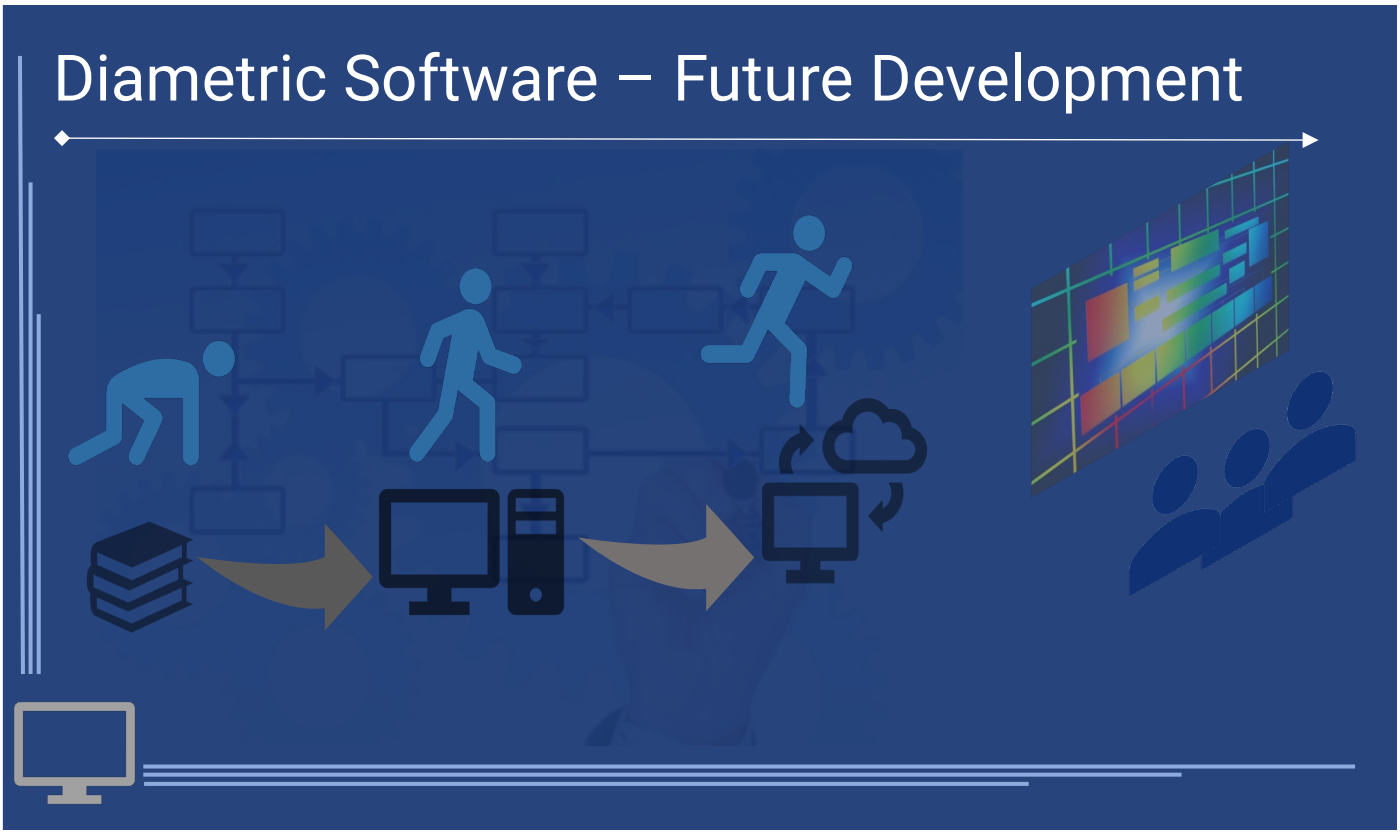
Diametric Software



"We must respect the past and mistrust the present if we wish to provide for the safety of the future."

(Joseph Joubert)

Email: info@diamtetricSoftware.com

Website: www.DiametricSoftware.com

Contents

Executive overview

The development of the Diametric Software for the Safety Manager will be founded on the input and feedback from future customers. This article aims to provide a number of possible developments based on current thinking in the safety management world and on the experience the Diametric team has gained through interactions with customers over the last 5 years.

Safety management continues to evolve and develop as understanding and technical capabilities improve. Governments are increasingly encouraging automation and businesses are continuing to digitise their systems to provide more reliable and effective safety management techniques. This trend, together with more robust and resilient organizational arrangements are moving companies beyond simple compliance to a more proactive and all-inclusive safety environment.

Diametric Software aims to develop the Diametric Safety Manager (DSM) to support Safety System Engineers in this new emerging safety environment. In addition to the development of 'Cloud' based technology and web-based interactions, it is planned to provide and continuously improve the integration of design and operational changes to the safety case. Facilitate the tracking of audits, the review of risks, the provision of an overarching network to manage System-of Systems and the alignment of safety culture precepts with the SMS. The integration of incident reporting systems and the analysis of incident information with hazards and an effective safety project management system will also be developed.

Safety cases and the supporting management systems are in a state of flux and the need to manage the interaction of a number of systems requires the development of new procedures and processes. A solid foundation of hazard analysis, safety case production and risk assessment needs to be incorporated into, and supported by, effective safety management capabilities. The spread, depth and intricacies of such an environment means that new tools need to be developed and introduced to deliver holistic and effective safety management practises. It is the aim of Diametric Software limited to achieve this aim.

This third article looks at how safety cases can be linked to ongoing operations and incident/accident reporting.

Roadmap for the Future

Introduction

Today's approaches for the management of safety, continue to evolve and develop as our understanding and technical capabilities improve. Governments are increasingly encouraging automation and businesses are progressively digitising their systems to provide more reliable and effective safety management techniques. This trend, together with more robust and resilient organizational arrangements are moving companies beyond simple compliance to a more proactive and encompassing safety environment.

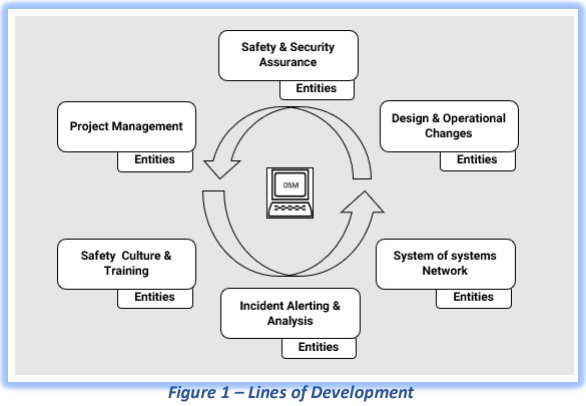


Figure 1 – Lines of Development

However, the safety culture of an organization and a safety management system are distinct and different, where one is based largely on attitudes and beliefs which are somewhat nebulous and unformatted whilst the other is focused on much more precise policies and procedures. To bring these two key aspects together, tracking safety communication, the delivery of training and the development of safety related skills must be continuously aligned with changing policy and regulation. Safety assurance will cover not only adherence to regulation but the effectiveness of the culture. The implementation of safety related recommendations need tracking and constantly reviewing to ensure actions are completed and compliance achieved. Moreover, the need for safety to reflect design changes throughout the *lifecycle* of the system or equipment dictates effective project management across the safety domain.

The complexity of our highly technical systems and the interaction of a number of equipment from dispersed locations have led to the development of an SoS ethos where safety management encompasses a number of distinct but closely related safety cases.

Tracking the development, changes and challenges to this fluid and complex environment calls for more capable and effective management tools. Incident reporting and analysis should be an integral part of and safety management system: the days when a safety case remains locked away in a draw are long gone.

Diametric Software aims to develop the Diametric Safety Manager (DSM) to support Safety System Engineers in this new emerging safety environment. In addition to the development of 'Cloud' based technology and web-based interactions, it is planned to provide and continuously improve the management of design and operational changes to the safety case, the tracking of audits and the review of risks, the

provision of an overarching network to manage SoS, the alignment of safety culture precepts with the SMS, the integration with incident reporting systems and the analysis of incident information with hazard analysis and finally an effective project management system.

Safety Assurance

Effective assurance needs to be driven at all levels of an organization, from executive boards to line managers, and when this happens, the effectiveness of safety management will improve considerably. If managers can review assurance information through an effective and easily accessible tool, they can then take a step back to properly test policies and observe processes.

Delivering effective safety relies on a number of effective practises and should encompass the following properties:

- It can be given and it can be received
- It is dynamic, rather than static
- It combines information (preferably from several sources) and assessments (expert judgements)
- It requires either actions, or a positive decision that no action is needed
- It can apply at different organizational levels, both internally and externally
- It addresses risks, processes and behaviours

Figure 2 – Providing Safety Assurance

Safety assurance within an industry will often have 3 overlapping dimensions: assurance within a company or department, assurance across interfaces with one or more companies or departments, and assurance across the whole of the organizational system. Ensuring that there is a single point of truth across the domains is critical and the DSM will provide that capability. It will capture and encapsulate strategy and key information elements linked for expert assessment, which will be recorded for review and audit. As throughout the management process, actions will be tracked and assigned to organizational elements for follow-up actions. Risk assessment will be captured and continuously updated as part of the assurance process.

Safety-critical domains can also be analysed from a security rather than safety aspect. Recent research shows that, despite the development of new security tools and techniques, successful security attacks are still taking place. The application of security related goals and structures of goals can be just as easily applied to a security system as to a safety case.

Design & Operational Change

The management of change is far more than an assessment of how the safety case is affected, it is about assurance and the need for the Duty Holder to implement changes effectively across the organization. Management of change can generally be broken down into four distinct areas or types:

Design Change

Changes in the design of a system or equipment, whether in the initial stages of introduction or later in the life of the programme, will dictate a review of the safety case and the hazards assessments that is inherent within it. New controls and procedure must be tracked to ensure the correct implementation and compliance and a further risk assessment conducted.

Technical change

The introduction of new technology is a significant change any organization. These can range from new systems or equipment, changes to safety management systems in existing technology, or extensive new training programmes for operational staff.

Operational change

Operational change encompasses the implementation of different operating formations, operating procedures or working practices by the duty holder.

Organizational change

Changes to an organization's structure or size which, without effective management, may introduce risks to the safety aspects of an operation.

In order to implement change effectively, the DSM will enable relationships to be made through safety entities (safety cases, risks, hazards etc) that link to design details, organizational structure, operational procedures, risk assessment and safety case reports. Action lists can be tracked and their status monitored to ensure that changes are implemented properly and on time.

System of Systems integration

In today's high-tech world, there is an increasing trend for more automation and businesses are gradually digitising systems or their System of systems (SoS). This tendency may ultimately result in the removal of skilled people from positions of control and safety must be inherently designed into new automated structures. Examples of these digital SoS include driverless trains, planes or drones, submersibles, and cars however; this trend extends into all industry domains including Health and Defence.

A SoS refers to systems that contain two or more independently managed elements with different parts being subject to different management, investment and control policies.

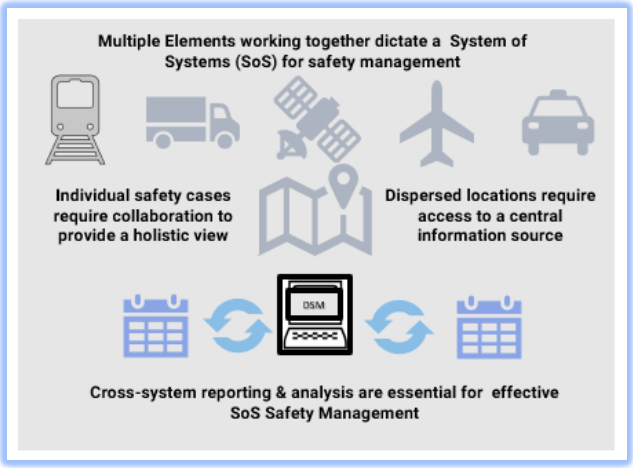


Figure 4 – Linking Systems

- A transport organization will consist of a number of interrelated systems, such as air traffic control, airport management, aircraft operating procedures etc.

- A military operational command like an Army Division or Air Group will consist of many system configurations with a variety of equipment each with its own safety case.

- Such organizations will be under constant safety review and will require active Risk & Hazard management where the Safety Case will play an important role.

- Responsibility for SoS safety and hazard management remains a problem as the people affected may not be in a position to ensure that all elements of the SoS are in a safe state. A deployed Battle Group or ISTAR force will consist of a multitude of systems that will operate in different locations and under different command levels but must still operate safely and effectively.

- The appointment of Duty Holders will be required where it has been assessed that there is credible and reasonably foreseeable risk to life from an activity.

There is clearly a need for designers and safety engineers to introduce a common methodology or framework across the SoS. Changes in one safety case may well require assessment and changes in another and a single source data base will provide the best way of fusing safety tenets together in such a complex environment. If a centrally located (stored in the DSM DB) hazard is updated as part of one safety case the DSM will automatically highlight where else in the SoS it has been used. The same will also occur for changes in design and procedures.

Incident Alerting & Analysis

The purpose of any Safety Case is to identify, assess and address serious risks to equipment, installations and operating procedure before it is too late: they present the best opportunity to prevent accidents before they happen. If changes in design through equipment modification or addition, are not properly assessed against existing hazards or new ones introduced, serious accidents can and will occur. Furthermore, incidents, whether minor or major, must be tracked and assessed against the current safety case to ensure existing hazard controls are adequate and fit for purpose. This is cognisant with a through-life policy for safety cases.

Large organizations will have an incident monitoring and reporting system that will support the reporting, management and analysis of safety occurrences, investigations and recommendations. In most cases, however, the cross-referencing of operational incidents to safety cases hazards remain a convoluted and lengthy process. This may result in lengthy downtimes while thorough investigations are conducted or the late identification of cross-platform applicability ie focusing on one area and not looking at the bigger SoS application.

Figure 5 – Aligning Incidents with Safety Cases

Integration of incidents and accidents into the DSM can be made at a number of levels. A simple key word search through the DSM would highlight related Safety Case and hazard areas which would then drive a more detailed investigation by safety specialists. Incident entities could be created in the DSM into which key data could be imported from the incident management system and then analysed against the Safety Case holdings. Actions could then be tracked to ensure completion.

Safety Culture & Training

In any organization its people are the key to providing effective and efficient safety. A good safety management System needs to encapsulate the safety culture including training, communication and behaviours.

History has shown that linking the safety culture to the Safety Management System is not any easy task and the complexity of these areas can be very challenging to effective integration. Moreover, a safety management system comprises more physical structures, systems and components such as policies procedures and reporting systems whereas the culture of an organization is based on perceptions, attitudes and beliefs which are more unformulated and precise.

Figure 5 – Aligning Incidents with Safety Cases

Nevertheless, alignment of policies, procedures, regulations and directives to safety communications, training and seminars can be achieved through the alignment of key precepts. Observations and recommendations from reviews and audits can be incorporated into lesson plans and safety education. For example, a new operating procedure for the closing of train doors can be easily broken down into a safety communication on why it was introduced, and the results of not following the procedure. Creating a relationship link between the two elements – a training entity and a procedure entity will help identify crossover areas and show reviewers that an active programme exists to bring together safety culture and safety practise.

The production of an ontology used in an organization can help understand the safety environment. Actively questioning processes and procedures to better understand the terminology and the semantics can then be feed into safety culture communications, training packs and safety seminars.

Programme & project management

Effective programme and project management play a critical role in the success of any SMS: they are key tenets that underpin any safety regime. Safety cases must be aligned to and coordinated with design and operational changes, milestones identified and actions tracked, stakeholders managed and effective planning & reporting are all required for successful safety management.

Figure 6 – Linking Safety Culture to the SMS

Using the Extension Editor, the DSM has the ability to create programme and project related fields that can be identified and tracked through queries and matrices. However; a Gannt style presentation, performance tracking and alerting dashboards will contribute significantly to managing safety cases and linking them to the main programme & project plans. Diametric Software Ltd will work closely with future clients to ensure the right capability is delivered.

Summary

Safety cases and the supporting management systems are in a state of flux and the need to manage the interaction of a number of systems requires the development of new procedures and processes. A solid foundation of hazard analysis, safety case production and risk assessment needs to be incorporated into, and supported by, effective safety management capabilities. The spread, depth and intricacies of such an environment means that new tools need to be developed and introduced to deliver holistic and effective safety management practises. It is the aim of Diametric Software limited to achieve this aim.

Andrew J King

Diametric Software

References

- *The "rise of the machine" and the need for a System-of-Systems safety methodology: Mike Brownsworld, Andy German, and In Mitchell*
- *Integrating Data into Safety Assessment Methodology for Defence: Louise Harney*
- *Accidents and Incidents; Viewing the World through Data Eyes: Paul Hampton and Mike Parsons*
- *Beyond arrangements – making the link between safety management and safety culture: Rebecca Canham, Ben McCaulder and Shona Watson*
- *Modelling the Data Safety Guidance: Dave Banham*
- *The Nimrod Review: Charles Haddon-Cave QC*

- *Strategy for regulation of health and safety risks - Management of change: Office of Rail and Road*

- *Modelling the Data Safety Guidance: David Banham*