Diametric Software

The Diametric Safety Case Manager

"The Safety Case shall contain a structured argument demonstrating that the evidence contained therein is sufficient to show that the system is safe. The argument shall be commensurate with the potential risk posed by the system, the complexity of the system and the unfamiliarity of the circumstances involved."

(Ministry of Defence - Defence Standard 00-56)

Email: info@diamtetricSoftware.com
Website: www.DiametricSoftware.com

Contents

Executive overview

Diametric Software is using the latest software to develop a flexible framework for model and diagram editing. This enables us to create component modules for specialist editors and then fuse them together using a common framework. Working with industry to develop the Diametric Software Case Manager (DSM), the initial aim is to produce a stand-alone capability for release in mid-2019 quickly followed by an enterprise product in the next year.

The DSM provides a single point of truth for safety case production and will save systems engineers time and money when implemented as part of a Safety Management System. It has been designed so that the user can align the software to meet their specific needs through editable fields and effective import and export capabilities. The initial capability will embrace Goal Structured Notation diagrams, Hazard and Operability Analysis (HAZOP), Bow-tie analysis and Failure Mode Effects Analysis and Risk Matrices. The user will be able to move seamlessly from cause & effect modelling into hazard analysis and on to risk reduction, all linked to a GSN Safety Case. It will interact with MBSE tools to deliver safety case arguments and reports.

The flexible reporting capability, using queries and matrices, creates reports that can be targeted to answer specific business questions such as "What evidence items are incomplete?" and "What needs to be updated in the safety case?". This fusion of safety management analysis and reporting capability delivers a powerful and user-friendly tool at a very competitive price.

The DSM's core metamodel is composed of entities within packages and allows those entities to be associated with other entities to build business architectures. These architectures are saved in file format (like Word & Excel) rather than in a data base backend for easy configuration management by the client. It allows the ability to cross reference multiple business safety cases and reuse component parts to quickly build additional ones. The effect of change is quickly identified and business rules prevent the addition of false entities while highlighting related areas for review and update. There is a diagram editing system which provides the display & editing function and facilitates query construction and report generation. Model entities have defined data types, each of which can include a relationship with other entities. The DSM will be built with the ability for the User to easily add or amend data fields attached to the entities, thus giving the customer the ability to refine the model to meet their specific needs and requirements. A Safety Case Viewer (SCV) will be available to auditors and regulators free of charge, allowing them to identify and gather the assurance they need for an accurate assessment of the safety case. Rather than implement an entire change control system it will allow the user to store the model files in their own file-based change control tool.

The DSM provides assurance that information is consistent and correctly referenced throughout the safety case and supports rapid analysis and reporting. Its use will give the systems engineer the ability to build up a repository of safety information and processes that will support the effective through life management of a systems safety case with the minimum of effort and time.

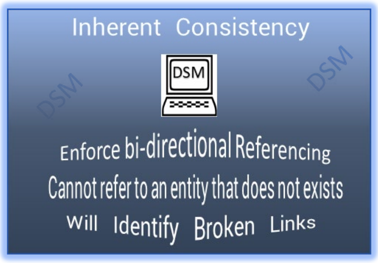
Using the latest software techniques, the DSM is very reliable, can be quickly updated and comes at a very competitive price. It is the next generation of safety information management and safety case production.

The Diametric safety case manager

Introduction

Complexity and constant change are inherent in today’s systems and engineers must adapt methods and procedures in order to provide safety assurance. A single point of truth for safety cases is now a key requirement as they cover the lifecycle of a system through its design and operations phases.

The DSM has built within its Metamodel, a series of entities (within safety related packages) with appropriate data fields that provide a ‘create once and use many times’ scenario for the system engineer. When an entity is updated or amended in one place it is automatically updated and amended in all places where that entity is used. It enforces bi-directional referencing to aid analysis and review and it will identify broken links accordingly. Furthermore, it cannot refer to entities that don’t exist, something that is all too common in paper safety cases that have been amended in one place and not in others. The DSM will allow the Systems Engineer to increase the quality within the Safety Case whilst at the same time reduce costs.


Inherent Consistency
DSM
DSM
DSM
Enforce bi-directional Referencing
Cannot refer to an entity that does not exists
Will Identify Broken Links

DSM software profile

In the search for reliability and cost effectiveness the Diametric Software team has adopted Haskell as its programming language. The language changes the way developers think about programming and we feel more confident our code will work correctly and will have longevity. We are using Haskell to develop a flexible framework for model and diagram editing and it enables us to create component modules for specialist editors and then fuse them together using a common framework. Building Programs using Haskell has several advantages:

- ❖ It provides lower development costs which feeds through to lower licensing & support costs
- ❖ It allows for faster development which means a more responsive and timely delivery
- ❖ It delivers a product with far fewer bugs and thus promotes reliability and confidence

It is the aim of Diametric Software to produce reliable and affordable software for today’s financially challenged markets.

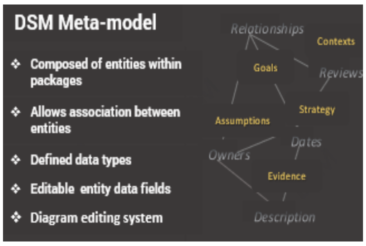
The meta-model

Safety cases are constructed using a number of building blocks such as technical papers, failure mode analysis, hazard analysis, risk management and safety arguments. A hazard might be applicable to a number of safety related areas and similarly with a Goal structure. As safety cases evolve to cover the whole of the life cycle, change and amendment will be a frequent occurrence. As has been said previously, this presents a significant challenge to System Engineers and the DSM meta-model has been designed to address these challenges.

Within the DSM meta-model, entities have been created that represent safety case building blocks:

- Goals
- Strategies
- Contexts
- Events
- Threats
- Requirements
- Justifications
- Assumptions
- Hazards
- Risks
- Controls
- FMEA Entity (Events)
- HAZOP Entity (Events)

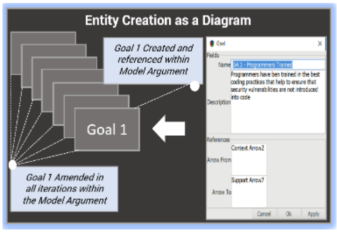
Each entity is grouped into packages with built-in defined data fields and each entity can have a relationship with another entity in the same package or a different one. Thus, associations can be built within the entity packages that deliver a formal structure representing or modelling a safety case argument and this is displayed as a diagram. When an entity (e.g. a hazard mitigation or a GSN argument goal) appears in two diagrams it is still the same entity. An update on one diagram is automatically reflected in the other and thus ensures that all internal references are consistent. Hence each entity is a *single point of truth* about some aspect of the safety case.


DSM Meta-model

- Composed of entities within packages
- Allows association between entities
- Defined data types
- Editable entity data fields
- Diagram editing system

The diagram editor

The DSM has a Diagram Editor that represents safety entities in the form of diagrams that can be easily produced, linked, referenced and edited as required. Goal Structuring Notation (GSN) has been adopted as the best way to portray a safety argument graphically, as it represents the individual elements of any safety argument and the relationships that exist between these elements (i.e. how individual requirements are supported by specific claims, how claims are supported by evidence and the assumed context that is defined for the argument). As stated earlier, the Meta-model ensures that each element of the diagram remains as the single source of truth throughout the model. When an entity is created a window allows meta-data to be added (name and description) and will show references to other entities. The entity itself can also hold a number of other editable data fields that can be used for managing the safety case. This data can be searched for and displayed using the query and matrix facilities explained further on.


Entity Creation as a Diagram
Goal 1 Created and referenced within Model Argument
Goal 1
Goal 1 Amended in all iterations within the Model Argument
Goal
Fields
References
Cancel
Ok
Apply

Name: G4.1 - Programmers Trained

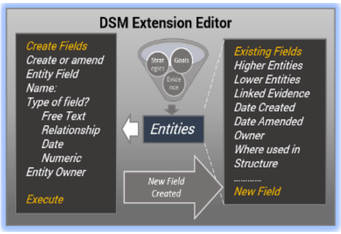
Description: Programmers have ben trained in the best coding practices that help to ensure that security vulnerabilities are not introduced into code

Arrow From: Context Arrow2

Arrow To: Support Arrow7

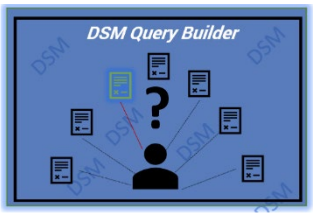
The extension editor

Diametric software recognises the need for a customer to create or amend data fields to meet the individual or organizational data requirements. To that end we have built into the software a field extension editor which will allow the customer to add extension data fields easily and quickly to any type of entity in the model. Once the field has been created (or amended), the Meta-model ensures that all entities in that particular package are automatically updated with the new data. For example, a document could be tagged "Not planned", "Planned", "In progress" or "Issued". A hazard could be "Red", "Amber" or "Green" depending on the overall risk level. For project management, authority, owner, date/time, update and amendment information could be added.



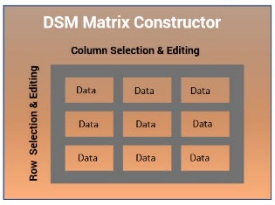
Queries – finding information

In the complex environment of Safety Cases, the ability to analyse the data base is essential if the Customer is to use the DSM effectively. To that end the DSM has a query function that can be used extensively to find safety elements that match a set of criteria. For example, you could write a query to return all Safety case goals that deal with the opening of train doors, in hierarchical order and the supporting evidence. Alternatively, you may wish to search the DSM for any event that leads to a degraded state, 70% or more of the time. As long as the data field is there, it can be used to contribute to a query and a query itself can be used to start another query. They can assemble information from across the model for ease of review and checking for high level consistency. The multiple combinations make queries very powerful but also complex, so the DSM uses the Diagram Editor which allows you to build them in manageable blocks represented as a diagram, test them as you progress and manage them centrally, allowing you to find them easily and re-use them elsewhere. An example of a query is shown in the case study later in this paper.



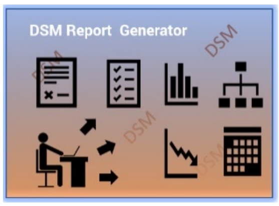
Matrices – displaying information

A matrix is a configurable table that is used by the DSM to display the data required by the systems engineer. They will have a starting or subject element and configurable rows and columns. This will put the data required into the correct form in order to demonstrate a safety concept such as a piece of analysis or an impact assessment on an existing safety case. They can be used by regulators to display results from a search on conformity and by managers to detail progress (or the lack of progress) of a safety case production. Matrices can display the results of a query or a number of queries and when combined with this capability they represent a significant analytic and reporting functionality. More about matrices in the case study.

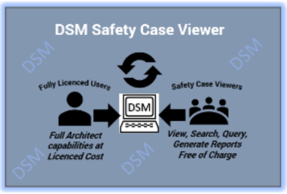


Report generation

The ability to generate reports, whether electronic or paper based is still a requirement in today's system engineering environment. Conventionally, the safety case is still thought of as a report and may regulatory bodies will require a paper-based report for review and filing. Of course, as soon as one report is released it becomes immediately out of date and the importance of the DSM as the single point of truth is further underlined. As new information is added to the safety cases in the DSM, reports can be automatically updated, and regulatory bodies notified. The DSM contains a number of templates for Safety Case Reporting and these can be refined or added to by the customer. The DSM also has the ability to generate documents such as HTML. Microsoft Word. Excel, PDF etc.



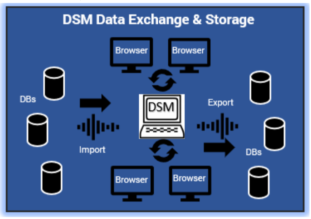
The safety case viewer


DSM Safety Case Viewer
Fully Licenced Users
Safety Case Viewers
DSM
Full Architect capabilities at Licenced Cost
View, Search, Query, Generate Reports Free of Charge
DSM
DSM
DSM
DSM

Working closely with industry, Diametric Software have identified the need for external organizations and regulatory bodies to have access to the safety case information contained in the DSM without the need for a full licence and financial penalty. To that end the DSM contains a Safety Case Viewer (SCV) which will be open to auditors and regulators free of charge. It will allow them to look at safety case diagrams, tables, etc and run any queries already stored in the model. An assessor can search and see the relevant goal structure and dive down into any solutions to examine evidence and changes. Once they have identified the relevant information they can check reports already generated or generate their own report.

Importing, storing & exporting data

Managing importing, storing and exporting data is very important in today's data-centric environment. Some of the data in the safety case peripherals such as Visio Fishbone or Bowtie diagrams are simply not structured well enough and are just too unstable to be easily imported. However; tables of entities, events, caused-effect pairs, hazards etc, *can* be easily imported and the Extension Editor will allow the customer the ability to align DSM internal fields with client external ones. In the next software release, the DSN will also support the import of GSN diagrams in the Adelard Safety Case Editor as well as CSV data from any number of programs.



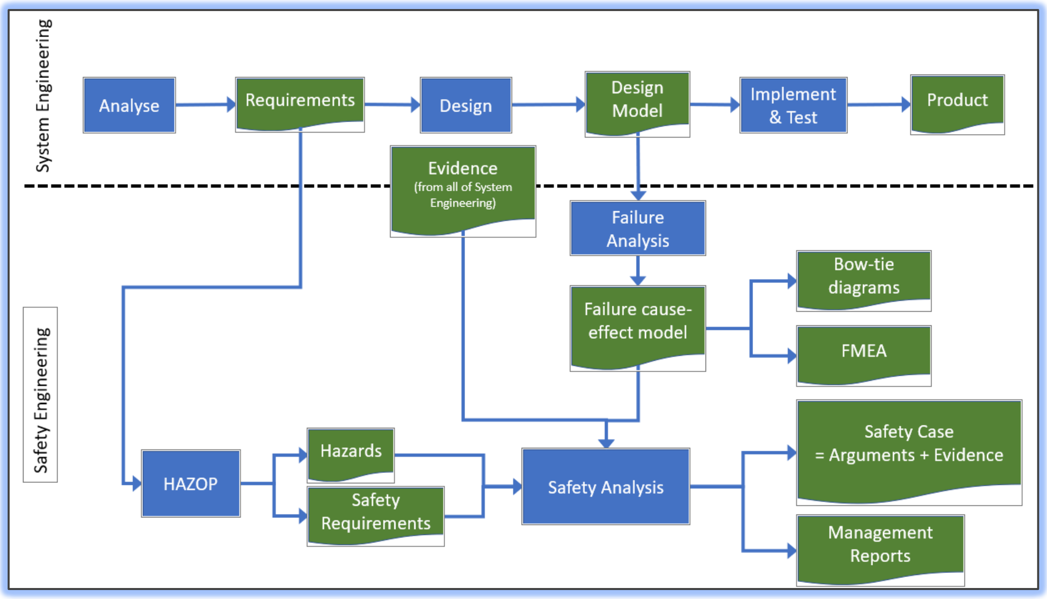
It would be impossible for the DSM to hold all safety data internally. GSN arguments have to be bottomed out with supporting evidence (design documents, standards, review reports etc) and these will be held by the client's document management system such as SharePoint. The DSM supports URL activation through a web browser and also has the functionality to read and write meta-models to disk files. Rather than implement an entire change control system it will allow the user to store the model files in their own file-based change control tool.

The DSM will handle inconsistences in a way that enables the user to understand and fix the inconsistencies. A utility will enable 2-way and 3-way comparisons between different model versions. This will highlight changes and show which version(s) differ. The user will be able to create a reconciled version containing a selected set of differences but will not be able to edit the models in any other way.

Model Based Systems Engineering (MBSE) Interface

As safety cases become more focused on through life cycles, interaction with Model Based Systems Engineering (MBSE) tools will be required. Integration with existing MBSE tools will be achieved through an Excel spreadsheet import/export feature or gateways specifically constructed to extract and return the required data.

The diagram below shows a simplified version of the system engineering process detailing how the safety engineering process takes information from system engineering in order to produce the safety case. Processes are shown in blue, work products in green. The "Evidence" box refers to all the work products produced during system engineering, including process evidence.



The system engineering process

The “Failure Analysis” box and the “Failure cause-effect model” emphasise that the behaviour being modelled here is the system in a failure condition. Normal operation and the response of components to detected failure are part of system engineering, but safety engineering needs to determine the system-level impact of possible failure events. In the past this has been done by manually writing FMEAs as tables and drawing bow-tie diagrams. The DSM provides a formal modelling language for describing the potential failure states of the system from which both bow-tie diagrams and FMEAs can be extracted. In the future it is planned to add numerical modelling of system reliability.

Although they are shown as separate products for simplicity, in practice the FMEA and bow-tie diagrams are part of the evidence that will be incorporated in the final safety case. The cause-effect model may also refer to arguments and evidence elsewhere in the safety case, for instance to demonstrate that a safety control will operate as intended.

DSM analysis tools

The DSM contains the following analysis tools: Hazard and Operability Analysis (HAZOP), Failure Mode Effects Analysis (FMEA), and Bowtie Analysis. Bowtie and FMEA are both different views on the same underlying model of cause and effect. These tools will also be editors in the same way as the GSM, so for instance if you add a cause to a bow-tie diagram, that adds it to the underlying model. The model itself will be very simple: event A can cause events B and C. Hence you can trace possible chains of events from initial cause to possible catastrophe. You can also have a chain of events representing recovery from a particular event. Capturing these events in the DSM is easy, either through on-screen window population or importing from a data base and this simple model can be enhanced in a number of ways to add more sophistication to the analysis:

- Event transitions can have probabilities and dependencies. So we might say that event A will lead to B 10% of the time, B 30% of the time and neither 60% of the time, but not both

- Events can have delays. E.g. "Fan failure will cause overheating after 10 minutes"

- Events can lead to state transitions. E.g. The system is normally in "Operational" state. If a certain component fails, then system enters a "Degraded" state. If the redundant component also fails, then the system enters "Failed" state. Other cause-effect relations can have conditions on the current state.

The key idea here is that once you have populated the model of cause and effect you can then illustrate it using multiple diagrams and matrices to highlight specific aspects. More detail of how the DSM supports these analysis tools is contained in the Case Study later on in this paper.

DSM functionality & Benefits summary

The DSM comes with an impressive array of capabilities and brings with it a significant return on investment. A summary is given below:

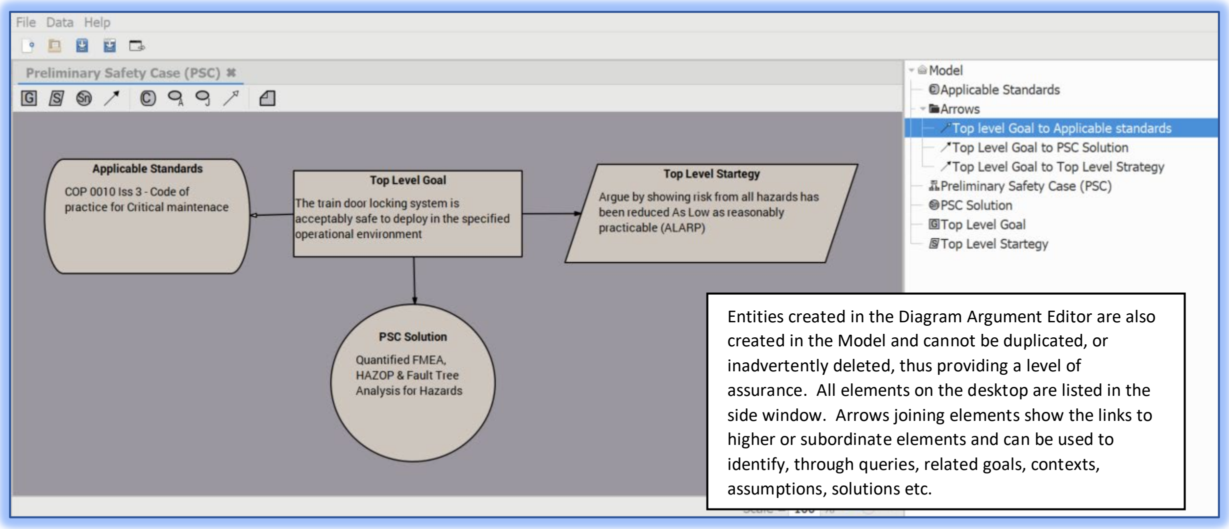
DSM Functionality	DSM Benefits
❖ Provides a single source of truth ❖ Effective safety orientated meta model ❖ Allows association between entities ❖ Extension Editor for data fields ❖ Editable entity data fields ❖ Diagram editing system ❖ Report Generator ❖ Safety Case Viewer ❖ Information Matrix Constructor ❖ Powerful query builder ❖ Inbuilt safety analysis tools ❖ Data Import/Export Capability ❖ MBSE Interfaces	➢ Very competitive software pricing through lower development costs ➢ Reduces cost and risk ➢ Improved quality ➢ Significant time saving ➢ Less prone to errors ➢ Better clarity through simple presentation & easy referencing ➢ Duplication of information prevented ➢ Meta-model provides a single source of truth ➢ Rapid analysis of information ➢ Enforced bi-lateral referencing ➢ Clear and easy navigation & links ➢ Identification of broken links ➢ Consistency across the safety cases ➢ Software more reliable and less prone to bugs ➢ Impact assessments easy to execute ➢ Effective & rapid Change management supported ➢ High level consistency delivered by the use of queries ➢ Flexible data fields allow for easy refinement by the client ➢ No cost facility for external viewers ➢ Data importing and exporting capability ➢ Utilisation of customer document management through URL linking

DSM case study

There are a number of ways of producing a safety case and the case study below does not recommend any particular methodology. The DSM is designed to be flexible to support any of the safety case production processes and the case study shows how the DSM supports some hazard analysis techniques as well as using GSN to build a credible safety argument structure. An example of a GSN argument for a fictional automatic door is detailed below. Using the DSM Diagram Argument Editor, a GSN Argument structure is created and imbedded in the Model for analysis, review and amendment as required. It should be noted that the identification of hazards is a key step to supporting a safety case.

The preliminary safety case

The concept of an evolving Safety Case is good one and will allow the construction of a Safety Case at the earliest possible stage so that hazards are identified and dealt with while the opportunities for their exclusion exist. Any change to the architecture, for safety reasons or otherwise, becomes increasing more difficult and expensive once designs are frozen and components are in manufacture. Most companies therefore, chose to adopt a phased approach to safety case development, beginning with a Preliminary Safety Case (PSC). Using the DSM Diagram Editor, the principle GSN elements for the automatic train door is detailed below.
Obviously further safety case phases may follow to support other phased such new equipment implementation. Each phase can use the preceding phase for refining and adapting the argument structure to meet changes in design and by adding more evidence to support the argument. The DSM capabilities for analysis and display, support these engineering processes by providing a structure in which to identify and document safety activities and processes.


File
Data
Help
Preliminary Safety Case (PSC)
Applicable Standards
Top Level Goal
Top Level Startegy
PSC Solution
Model
Applicable Standards
Arrows
Top level Goal to Applicable standards
Top Level Goal to PSC Solution
Top Level Goal to Top Level Strategy
Preliminary Safety Case (PSC)
PSC Solution
Top Level Goal
Top Level Startegy

COP 0010 Iss 3 - Code of practice for Critical maintenace

The train door locking system is acceptably safe to deploy in the specified operational environment

Argue by showing risk from all hazards has been reduced As Low as reasonably practicable (ALARP)

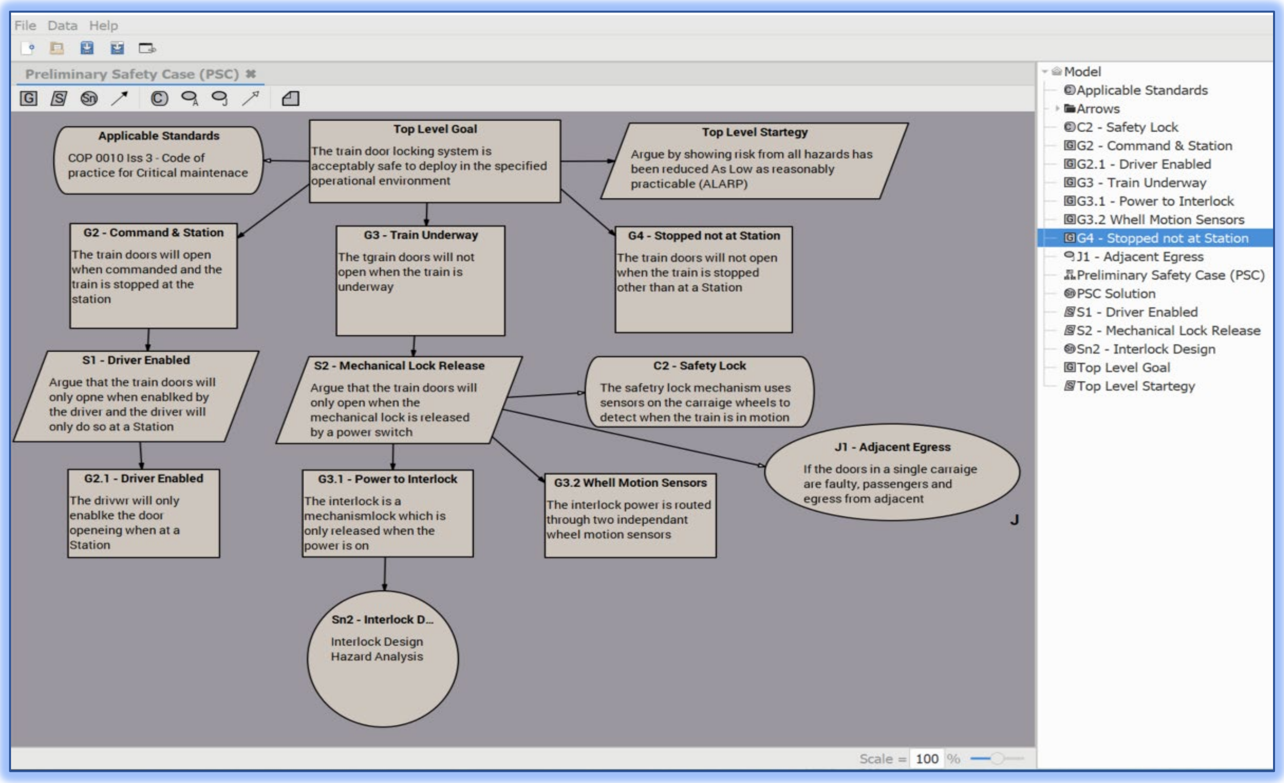
Quantified FMEA, HAZOP & Fault Tree Analysis for Hazards

Entities created in the Diagram Argument Editor are also created in the Model and cannot be duplicated, or inadvertently deleted, thus providing a level of assurance. All elements on the desktop are listed in the side window. Arrows joining elements show the links to higher or subordinate elements and can be used to identify, through queries, related goals, contexts, assumptions, solutions etc.

Building the safety case

Once the principle elements have been established the PSC can be further developed with increased level of detail about the system architecture. In dealing with the complexity of the safety case argument the grouping of hazards by system function provides a logical way to present information and will help make clear the commonality between the evidence presented for the hazards in a group. The DSM Matrix Constructor can quickly generate a matrix showing the functional breakdown of system hazards and this will allow reviewers to quickly identify hazard to function and function to hazard relationships.

The DSM Argument Editor is easy to operate and the user can build complex structures quickly and effectively. Elements can be added in the Explorer bar and dragged on to the desktop where editing can take place and once created are placed in the model. Elements can also be created by clicking the icon on the top menu. A single model entity may appear in multiple diagrams with different graphics, however, an update to one of these diagrams will be propagated to the model and hence other diagrams. A single source of truth.



Applicable Standards
COP 0010 Iss 3 - Code of practice for Critical maintenace

Top Level Goal
The train door locking system is acceptably safe to deploy in the specified operational environment

Top Level Startegy
Argue by showing risk from all hazards has been reduced As Low as reasonably practicable (ALARP)

G2 - Command & Station
The train doors will open when commanded and the train is stopped at the station

G3 - Train Underway
The tgrain doors will not open when the train is underway

G4 - Stopped not at Station
The train doors will not open when the train is stopped other than at a Station

S1 - Driver Enabled
Argue that the train doors will only opne when enablked by the driver and the driver will only do so at a Station

S2 - Mechanical Lock Release
Argue that the train doors will only open when the mechanical lock is released by a power switch

C2 - Safety Lock
The safetry lock mechanism uses sensors on the carraige wheels to detect when the train is in motion

J1 - Adjacent Egress
If the doors in a single carraige are faulty, passengers and egress from adjacent

G2.1 - Driver Enabled
The drivwr will only enablke the door openeing when at a Station

G3.1 - Power to Interlock
The interlock is a mechanismlock which is only released when the power is on

G3.2 Whell Motion Sensors
The interlock power is routed through two independant wheel motion sensors

Sn2 - Interlock D...
Interlock Design Hazard Analysis

In the DSM Argument Editor, the detailed train door lock argument structure is broken down further and using the GSN format it is easy to understand and review.

Challenge to the safety case

When an incident occurs where the train doors unlocked unexpectedly (when the train was underway) a challenge can be made against the original safety case. Using the search facility built into the DSM, the safety Goal G3 is identified and through subordinate goals the Solution Sn3.1 is identified as the source of that challenge ie the interlock design document is not valid. Having reviewed the interlock design hazard analysis and identified that there is no flaw, the GSN takes you to Goal 3.2 and an assessment of whether the sensors were working.
The fault is then identified as a faulty wheel motion sensor and the engineer can then work on a replacement program and search the Safety case for other areas where motion sensors are mentioned – maintenance plans – main engine etc. This avoids detailed manual and lengthy searches of a paper-based safety case.

Access and review

A key requirement of any PSC is that it must be accessible (and acceptable) to all of the engineering and management disciplines involved in the project. At various stages throughout the process of creating the PSC, a range of reviews will be needed and the benefits of the DSM Safety Case Viewer here is readily apparent. Access by engineering and management staff to the relevant sections can be quickly set up and feedback easily captured. The DSM also has the ability to 'snapshot' a fragment of the GSN structure relevant to a particular SME and generate a report, slide or discussion document for publication and review.

Failure mode and effects analysis (FMEA)

The purpose of FMEA is to evaluate the effect of failure modes to determine if design changes are necessary due to unacceptable reliability, safety or operations resulting from potential failure modes. When component failure rates are attached to the identified potential failure modes, a probability of sub-system or component failure can be derived.

The DSM Meta-model contains FMEA entities and each FMEA entity contains the following fields:

- Item/Component
- Failure Mode
- Failure Rate
- Causal factors
- Immediate Effect
- System Effect
- Method of detection
- Current controls
- Hazard
- Risk
- Recommended action

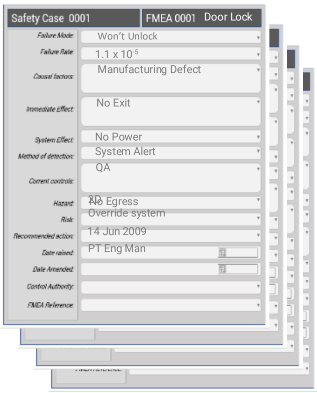
Notes:

1. These fields can be amended, added to or removed according to the requirements of the client using the DSM Field Editor prior to population

2. The failure mode, immediate effect, system effect, hazard, method of detection and controls will all be events. The failure mode (e.g. "Fan failure") will be an event that is linked to an immediate effect event ("train door mechanism overheats"), which in turn is linked to a system effect event ("Door fails to open"), which in turn is linked to a hazard event ("Passengers unable to exit").

3. The FMEA matrix will use queries to extract a tree of possible successor events for each initial trigger event and present them in a tabular format. FMEAs in Excel often have joined cells to create a tree structure, so this should be familiar to the users.

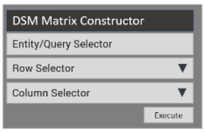
Populating these fields can be done directly through an entity input window on the DSM desktop or imported from a CSV spreadsheet directly into the DSM. It is envisaged that the manipulation of data into the correct format for importing will be carried out externally from the DSM.



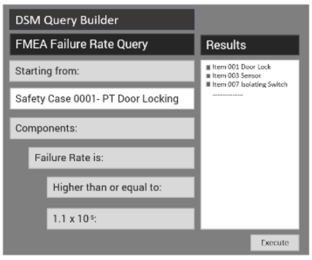
Safety Case 0001 | FMEA 0001 Door Lock

Failure Mode:	Won't Unlock
Failure Rate:	1.1 x 10^{-5}
Causal factors:	Manufacturing Defect
Immediate Effect:	No Exit
System Effect:	No Power
Method of detection:	System Alert
Current controls:	QA
Hazard:	2D No Egress
Risk:	Override system
Recommended action:	14 Jun 2009
Date raised:	PT Eng Man
Date Amended:	
Control Authority:	
FMEA Reference:	

The DSM Matrix Constructor will allow the client to produce FMEA worksheets presenting the data fields in the format of rows and columns they require. The Matrix Constructor can also produce matrices from queries so detailed analysis of the database using queries is quickly replicated in tabular form for review and publishing. The selection and order of columns is easily implemented and different formats can be saved for future use in the same or other safety cases. Links to other documents can also be placed in a matrix produced worksheet. The query builder allows a number of criteria to be applied when searching the database and is a powerful analytical tool. Refined worksheets and analytical tables can be rapidly produced and saved in the data base that can then be used for further review and presentation.



Item	Failure Mode	Failure Rate	Casual Factors	Immediate Effect	System Effect	Method of Detection	Current Controls	Hazard	Risk	Recommended Action	Date Raised	Control Authority
Door Lock	Won't unlock	1.1 x 10^{-5}	Manufacturing defect	No exit	No power	System alert	QA	No egress	2D	Override system	14 Jun 2009	PT Eng Man
	Won't lock	1.1 x 10^{-5}	Manufacturing defect	Door opens in transit	No Power	System alert	QA	Exit while in motion	3D	Override system	14 Jun 2009	PT Eng Mna
Motion Sensor	Fails to work	2.2 x 10^{-5}	Wear & tare	Doors open in transit	No alarm	Electric sensor	Maintenance testing	Exit while in motion	3D	Regular maintenance	12 Apr 2008	PT Eng Man



DSM Query Builder

FMEA Failure Rate Query

Starting from:

Safety Case 0001- PT Door Locking

Components:

Failure Rate is:

Higher than or equal to:

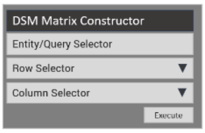
1.1 x 10^{-5}:

Results

- Item 001 Door Lock
- Item 003 Sensor
- Item 007 Isolating Switch

……………

Item	Failure Mode	Failure Rate	Date Raised	Risk	Status
Door Lock	Won't unlock	1.1 x 10^{-5}	Manufacturing defect	2D	Open
	Won't lock	1.1 x 10^{-5}	Manufacturing defect	3D	Open
Motion Sensor	Fails to work	2.2 x 10^{-5}	Wear & tare	3D	Open



Hazard and operability (HAZOP)

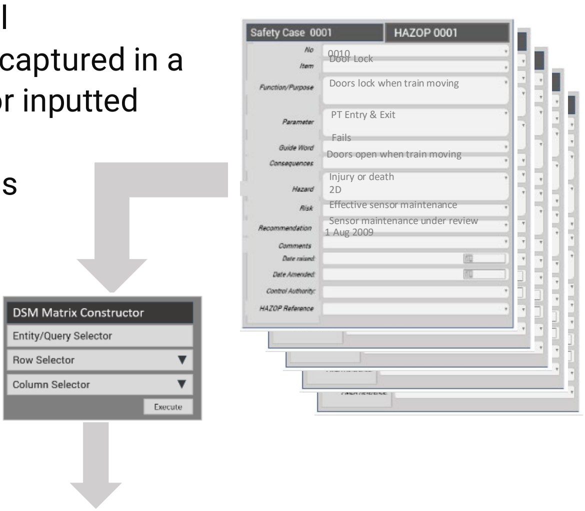
HAZOP analysis is a technique used for identifying and analysing hazards and operational concerns of a system. Its purpose is to identify the potential for the system deviations from intended operational intent through the unique use of key guide words. The potential system deviations then lead to the identification of possible system hazards. Similar in function to an FMEA, the HAZOP uses guide words to ensure that the designs explored in every conceivable manner. Hazards are treated as another type of event. Once the hazardous events are identified the user can then start linking in events representing the causes, effects, controls etc.

- Number
- Item
- Function /purpose
- Parameter
- Guide word
- Consequence
- Cause
- Hazard
- Risk
- Recommendation
- Comments

The HAZOP technique is a detailed hazard analysis utilizing structure and rigor. It is desirable to perform the HAZOP analysis using a specialized worksheet. Although the format of the analysis worksheet is not critical, typically, matrix or column worksheets are used to help maintain focus and structure.

Here the DSM comes to the fore with its Matrix Constructor which builds bespoke worksheets for use by the client. HAZOP entities in the meta-model contain all the necessary fields for effect HAZOP analysis and will share similar fields with the FMEA Entities Hazard, Risk etc so cross technique analysis is enabled.

The HAZOP Analysis is normally carried out by a multidisciplinary team with members being chosen for their individual knowledge and experience. Data can be captured in a spreadsheet and imported into the DSM or inputted directly into the system through a HAZOP data form. Many HAZOP studies can be completed in 5 to 10 meetings, however, for a large project it may take several months. The DSM will assist the team in keeping track of updates and enable rapid review of existing work.



Safety Case 0001 HAZOP 0001

No: 0010
Item: Door Lock
Function/Purpose: Doors lock when train moving
Parameter: PT Entry & Exit
Guide Word: Fails
Consequences: Doors open when train moving
Hazard: Injury or death
Risk: 2D
Recommendation: Effective sensor maintenance
Comments: Sensor maintenance under review
Date raised: 1 Aug 2009
Date Amended:
Control Authority:
HAZOP Reference:

No	Item	Function/Purpose	Parameter	Guide Word	Consequence	Cause	Hazard	Risk	Recommended Action	Comments	Date Raised	Control Authority
0010	Door Lock	PT Entry and Exit	Doors lock when train moving	Fails	Doors open when PT is moving No Power	Sensor failure Power failure	Passenger falls out of train	2D	Effective sensor maintenance Back-up electrical circuit	Sensor maintenance under review	1 Aug 2009 14 Jun 2009	PT Eng Man PT Eng Mna

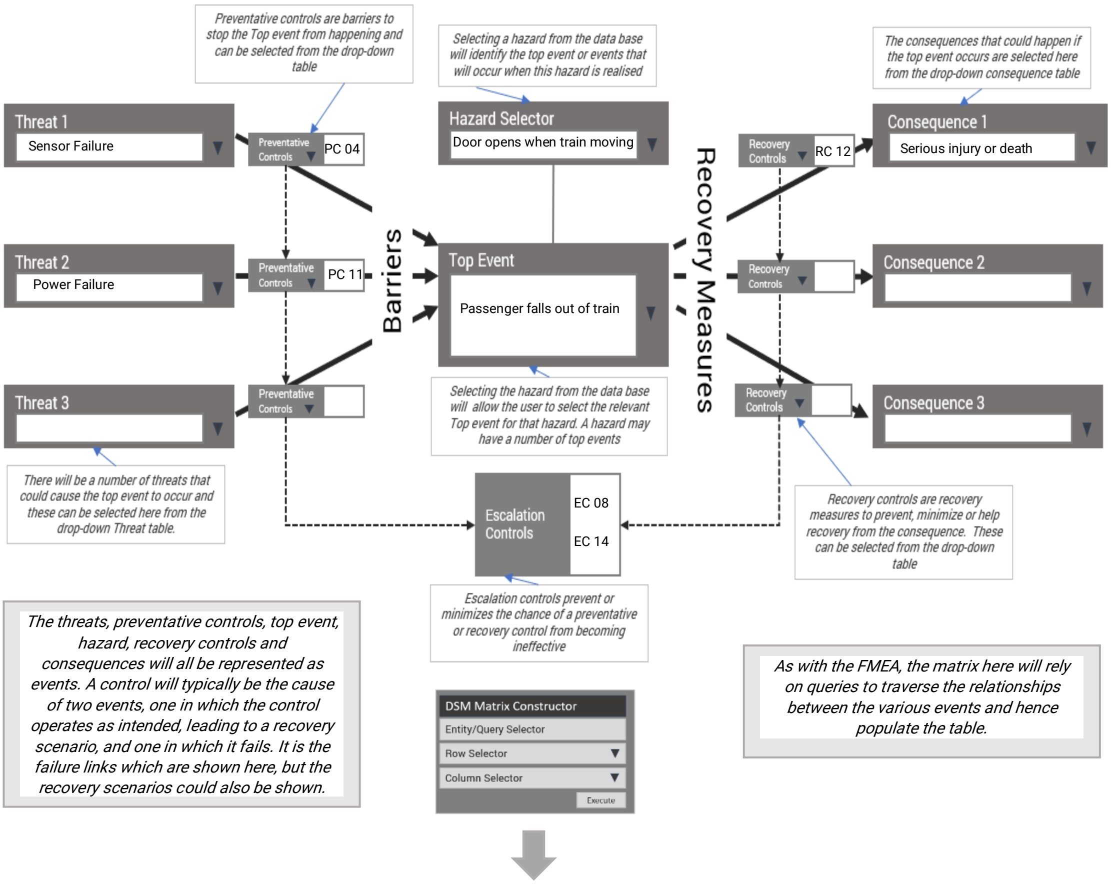
0017	Wheel Motion sensor	Identifies train is moving	Triggers door locking mechanism	Fails	Doors can be opened when train is moving	Ware & Tare	Injury & death	3D	Regular maintenance		12 Apr 2008	PT Eng Man
…….	………	………	…….	……..	……..	…….	……..	…….	……	…….	……	……

Queries can be used to analyse both an FMEA and HAZOP output for similar or missed items/components and with the inherent consistency provided by the DSM the client can be reassured about the correctness of the result.

Effects or consequences can be inputted into the model as an entity of field to an entity and selected in the effects box. Causes or threats can also be entered and selected I for the spines of the fishbone. A more detailed breakdown of causes can then be added to the main cause spine to identify root causes. Each cause can be ranked according to a taxonomy. The diagram can then be exported or shown in a worksheet through the Matrix Constructor.

Bowtie Analysis

Once hazards, their causes and the consequences have been identified and their causes, consequences and controls understood through FMEA or HAZOP, there is a need to manage them by prevention, mitigation and recovery.



Preventative controls are barriers to stop the Top event from happening and can be selected from the drop-down table

Selecting a hazard from the data base will identify the top event or events that will occur when this hazard is realised

The consequences that could happen if the top event occurs are selected here from the drop-down consequence table

Selecting the hazard from the data base will allow the user to select the relevant Top event for that hazard. A hazard may have a number of top events

There will be a number of threats that could cause the top event to occur and these can be selected here from the drop-down Threat table.

Recovery controls are recovery measures to prevent, minimize or help recovery from the consequence. These can be selected from the drop-down table

Escalation controls prevent or minimizes the chance of a preventative or recovery control from becoming ineffective

The threats, preventative controls, top event, hazard, recovery controls and consequences will all be represented as events. A control will typically be the cause of two events, one in which the control operates as intended, leading to a recovery scenario, and one in which it fails. It is the failure links which are shown here, but the recovery scenarios could also be shown.

As with the FMEA, the matrix here will rely on queries to traverse the relationships between the various events and hence populate the table.

Hazard	Top Event	Threats	Consequences	Preventative Controls	Recovery Controls	Escalation Controls
H12: Doors open when train is moving	TE 02: Passenger falls out of train	T01: Movement sensor failure leaves doors unlocked	C001: Serious injury or death to passenger	PC 04 – Indication to Driver that doors are not locked	RC 13: Driver instigates override switch	EC 002: Regular testing of alarm and override system

		T102: Power Failure leaves doors unlocked	C001: Serious injury or death to passenger	PC 11- Back up generator restores power	RC 14: Manual override to lock doors by guard	EC003: Effective training for PT crew
…….	………	………	…….	……..	……..	…….

Bowtie analysis links hazards & consequences to an event and thus makes it possible to develop the relationship to include the causes, or threats, and the prevention & recovery controls. The DSM meta-model contains all these elements (captured in the model during FMEA and HAZOP analysis) and allows the user to select them in the Bow-tie Applicator above. Once selected and saved (the meta-model creates the relationships between entities) the output can be delivered in a matrix as a hazard management worksheet.

Summary

The DSM provides a single point of truth for safety case production and will save systems engineers time and money when implemented as part of a Safety Management System. It has been designed so that the user can quickly align the software to meet the specific needs of the Company through editable fields and effective import, export and linking capabilities.

The DSM provides assurance that information is consistent and correctly referenced throughout the safety case and supports rapid analysis and reporting. Its use will give the systems engineer the ability to build up a repository of safety information and processes that will support the effective through life management of a systems safety case with the minimum of effort and time.

Using the latest software techniques, the DSM is very reliable, can be quickly updated and comes at a very competitive price. It is the next generation of safety information management and safety case production.

Andrew J King

Paul Johnson

Diametric Software

References:

Hazard Analysis Techniques for System Safety - Clifton A Ericson II

Arguing Safety – A Systematic Approach to Managing Safety – Dr Tim Kelly