into account. Also, they have to be effective, efficient and auditable. For that, the business process of the primary process (regardless whether that be train transport or oil-production) has to be

well understood as well as the business process for the barrier. Whether the safety business process depend on prescribed human inspections or remote-conditioning systems that produce massive amounts of data is irrelevant from a safety perspective; but from a digital re-engineering perspective it is hugely relevant.

Level 2: Re-engineering of a hazard system

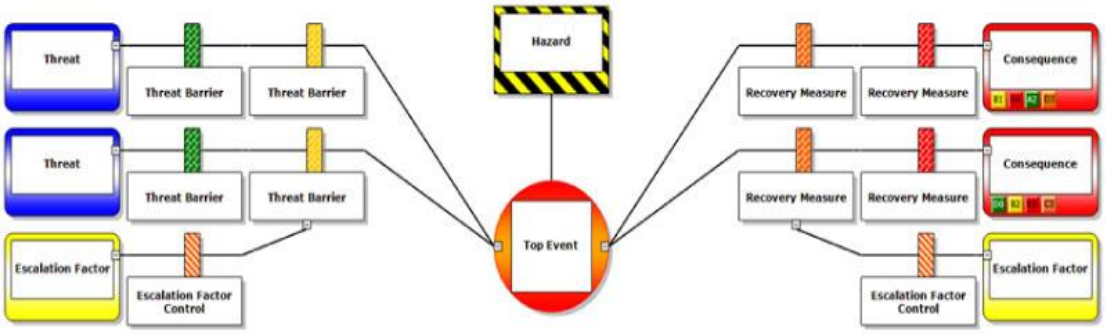

Figure 2: a hazard system, an entire BowTie.

The second level of re-engineering captures a larger part of the safety management system: the hazard system. The simplest form of a hazard system is a LOPA threatline: one LoC, one threat and one consequence with barriers lowering the probability that a hazard propagates into adverse consequences. However, for practical safety management purposes, it is better to capture a larger space: a BowTie that captures one LoC, multiple threats, multiple consequences and relevant barriers (see figure 2).

Re-engineering digital systems to support BowTies integrates barrier systems of individual barriers as well as information in relation to threats, consequences, the hazard and the LoC event. That means that re-engineering of a hazard system is about system integration rather than data gathering and analytics.

Let's take the example of a train passing a red signal, a key safety precursor for safety on the railways. The hazard is the normal business process in which the undesired state emerges: a train in motion. The LoC is the train passing a red signal; once a train passed a red signal, it is uncertain whether it is still safe and safe operation is breached. Threats are observable (real) events or states that, if not controlled, can directly to the LoC event on their own (unassisted by other threats). Threats include defects in train equipment (particularly brakes), low-adhesion conditions, signal obscured, driver errors and communication errors. Barriers include train maintenance, sanders, vegetation management, driver route knowledge training, and communication protocols. So a BowTie does not control a single safety business process but several at the same time: it deals with system integration. That requires different methods and techniques both for safety and IT experts.

First, the different types of information have to come together in terms of a common unit for comparison. Depending on the use of the BowTie the unit of comparison may be based on frequencies (capturing threat occurrence and barrier failure), the unit of comparison may be based on success criteria (indicating whether barriers function as expected), or they may be based on compliance KPI's (to indicate legal compliance, or any other kind of compliance indicator that is sensible in the BowTie's use case). There is less emphasis on advanced analytics and more on harmonization and efficient integration of business processes and data.

Second, a knowledge-model has to be constructed so that key concepts for the BowTie can be harmonized between barrier systems. For technical systems that means that data formats and nomenclature for different barriers and threats have to be linked. For instance, in Close Call near-miss reports a railway signal is simply called a 'the signal at the end of platform 8 in Huddersfield', in the Network Rail Signal database it is identified by a signal area and a number (e.g. Y312), in the Ellipse asset database it has a sixteen-digit unique identifier. The knowledge model facilitates the construction of the data model that is required for the integration of different data-streams.

Third, the data model has to be constructed. The data model governs the actual integration of the data; it informs which parts of the data-streams are relevant for the extraction of performance indicators, which analytics are required for the performance indicators, which data goes where in the BowTie, the frequency of data-updates and so on.

Forth the actual data system, or sandbox, has to be constructed. This, amongst others, involves the computer, communication links, disk space, processors time, user interfaces and IT support.

In terms of the digital re-engineering of the hazard system, the functional system facilitates the control of a significant part of the risk system. In principle, all known hazard systems in the risk systems can be re-engineered in this way. That would, in principle, cover all barriers in the risk system and thereby cover business processes for operational safety control. However, it does not cover safety management systems in its entirety.

Level 3: Re-engineering of a safety management system

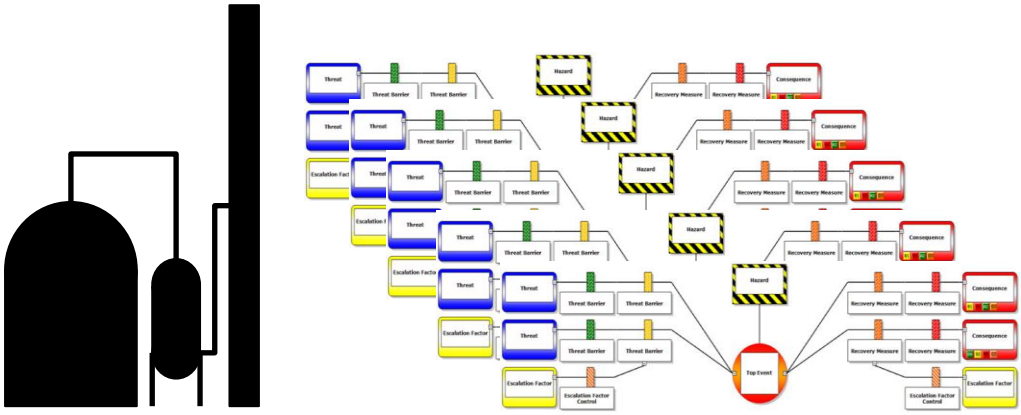

Figure 3: Multiple BowTies in a Safety Management System.

The re-engineering of the SMS as a whole requires the complete overhaul of the Safety Management System for complete integration with digital systems (see figure 3). It entails the complete re-engineering of safety delivery, the safety management system, the HSE department and the skills and tools of safety experts. Instead of having a traditional safety management system that is supported with disaggregated software solutions, software solutions are embedded in an integral digital system that connects all relevant information with the right people at the right time in the right format to achieve the business objectives. IT becomes the backbone of the management system rather than a collection of support system: it becomes an enterprise system that is designed with Enterprise Architecture techniques (EA).

Every EA framework typically embraces a reference enterprise architecture, a planning and implementation methodology, guidelines tools and common vocabulary (Ahlemann et al. 2012). Several alternative EA methodologies can be used to support all aspects of the EA lifecycle though technology complexities, operational uncertainties, changing social realities and evolving businesses. Ultimately, EA brings business advantages such as (TOGAF 2011):

- More efficient business operation
- A more efficient IT operation
- Better support for investment decisions and
- Faster, simpler and cheaper project management and procurement.

The Zachman Framework provides a business approach for Enterprise Architecture. It provides a concise framework to structure and model business views to support the design of enterprise architectures. J. A. Zachman introduced of Enterprise Architecture from his paper title "A Framework for Information Systems Architecture." He wrote it in the IBM systems journal where he presented his Zachman grid to provide an EA framework (Zachman, 1987). The framework defines an enterprise as a two-dimensional classification matrix, based on the intersection of six communication questions (what, where, when, why, who and how) with six rows according to data model transformation perspectives (transformation planner, business owner, system designer, system builder, and subcontractor). The rows and columns create cells where each cell results in an EA activity depending on the system's aspect for a particular stakeholder. The Zachman Framework is the most accessible of the EA frameworks in relation to business process objectives, stakeholder views and selection between alternative options. However, it is less strong in relation to the actual development of software solutions or governance mechanism. The Zachman Framework, although self-described as a framework, is more accurately defined as a taxonomy for organizing architectural artifacts.

Table 1: Overview of Zachman framework.

	What	How	Where	Who	When	Why
Scope	knowledge	business process	locations	stakeholders	events	goals
Business model	semantic model	business model	logistics	work flow	schedule	business plan
System model	logical data model	applications	distributed systems	human interface	processing schedule	business rules

Technology model	physical data model	system design	technology architecture	visual interface	control structure	rule design
Detailed representations	data definition	program	network architecture	work policies	flowsheeting	rule specifications
Functioning enterprise	live data	function	network	organization	schedule	strategy

The Open Group Architecture Framework (TOGAF) is standardized approach that focuses on the process of the development of enterprise architectures. TOGAF is comprehensive with regards to actual re-engineering process involved. TOGAF's view of an enterprise architecture consists of business, application, data and technical architectures.

At the heart of TOGAF is the Architecture Development Method (ADM); a process development model for the re-engineering of systems. It includes architecture views, the knowledge base, repositories for resources, implementation guidelines, templates and background information. It provides a strategy and governance support the designing, planning and implementation of an architecture based on the enterprise requirements.

The TOGAF-Architecture Develop Method (TOGAF-ADM) is a step-by-step process that supports the creation of EA and consists of a preliminary phase, followed by eight transformation phases that guide the users through various levels of architecture maturity in a managed manner through the transition. TOGAF is flexible and allows phases to be performed incompletely, skipped, combined, reordered, or reshaped as per the stakeholder's requirement to fit any organization's needs.

Table 2: TOGAF-ADM.

Step	Description	
A	Preliminary system description	Requirements management
B	Business Architecture	
C	Information systems architecture	
D	Technology architecture	
E	Opportunities and solutions	
F	Migration planning	
G	Implementation governance	
H	Architecture change management	

Enterprise Architecture was introduced to structure enterprise processes and to inform the design of software systems to support them. Enterprise Architecture is the instrument to integrate the constituents of safety management systems. It is a holistic approach to system analysis that is specifically tailored to the needs of IT developers in the sense that it specifies the requirements of the software systems on a high level.

The first step of safety system design is the formulation of aims. On an industry level it is any collection of organizations that have a common set of goals and/or the bottom line for process safety objectives for the plant or the organization as a whole. In addition to that there are financial and operational goals. The enterprise architecture approach provides industry safety systems with clear business objectives, assigns ownership and responsibilities, the blueprint for organizational design and the framework for the IT systems that support safety delivery.

Meta-models are the bridge between enterprise architecture and operational safety delivery systems. Meta-model platforms provide an environment for the framework in which goals, models, rules and constraints are formulated. In IT the meta-model entails a method to design software solutions based on conceptual models, a selection of software solutions and capture of knowledge in ontologies. In this work, the conceptual model is the BowTies, the key software solution is the graph database and knowledge is captured with semantic analysis with NLP techniques and knowledge modeling (Hughes et al. 2018).

Data for integration in a hazard system (Level 2)

This paper treats a use case for safety intelligence on the hazard system level (Level 2). It is beyond the scope of this paper to describe the digital system and the integration of different data-sources. Rather it shows what kind of safety intelligence safety managers can expect from data-integration from different data systems for a single BowTie. The point in case is a railway safety BowTie: a signal passed at danger but the method is transferrable to chemical safety systems.

BowTie meta-model

The meta-model for the BowTie provides the blue-print of the BowTie in an IT system. The approach is based on a three-step approach: defining concepts, describing taxonomical linkage and coding in the IT system. For the BowTie, key concepts are shown in table 3 and the linkage between the concepts are in figure 4. The diagram in figure 6 was coded into a Neo4J database.

Table 3. Definition of elements of a bowtie model.

Concept	**Ontology definition**
Hazard	OBJECT or ACTIVITY which has the potential to cause HARM. It is PART OF the TOP EVENT and is RELEASED by a THREAT
Top event	SCENARIO or UNDESIRED STATE which is PRODUCED in a point of TIME by a THREAT. It is PREVENTED by BARRIERS and RELEASES CONSEQUENCE EVENTS.
Threat	A possible CAUSE that produces a TOP EVENT where the HAZARD is RELEASED. BARRIERS are ATTACHED to specific CAUSES.
Barrier	A MEANS of PREVENTING a TOP EVENT or MODIFYING the CONSEQUENCE EVENTS in order to REDUCE the DAMAGE. It PREVENTS other BARRIERS in a point of TIME and is ATTACHED to a specific THREAT.
Escalation factor	A CONDITION that DEFEATS a BARRIER.
Consequence event	A potential EVENT RELEASED by a TOP EVENT, which directly PRODUCE DAMAGE. This EVENT is MODIFIED by BARRIERS.
Damage	HARM PRODUCED in a CONSEQUENCE EVENT.

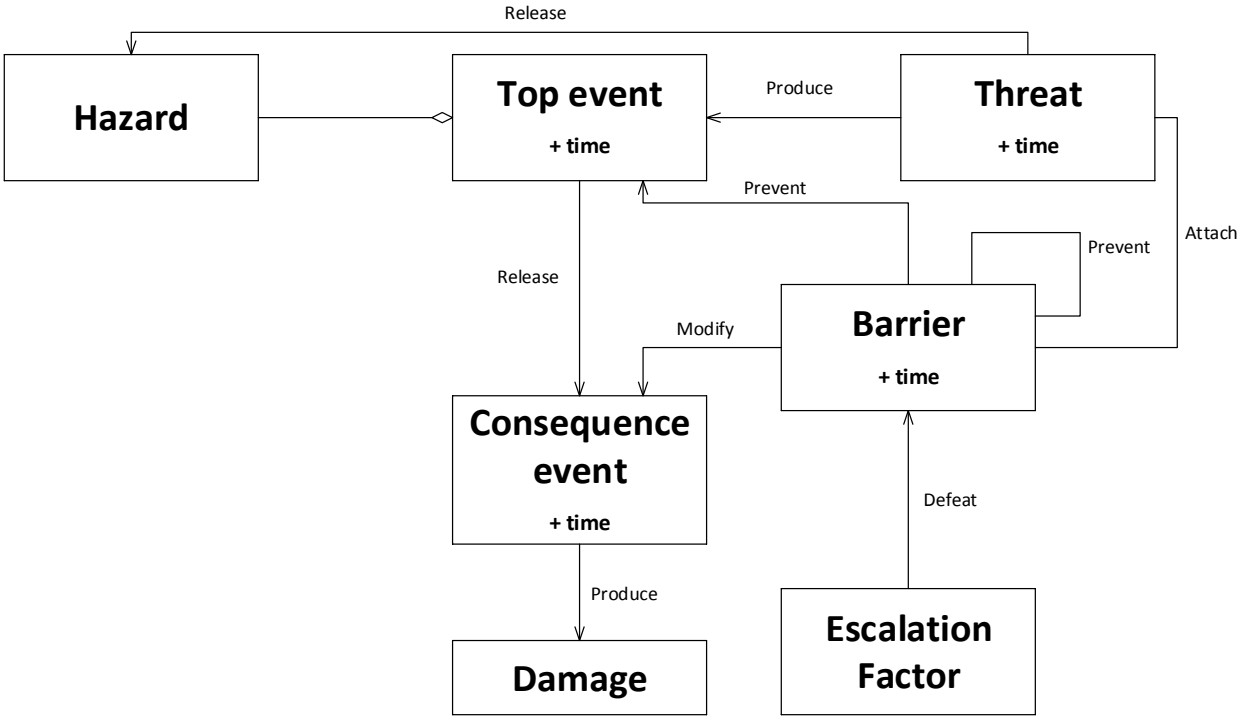

Figure 4: The structure of the BowTie data model.

Data for the BowTie

Three different types of data were connected to the BowTie *viz.* structured incident reports, unstructured near-miss reports and numerical data from train operations.

Incident registrations were used from the Safety Management Intelligence System (SMIS). SMIS is the GB rail industry's national database for recording safety-related events that occur on the rail network in Britain. The latest version of SMIS was launched in March 2017 as part of an industry programme to develop a modern digitized safety reporting system. SMIS is managed by RSSB and it provides online services for incident reporting, data collection, online analysis and sharing of information. Railway organisations such as Network Rail, train and freight operators and construction companies enter about 75,000 events into SMIS each year. Data in SMIS are characterized by pre-defined 'drop down' categories that users fill out (e.g. SPAD risk) but they also contain a lot of text; the latter of which is used in this work. The incident registration system is fundamentally similar to incident registrations in the process industry.

A near-miss reporting system was used: Close Calls (NR, 2018). Close Calls are voluntary and aim to remove immediate risk and improve understanding where improvements can be made by identifying areas of high risk. A Close Call is defined as anything that has the potential to cause harm or damage, but has not led to an accident. Close Calls are essentially text-based reports that contain incident details, descriptions of what could have happened and whether something was done about it. Although there are field for location and personal details, the safety intelligence is captured in the text in Close Calls. The near-miss system is similar to such systems in the process industries.

Numeric data came from train operations and the signalling system: OTDR and RAATS. The data from trains and signals are structured, numerical data similar to SCADA data or measurement data from chemical plants. OTDR is used within the GB Railways to collect data relating to train operations and the state of various train systems throughout a journey, for instance power use, brake controller, train position and driver acknowledgment of signalling system warnings. RAATS combines two types of messages from the wayside signalling system: C-class messages that track train movements from one berth (stretch of rail) into another, and S-class messages that track when signal aspects are changing. RAATS software uses analytics to assess whether a train enters a berth which has a red signal at the end of that berth and thus records which train approaches a red signal. More details can be found in (Zhao et al., 2017). Although the data systems and formats are unique to the railways, the process industry is similarly awash with digital SCADA systems that form the basis for remote safety condition monitoring.

Intelligence from a hazard system (Level 2)

Safety KPI's from numeric data in OTDR and RAATS.

The numeric data from OTDR and RAATS data supplies two technical barriers with relevant information: the automatic warning systems (a system where an alarm is given if the train approaches a red signal and the driver does not responded to timely to an initial warning, and in some instances an automatic trip) and the drivers' reminder appliance (a system that demands that the driver acknowledges safely putting traction power after being stopped at a red-signal). These barriers are threat-line specific and appear in several threat lines, consequently, the results from the analysis are the same for every repeat-instance of the barrier.

Figure 5 presents the results of these barriers in BowTieXP format. The results cover for about 10 days of operation for a single train on the GB railway network which equals about 15 MB of data. The bars in the lower part indicate the drivers' response time to the technical system is adequate; that is to say, the ratio of positive activations (green) and the number of failures (red) is within tolerable limits for these KPI's.

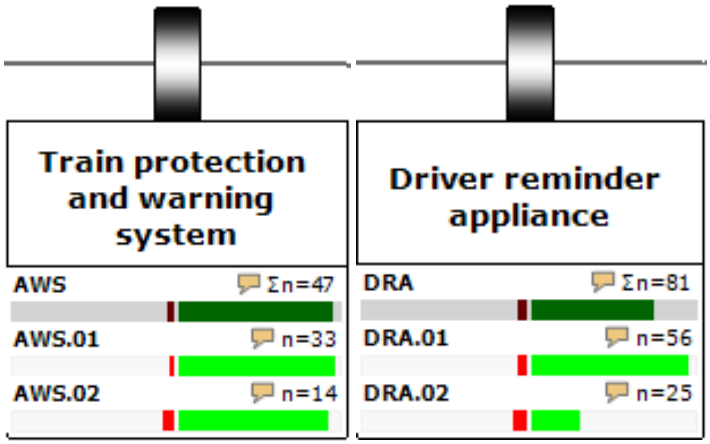

Figure 5: representation of audit questions in BowTieXP barriers.

Threat intelligence from Close Calls

Close Calls are provide intelligence about threats. For this work 327,546 Close Call records were read with computer-supported text analysis and automatically categorized against threat lines (so the threat and the barriers in one threat line in the left-hand side of the BowTie). The classification against threats was manually verified and false positives were removed. Many Close Calls have sufficiently detailed information to map them against individual barriers as well. Some of the Close Calls cannot be mapped against existing threats and represent 'new' threats that are not in the BowTie. Figure 6 shows how the data is represented in BowTieXP (alongside the number of SMIS records associated with the barriers in this threat).

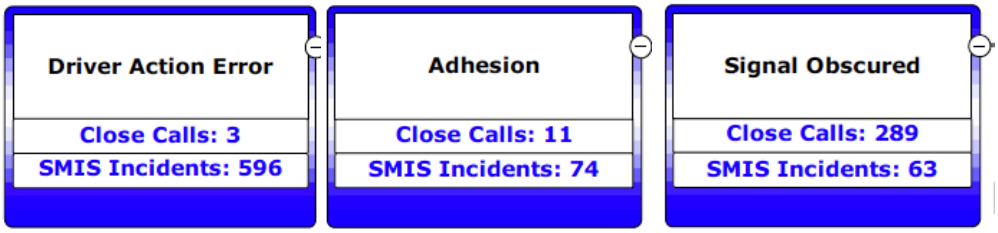

Figure 6: Excerpt from BowTieXP showing Close Calls in threats.

The Close Calls show a number of things. Primarily it shows that not all threat lines are reported about with equal frequency; some threats actually have a very low number of hits. This being a voluntary system to record what might have gone wrong, a reporting bias probably interferes. Another complication is that many Close Calls are written by construction and maintenance staff; train driving is not within their natural reporting scope. Also, the authors of Close Call may not be familiar with all the threats on the BowTie and do not write their Close Calls to align with threat pathways; they simply report what they think might be dangerous. Despite such reporting biases, the Close Calls show that some of the hazards in the BowTie occur relatively frequently and therefore require attention.

Barrier intelligence from SMIS

1520 SPAD incident reports were identified from 406,578 SMIS records between 2012 and 2016. Text analysis was used to classify them against 12 threats and subsequently knowledge-graphs, similar to the one used to describe the BowTie, were used to classify them to the barriers within the threat line. The classification against threats was manually verified and false positives were removed. Figure 7 shows the results as they appear in BowTieXP format, table 7 shows a table of counts.

The results show that practically all threats and barriers are found in the incident records. That means that the threats and the barriers that are in the BowTie are all relevant in SPAD incidents. The results also showed that threats relating to human error dominate. 1057 out of 1520 records are related to human errors. This re-enforces the view that the driver plays an important part when it comes to controlling SPAD risk but it also shows that it is important to maintain the safety barriers in human error threat lines.

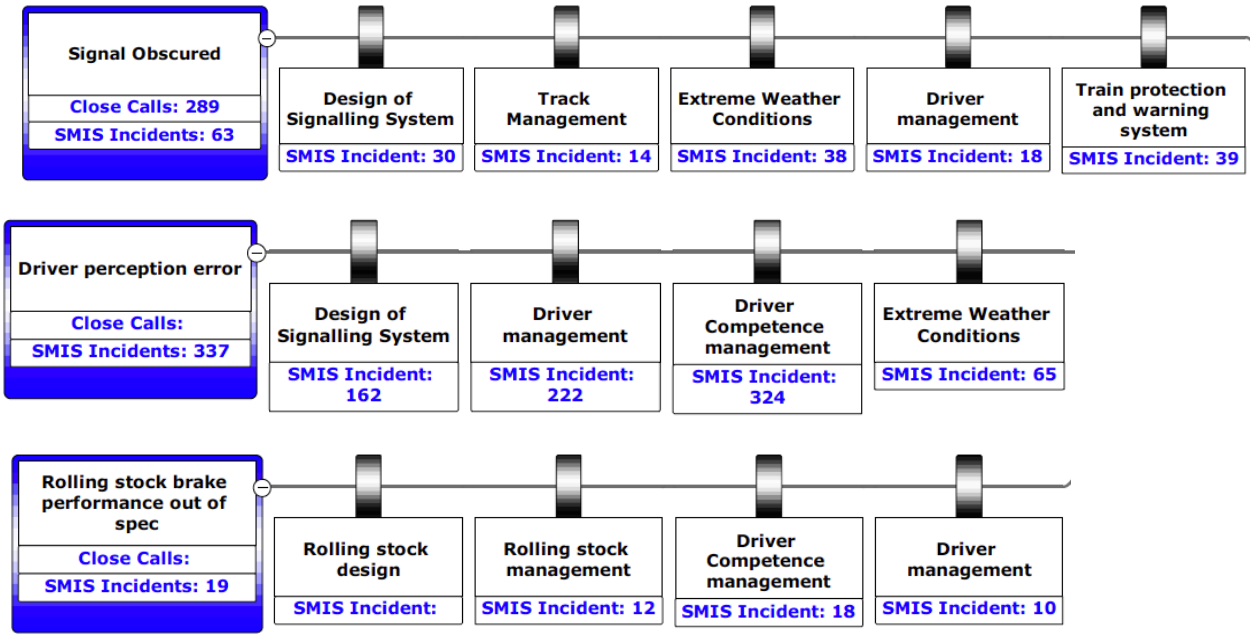

Figure 7: Excerpts from BowTieXP showing SMIS record counts in barriers.

Combined safety intelligence in the BowTie (Level 2).

In the previous sections the analyses of numeric data, near-miss records and incident registrations were treated separately to yield intelligence about audits, threats and barriers, respectively. However, a broader safety intelligence to be found that emerges from the combination of these different types of intelligence in the BowTie.

First, the SMIS intelligence for barriers shows that the barriers for Train protection and warning systems (TPWS) are essential for protection against SPADS. That justifies developing numerically advanced KPI's for the performance of those barriers. As such, data from one system provides support for the extraction of data from another system. Together, the data systems demonstrate that train protection and warning systems are important in the hazard space and therefore require constant management attention.

Cross-referencing between near-misses and incidents shows that near-misses cover a risk that is not well captured in incident records: vegetation management. In that way near-miss records add to the risk profile for the SPAD BowTie: one data-source captures a gap in another data-source. Also, when near-misses and incidents touch upon the same safety barrier, near-misses tend to focus on management issues where incident data emphasizes competence issues. It seems that near-misses are more suited to comment on managerial and procedural errors than incident records are. In that sense near-miss records are complementary to incident records.

A final observation is that where near-miss records overlap with incident records, the number of near-miss records is actually relatively small. This is contrary to the belief that for each incident, a large number of near misses should happen which could be recorded in near-miss records. This difference may be due to the fact that the SPAD risks are not reported through near-miss recording because they are entered by a different group of staff. Without analysis of a second BowTie this cannot be verified but the finding is intriguing because it challenges the traditional view that there should be many near-misses before an accident happens.

Conclusion

This paper sheds light on the inevitable digital re-engineering of safety management system. Digital re-engineering is inevitable because it leads to more efficient business operation, better support for investment decisions and faster, simpler and cheaper project management and procurement (TOGAF 2011).

The BowTie offers an efficient way to monitor the state of safety controls in a chemical plant but it tends to be laborious to populate it with relevant data. This work demonstrates how automatic classification techniques populate of the BowTie with different data-sources and it demonstrates the added value of using multiple data-sources in the same BowTie.

But the BowTie adds even more added value for the digitalization of Safety Management. By the way it is designed it offers a clear structure for the integration of digital barrier management systems and remote condition monitoring. This feature is very important when barriers that use different amounts of data have to be put at par in the operational safety management system. The BowTie also helps explain why different transformation processes require different types of expertise from safety managers and IT specialists: it is not just a matter of introducing artificial intelligence for the prediction of barrier failures, it is also about integration of data-streams and the design of data-systems to support a plant or organization in it's entirety.

Most of this work was performed within the railway industry but the methods and approaches are transferrable to any industry; in fact, the process industry is flooded with digital technologies to monitor safety and the added value for combining data in a BowTie is potentially even more beneficial to the process industries than it is to the railway industry. However, it does mean that safety experts, whether they work in the process industry or elsewhere, will have to increase their understanding of digital transformation processes and the basic lingo of digital safety techniques.

Acknowledgements

RSSB is gratefully acknowledged for co-sponsoring this work.

References

Ahlemann, F. Stettiner, E. Messerschmidt, M. Legner, C. (2012) *Strategic Enterprise Architecture Management: Challenges, Best Practices, and Future Developments.* Springer Heidelberg Dordrecht London New York.

Huang Z (2017) Integrated railway condition monitoring, PhD thesis, University of Birmingham.

Hughes, P., Shipp, D., Figueres-Esteban, M. & Van Gulijk, C. (2018) From free-text structured safety management: introduction of a semi-automated classification method of railway hazard reports to elements on a bow-tie diagram, Safety Science 110, 11-19.

NR (2018) https://safety.networkrail.co.uk/safety/close-call/

RSSB (2017) The Rail Industry's Data and Risk Strategy, Railway Safety and Standards Board, London.

TOGAF Version 9.1. (2011) The Open Group Architecture Framework, Van Haren Publishers, The Netherlands.

Zachman, A. J. (1987) A framework for information systems architecture. *IBM Systems Journal.* 26(3). 276–292.

Zhao, Y., Stow, J. & Harrison, C. (2016) Estimating the frequency of trains approaching red signals – a key to improved understanding of SPAD risk. IET Int. Transp. Systems 11(1): 1–8.