



The cover of the user manual is set against a dark background with glowing blue and purple circuit board patterns. It features several screenshots of the software interface, including a hazard log, safety case reporting, query & matrix analysis, and data field extensions. A large central title reads "DIAMETRIC SAFETY CASE MANAGER (DSM)". Below it is the subtitle "User Manual v1.2.6". At the bottom left is the date "19 Apr 2021". On the right side, there are three vertical columns of text and diagrams: "Import and Export DSM Files", "Goal Structured Notation", and "Causality Modelling".

"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@diametricsoftware.com

Website: www.DiametricSoftware.com

Contents

<i>Introduction to the Diametric Safety Case Manager(DSM)</i>	6
<i>The DSM Desktop</i>	7
The Model Tree.....	7
The Diagram Window	8
Packages.....	8
<i>Goal Structured Notation (GSN)</i>	9
Diagrams.....	10
Alignment Tools.....	10
GSN Extensions	11
Multiplicity.....	11
Optionality.....	11
Element Abstraction.....	12
Comment Boxes	13
Link Boxes.....	13
Arrows and Relationships	14
<i>Splitting and Merging the Diagram Window</i>	14
<i>Working with Entities</i>	15
Entity Properties.....	15
Creating Extension Fields.....	16
Assigning and Changing Fields.....	18
Diagram Stylesheets.....	18
Creating Model or Package styles in the Model Tree	20
Extension References.....	21
<i>Queries</i>	23
Analysing the Model	23
Query Symbology and Function	24
Building Queries	25
Testing Queries.....	26
Finding Evidence.....	27
Working with Colours	28
<i>Matrices – Presenting the Analysis</i>	29
Constructing a Matrix	30
Adding Columns to the Matrix	31
Running the Matrix.....	33
Adding Another Group to the Matrix.....	34
Adding URL Links to the Matrix.....	35
Adding Lookup Tables to Matrices.....	38
Interacting with a Matrix.....	40
<i>Formulae</i>	41

Useful Analytical Examples	41
Filter Condition.....	43
Formulae in Queries and Matrices	43
Reports.....	44
Generating Reports.....	44
Creating a Report.....	46
Adding Information into a Report.....	47
Previewing Reports.....	50
Publishing Reports.....	50
Cloning Entities.....	51
Importing & Exporting.....	51
Exporting Selected Data & Extensions.....	51
Exporting from a Matrix into Microsoft Excel.....	52
Exporting Diagrams	53
Importing Selected Data & Extensions	54
Importing Data from an Excel File.....	54
Caution.....	54
Bowtie	55
Bowtie Functionality	55
Bowtie Diagrams.....	56
Building the Bowtie	56
Linking the Bowtie Entities	56
Creating Controls.....	57
Assigning Controls	58
Assigning Evidence.....	58
Generating the Output	59
Building the Queries.....	59
Building the Matrix.....	60
Matrix Output	61
Failure Mode & Effects Analysis (FMEA).....	61
FMEA Diagram.....	61
Aligning the FMES with DSM Entities	62
Building the FMEA Matrix	64
Hazard and Operability (HAZOP) Analysis.....	65
Building HAZOP Relationships	65
HAZARD Logs	66
Using Bowtie	67
Hazard Log Queries	67
Hazard Log Matrix	68
Modular Safety Cases.....	69
Creating a Template	69
Exporting and Importing sub-system Safety Cases.....	69

Annex A 71

A1 - Further Details on Formulae	71
A2 - Types of Value.....	71
A3 - DSM Formula Operators:	71
A4 - Handling No-values.....	71
A5 - Functions	72
A6 - Characters	72
A7 - Words.....	72
A8 - Strip.....	72
A9 - Find	72
A10 - Mid.....	72
A11 - Left.....	72
A12 - Right.....	73
A13 - LeftWords, MidWords, RightWords	73
A14 - If	73
A15 - Round.....	73
A16 - Upper, Lower.....	73
A17 - Day, Month, Year	74
A18 - Weekday	74
A19 - DayName, MonthName.....	74
A20 - Today	74
A21 - Lookup.....	74

TABLE OF FIGURES

FIGURE 1: THE DSM DESKTOP	7
FIGURE 2: MODEL TREE	9
FIGURE 3: ALIGNMENT TOOLS.....	10
FIGURE 4: GSN MULTIPLICITY EXTENSIONS (FOR STRUCTURAL ABSTRACTION)	11
FIGURE 5: GSN OPTION ELEMENT.....	11
FIGURE 6: GSN EXTENSIONS FOR ELEMENT ABSTRACTION	12
FIGURE 7: WORKING WITH GSN	12
FIGURE 8: WORKING WITH GSN	13
FIGURE 9: ADDING HYPER LINKS.....	14
FIGURE 10: ARROWS & RELATIONSHIPS	14
FIGURE 11: SPLITTING THE SCREEN	15
FIGURE 12: WORKING WITH ENTITIES.....	16
FIGURE 13: EDITING FIELDS	17
FIGURE 14: ADDING EXTENSION FIELDS	18
FIGURE 15 - SELECTING THE ENTITY TO SHOW DATA FIELDS.....	19
FIGURE 16: ADDING THE FIELDS FROM ENTITIES.....	19
FIGURE 17: FIELDS ADDED TO THE DIAGRAM	20
FIGURE 18: CHANGING ALL DIAGRAMS USING THE MODEL TREE	20
FIGURE 19: EXTENSION REFERENCES	21
FIGURE 20: ADDING ENTITY TYPES TO A REFERENCE FIELD	22
FIGURE 21: REFERENCE TYPE WITH SECOND LINE	22
FIGURE 22: EDITING REFERENCES	23
FIGURE 23: AN EXAMPLE OF A QUERY	24
FIGURE 24: QUERY ALIGNMENT WITH A GSN DIAGRAM	25
FIGURE 25: BUILDING QUERIES.....	26
FIGURE 26: TESTING QUERIES	27
FIGURE 27: FINDING EVIDENCE.....	27
FIGURE 28: BUILDING THE HIGHLIGHT QUERY	28
FIGURE 29: USING THE DIAGRAM APPEARANCE WINDOW	28
FIGURE 30: USING THE COLOUR PALLET.....	29
FIGURE 31: HAZARD LOG EXTRACT MATRIX & DESIGN WINDOW EXAMPLE	29
FIGURE 32: HAZARD QUERY.....	30
FIGURE 33: ADDING THE QUERY TO THE MATRIX DESIGN WINDOW	31
FIGURE 34: ADDING COLUMNS TO THE MATRIX	32
FIGURE 35: ADDING ADDITIONAL COLUMNS TO THE MATRIX	33
FIGURE 36: RUNNING THE MATRIX.....	33
FIGURE 37: POPULATING THE MATRIX.....	34
FIGURE 38: ADDING ANOTHER COLUMN.....	34
FIGURE 39: ADDING ADDITIONAL GROUPS TO A MATRIX	35
FIGURE 40: EVIDENCE MATRIX.....	35
FIGURE 41: BUILDING AND ASSIGNING A URL LINK FIELD	36
FIGURE 42: LINKING A URL TO A COLUMN	36
FIGURE 43: ENTERING THE URL INFORMATION	37
FIGURE 44: ADDING A URL LINK ARROW TO THE MATRIX	37
FIGURE 45: ADDING A LOOKUP TABLE	38
FIGURE 46: BUILDING THE LOOKUP TABLE	39
FIGURE 47: ADDING THE LOOKUP TABLE TO THE MATRIX	39
FIGURE 48: INTERACTING WITH MATRICES	40
FIGURE 49: INTERACTING WITH REFERENCES	41
FIGURE 50: ERROR MESSAGE FROM PARTLY COMPLETED FORMULA.....	43
FIGURE 51: FORMULAE IN QUERIES & MATRICES	43
FIGURE 52: IMPORTING INTO WORD	44
FIGURE 53: CREATING A REPORT IN THE MODEL TREE	44
FIGURE 54: USING A QUERY TO BRING GOAL ENTITIES.....	45

FIGURE 55: USING A SECOND QUERY TO BRING IN GSN DIAGRAMS	46
FIGURE 56: USING A MATRIX TO BRING IN ADDITIONAL DATA	46
FIGURE 57: ANATOMY OF A REPORT	47
FIGURE 58: BUILDING A REPORT	48
FIGURE 59: ADDING A SECTION TO THE REPORT	49
FIGURE 60: ADDING QUERIES TO A SECTION	49
FIGURE 61: ADDING DIAGRAMS AND MATRICES TO A SECTION	50
FIGURE 62: PUBLISHING A REPORT	51
FIGURE 63: EXPORTING SELECTED DATA & EXTENSIONS	52
FIGURE 64: EXPORTING FROM A MATRIX TO EXCEL	53
FIGURE 65: EXPORTING DIAGRAMS	53
FIGURE 66: IMPORTING SELECTED DATA AND EXTENSIONS	54
FIGURE 67: IMPORTING SELECTED DATA FROM A SPREADSHEET	55
FIGURE 68: ENTITY TYPE	55
FIGURE 69: BUILDING THE BOWTIE	56
FIGURE 70: LINKING THE ENTITIES	57
FIGURE 71: CREATING CONTROLS	57
FIGURE 72: ASSIGNING CONTROLS TO A THREAT LINE	58
FIGURE 73: LINKING TO EVIDENCE	58
FIGURE 74: FINDING THE HAZARDS QUERY	59
FIGURE 75: FINDING THE CONTROLS QUERY	60
FIGURE 76: BUILDING A BOWTIE MATRIX	61
FIGURE 77: BOWTIE MATRIX	61
FIGURE 78: AN EXAMPLE OF AN FMEA DIAGRAM	62
FIGURE 79: ALIGNING DSM ENTITIES WITH FMEA FIELDS (1)	62
FIGURE 80: ALIGNING DSM ENTITIES WITH FMEA FIELDS (2)	63
FIGURE 81: ALIGNING DSM ENTITIES WITH FMEA FIELDS (3)	63
FIGURE 82: ASSIGNING CONTROLS TO THREAT LINES	63
FIGURE 83: ASSIGNED CONTROLS IN AN FMEA DIAGRAM	64
FIGURE 84: QUERIES FOR THE FMEA MATRIX	64
FIGURE 85: FMEA MATRIX	65
FIGURE 86: HAZOP DIAGRAM	66
FIGURE 87: CAPTURING THE HAZOP IN THE DSM	66
FIGURE 88: BUILDING A HAZARD LOG USING THE BOWTIE DIAGRAM	67
FIGURE 89: HAZARD LOG QUERIES	68
FIGURE 90: HAZARD LOG CONSTRUCTION	68
FIGURE 91: HAZARD LOG MATRIX EXTRACT	69
FIGURE 92: MODULAR SAFETY CASES	70

Introduction to the Diametric Safety Case Manager(DSM)

The DSM is the next generation safety case management tool that delivers an extensive analysis and reporting capability using the latest development software. It 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.

The guiding philosophy of the DSM is the “single point of truth”. Each fact about the system is represented by a single entity in the model. When the system changes the model can be updated without fear of inconsistency. This in contrast with previous practice where the same fact might be found in different diagrams, tables and documents, making updating the safety case a tedious and error-prone business.

Designed for safety engineers, the DSM stores its data in plain file format rather than in a data base. This allows ease of sharing with safety case contributors and allows version & configuration control to be conducted using the client's own systems. In the DSM you have the flexibility to create your own data field requirements and not have to adhere to a rigid structure. Using data field extensions you can build Hazard Logs, FMEA, HAZOPs etc all of which can be saved as a template or exported into another model. One of the underlying tenets of the DSM is the ability to reuse models, queries, matrices and reports, saving the system engineer time and money.

The DSM Desktop

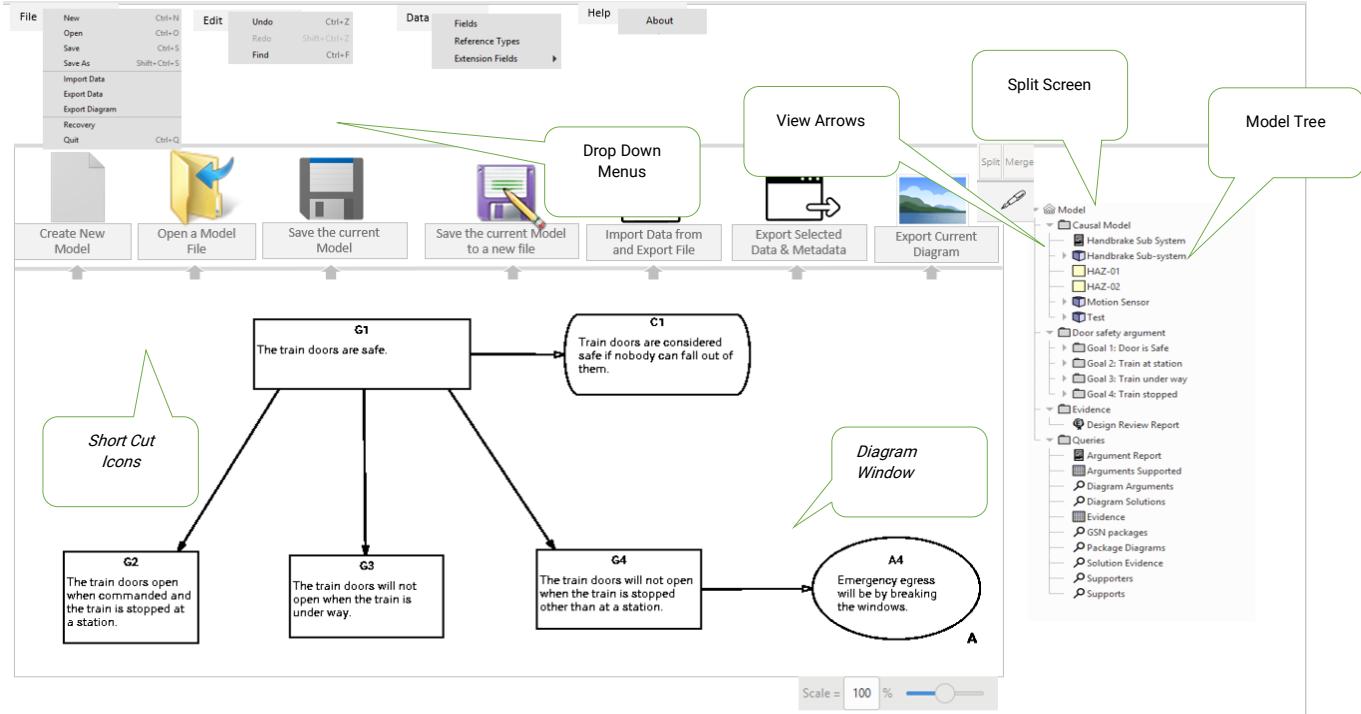


Figure 1: The DSM Desktop

The DSM application has three main areas:

- The toolbar at the top containing menus and short-cut icons.
- The model tree on the right-hand side, showing the contents of the safety case.
- The diagram window, here showing a GSN diagram.

The Model Tree

The Diametric Safety Case Manager (DSM) maintains a model of the arguments and evidence for a safety case. The model is organized as a tree and is shown on the right-hand side of the DSM desktop. Everything in the model can be found in the Model Tree. The individual items in the model tree are known as "entities". Entities come in many different types, and each type has its own icon in the model tree. "Packages" (with the folder icon) are used to organise entities into convenient groups and the Model Tree allows you to create, edit or delete these entities through drop-down menus. Packages can contain sub-packages, and so on without limit.

The meta-model ensures that each entity remains as a single source of truth throughout the model; a single entity can appear in several diagrams and matrices, but when it changes the updated version automatically appears throughout.

When an entity is created a window allows meta-data to be added (name, description, etc) and will show references to other entities. The entity itself can also hold customised data fields known as “extension fields”. This extension data can be searched for and displayed using the query and matrix facilities (See Sections Queries and Matrices – Presenting the Analysis). There are no rules about how entities are organized within packages; users are free to set up their own system. When considering this, bear in mind that queries (See Section Matrices – Presenting the Analysis) can be used to search within packages, so an organization that reflects the overall structure of the safety case will make life easier.

The Diagram Window

The DSM has a diagram window that represents safety entities in the form of diagrams that can be easily produced, linked, referenced and edited as required. The diagram window is also used for editing matrices and reports.

The diagram window has two buttons in the top right-hand corner labelled “Split” and “Merge”. These allow the diagram window to show multiple diagrams at the same time (See Section Splitting and Merging the Diagram Window) for more details of this feature.

The DSM supports the following diagram types:

- Goal Structuring Notation (GSN) represents the individual elements of a safety argument and the relationships that exist between these elements; how individual requirements are supported by specific claims, how claims are supported by evidence and the assumed context that is defined for the argument.
- Bow-tie diagrams represent the high-level relationships between hazards, causal events and controls within the system.

Packages

Packages are folders that hold associated entities. Within the model tree window they can be expanded or collapsed as required. To create a new package right-click on an existing package or the Model icon  at the top and select ‘Add package’. Please note that two entities with the same name cannot appear within a package but can appear in different packages.

Packages are important in managing safety cases. If you number a package as ‘Goal 1.0 ie, it has a dotted sequence of numbers in its title, then the DSM will pick that up and number new goals appropriately. So if you name a Package Goal 1.2, all subsequent Goals in the package will be named 1.2.1, 1.2.2, 1.2.3 etc. This allows you to break down lengthy GSN diagrams into smaller more manageable diagrams in their own packages but still retain the links between packages. The same principle applies to other GSN entities within the Diagram such as Strategies, contexts, assumptions etc. There is more on using packages in Chapter 16 - Modular Safety Cases.

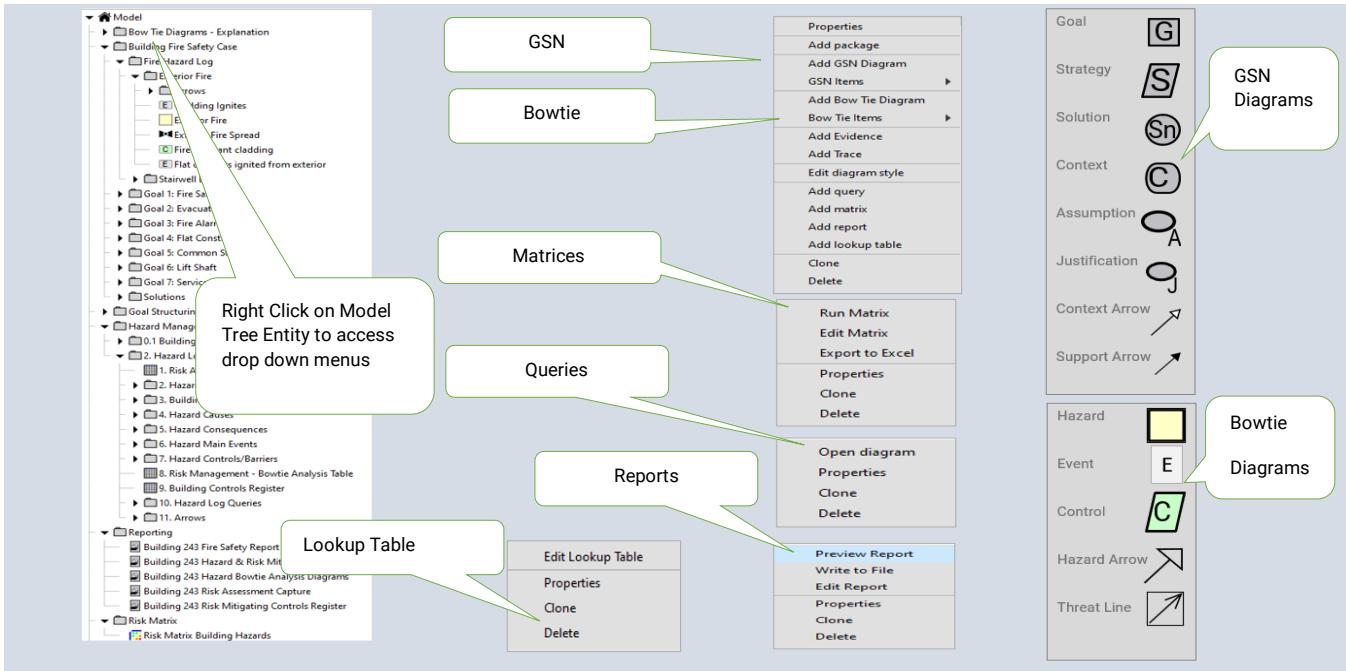


Figure 2: Model Tree

There are a number of different types of icon in the model tree and the key ones are detailed below. Others will be covered under the relevant sections.

Icon	Entity Type
🏠	Model name. This is the root of the model tree and cannot appear anywhere else.
📁	Package containing other entities.
🔍	Query: a way to search the model. (See Section Queries)
📊	Matrix: a tabular list of entities and their contents. (See Section Matrices – Presenting the Analysis)
🖨️	Report: output data from the model to Word or HTML documents. (See Section Reports).
🔢	Lookup table: (See Section Adding Lookup Tables to Matrices)
🔗	Evidence: Links to a GSN Solution providing links to single or multiple documents
➡️➡️➡️	Goal Structuring Notation (GSN) diagram. (See Section Goal Structured Notation (GSN)).
➡️➡️➡️➡️	Bow Tie diagram. (See Section Bowtie)

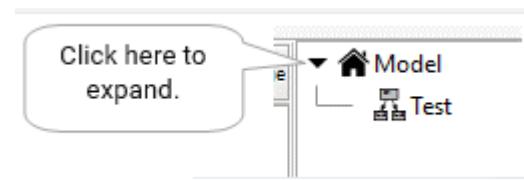
Table 1: Key Icons in the Model tree

Goal Structured Notation (GSN)

Diagrams

This manual assumes a basic familiarity with GSN. For more information see “The Goal Structuring Notation – A Safety Argument Notation” by Tim Kelly and Rob Weaver¹ or the GSN Group website².

To add a GSN diagram right-click on a package or the model root and select “Add GSN Diagram” from the menu. A dialog box will pop up asking for the name of the new diagram. Enter a name and press “OK”. You may need to click on the “expand” chevron in the model tree to see the new diagram.



Once the diagram has been created in the model tree you can double-click it to open it for editing. The diagram has its own toolbar with buttons for creating new entities.

- To create a new Goal box, click on the button and then click and drag on the diagram to indicate the corners of the box. A dialog will appear for you to enter the goal name and description. Create other types of box in the same way.
- To connect two boxes with an arrow, click on the appropriate arrow icon and then click and drag from the start to the finish.

You will find that arrows will stick to boxes when they are connected. Once an arrow is connected to a box you can drag the box around and the arrow will follow. Arrows will only connect boxes in accordance with the rules of GSN. You can create arrows with bends by making several clicks and drags in succession. The arrow will stop when you either join it to a box or make a single click. You can also right-click on an arrow to add or delete a bend. When you create a box or an arrow in a GSN diagram the corresponding entity is automatically added in the same package as the diagram. GSN arrows don't carry much information, so for convenience the DSM automatically creates a separate package called “Arrows” to contain them.

Alignment Tools

There are a number of alignment tools in the DSM that allow to select multiple entities and align them in a number of ways, these are shown below. Simply select the entities you want to align and apply the relevant filter.

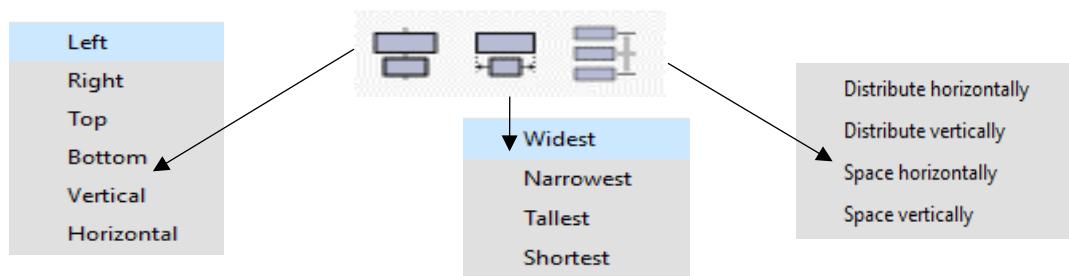


Figure 3: Alignment Tools

¹ <https://www-users.cs.york.ac.uk/tpk/dsn2004.pdf>

² <https://www.goalstructuringnotation.info/>

GSN Extensions

In order to represent patterns of argument rather than merely argument instances, GSN has been extended to support structural and element abstraction and the DSM supports these extensions.

Multiplicity

Multiplicity addresses generalised n-ary relationships between GSN elements.

	A solid ball is the symbol for many (meaning zero or more). The label next to the ball indicates the cardinality of the relationship.
	A hollow ball indicates 'optional' (meaning zero or one).

Figure 4: GSN Multiplicity Extensions (for Structural Abstraction)

Figure 3 illustrates the extensions made to GSN to facilitate the representation of multiplicity. The symbols are designed as decorators or additions to all existing GSN relation types. Multiplicity symbols can be used to describe how many instances of one element-type relate to another.

Optionality

The optionality extension to GSN allows the representation of structural options using the notation. The GSN option symbol is rendered as a solid diamond as shown in diagram 4 however, the DSM represents the option as a diamond with a numerical notation.



A GSN option can be used to denote possible alternatives in satisfying a relationship. It can represent 1-of-n and m-of-n selection, a textual annotation indicating the nature of the choice to be made. In Figure 4, one goal can be supported by any one of three possible sub-goals.

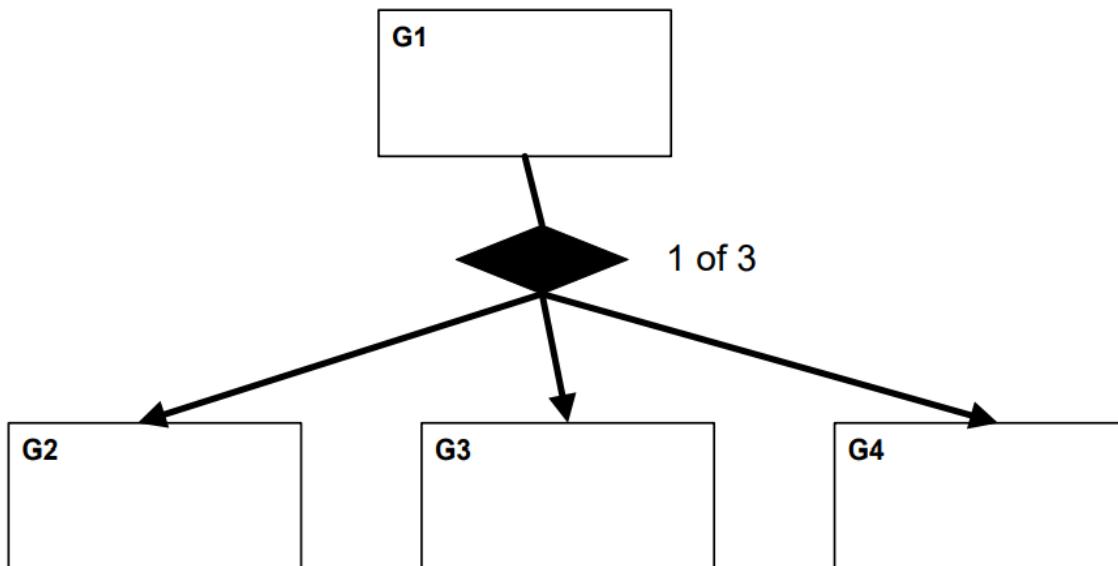


Figure 5: GSN Option Element

Element Abstraction

Element abstraction in GSN is shown in Figure 5. A simple tick box in the properties window of a GSN element allows you to select the appropriate extension.

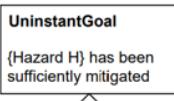
 Uninstantiated Element	This decorator denotes that the attached element remains to be instantiated, i.e. at some later stage the 'abstract' element needs to be replaced (instantiated) with a more concrete instance. This decorator can be applied to any GSN element type and should be applied to the bottom centre of the element.
 UninstantGoal {Hazard H} has been sufficiently mitigated	Example of an uninstantiated goal, demonstrating the application of the decorator. The token to be instantiated is contained within curly brackets.
 Undeveloped & Uninstantiated Element	This decorator denotes that the attached element requires both further development and instantiation. This decorator can be applied to GSN goals and strategies, and should be applied to the bottom centre of the element
 UndevelGoal All hazards have been mitigated	Example of an undeveloped goal, demonstrating the application of the decorator

Figure 6: GSN Extensions for Element Abstraction

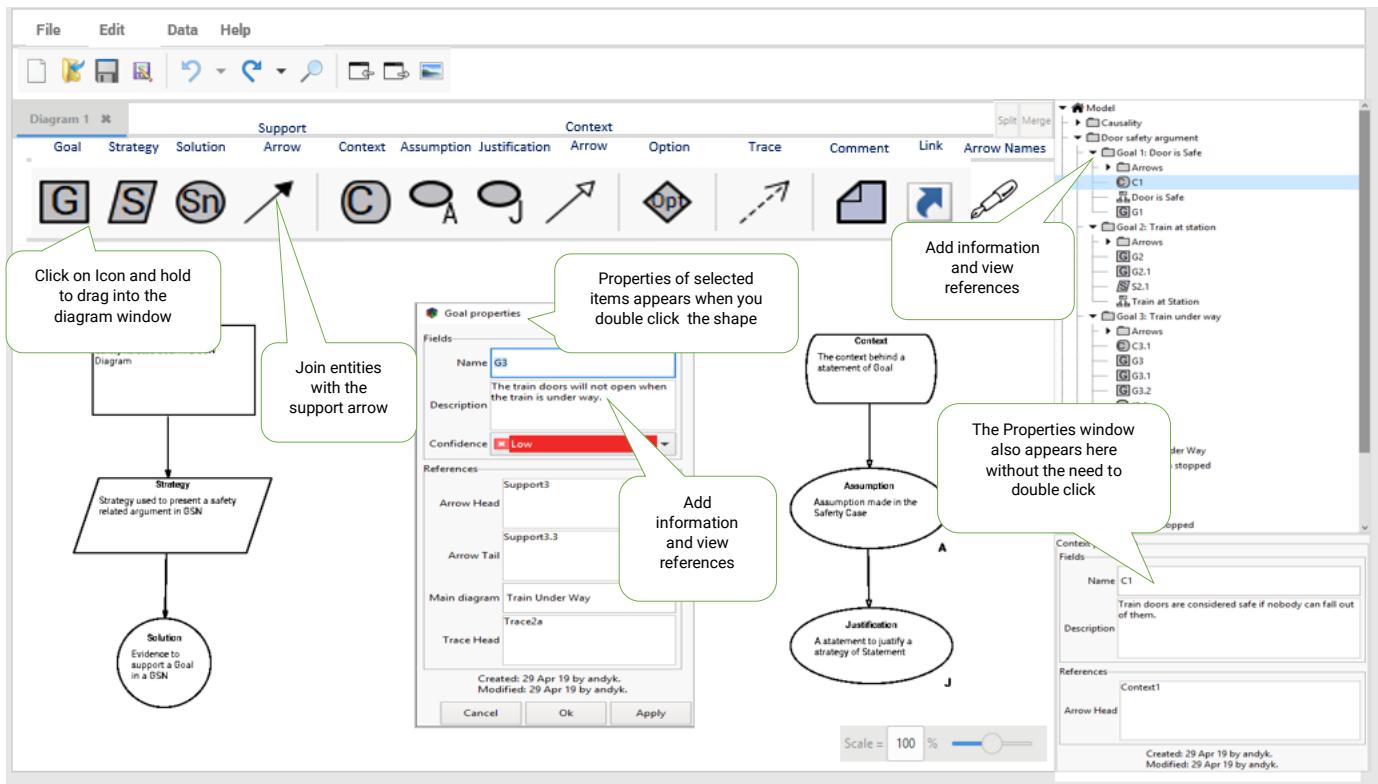


Figure 7: Working with GSN

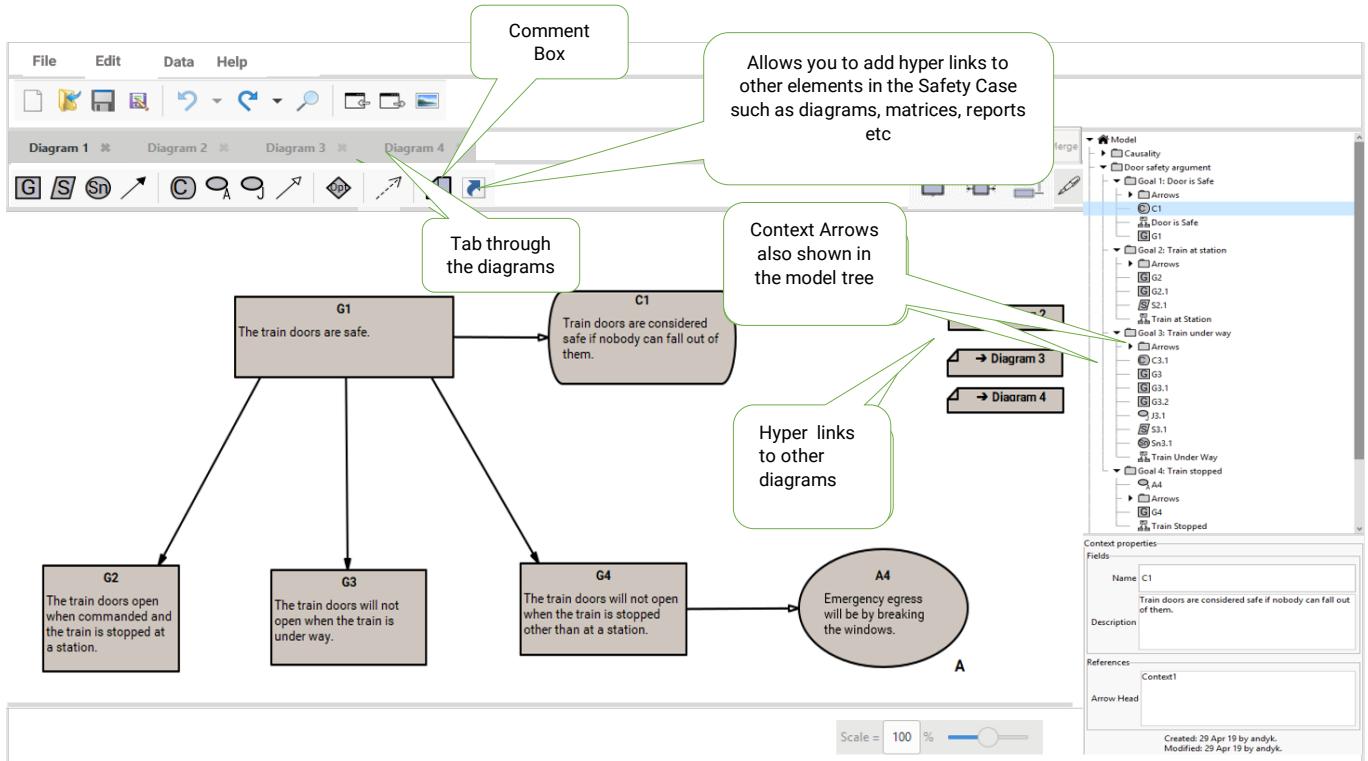


Figure 8: Working with GSN

Comment Boxes

A comment box allows you to add comments to a diagram for better understanding or additional explanation. The comment box is not an entity and so does not appear in the model tree, nor does it link to any other entity. It is just a format for adding notes to a diagram.

Link Boxes

Link boxes allow you to provide a link to other elements in the model tree such as other diagrams or to a matrix or a report. When you click on the Link icon a window will appear where you can select the target for the link and add explanatory text. Left click into Link target window and a single selector window will appear from which you can select the target. Click on the target and it will appear in the window.

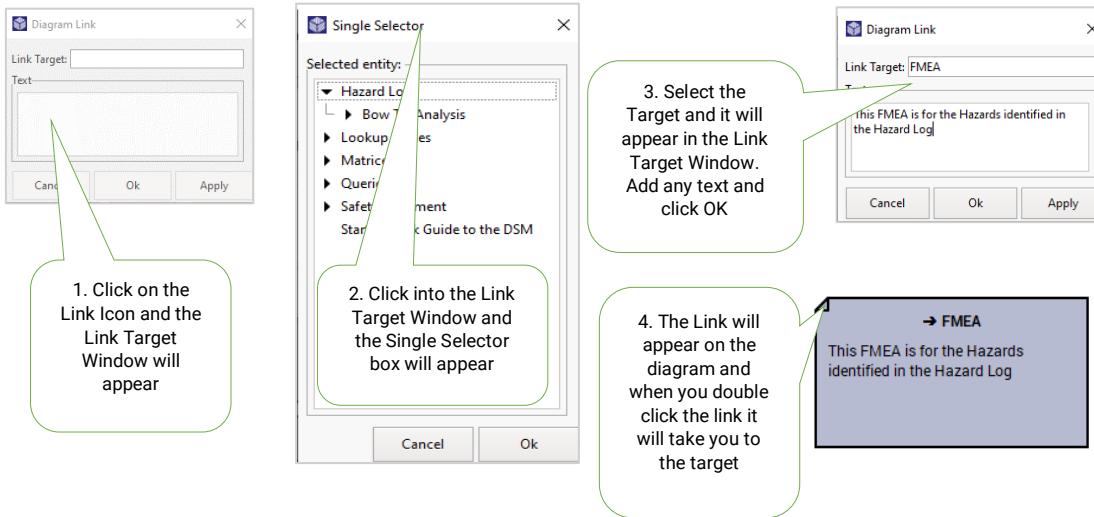


Figure 9: Adding Hyper Links

The simplest way to add a link is to simply drag the entity you wish to link to onto the desktop and the link is created automatically.

Arrows and Relationships

Arrow connections affect the model as well as the diagram. Right-click on an arrow that connects two boxes and select “Properties”. You will get a dialog box showing the arrow name and the names of the boxes at each end, like this:

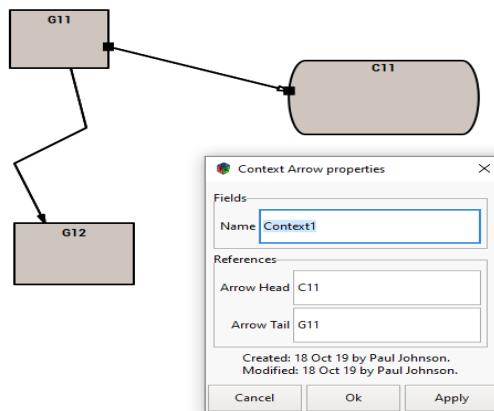


Figure 10: Arrows & Relationships

The properties for boxes G11 and C11 will also show relationships with the arrow (in this case named “Context1”). Other diagram types use boxes and arrows in the same way. Entities or symbols on the desktop are linked using support or context arrows (arrows can hold information in their own right). Hyper-links to other diagrams can be added to allow easy access and clarity with other diagrams. You can also tab through diagrams on the top of the desktop.

Splitting and Merging the Diagram Window

The diagram window in the DSM can be split any number of times using the Split-Merge button at the top right of the screen. The window splits horizontally first, vertically second, then horizontally third and so on. The merge button reverses the

order the windows were split. Be careful to make sure you are clicked onto the right window when you use these features; the inactive windows will be greyed out.

Each separate window can have any number of tabs, each of which shows a different entity. You can rearrange tabs by dragging them from one window to another. When you merge a split window the tabs for the two windows are merged as well.

The scale slider at the bottom of the page will work on the window you have selected. The split windows can also show queries, matrices and reports.

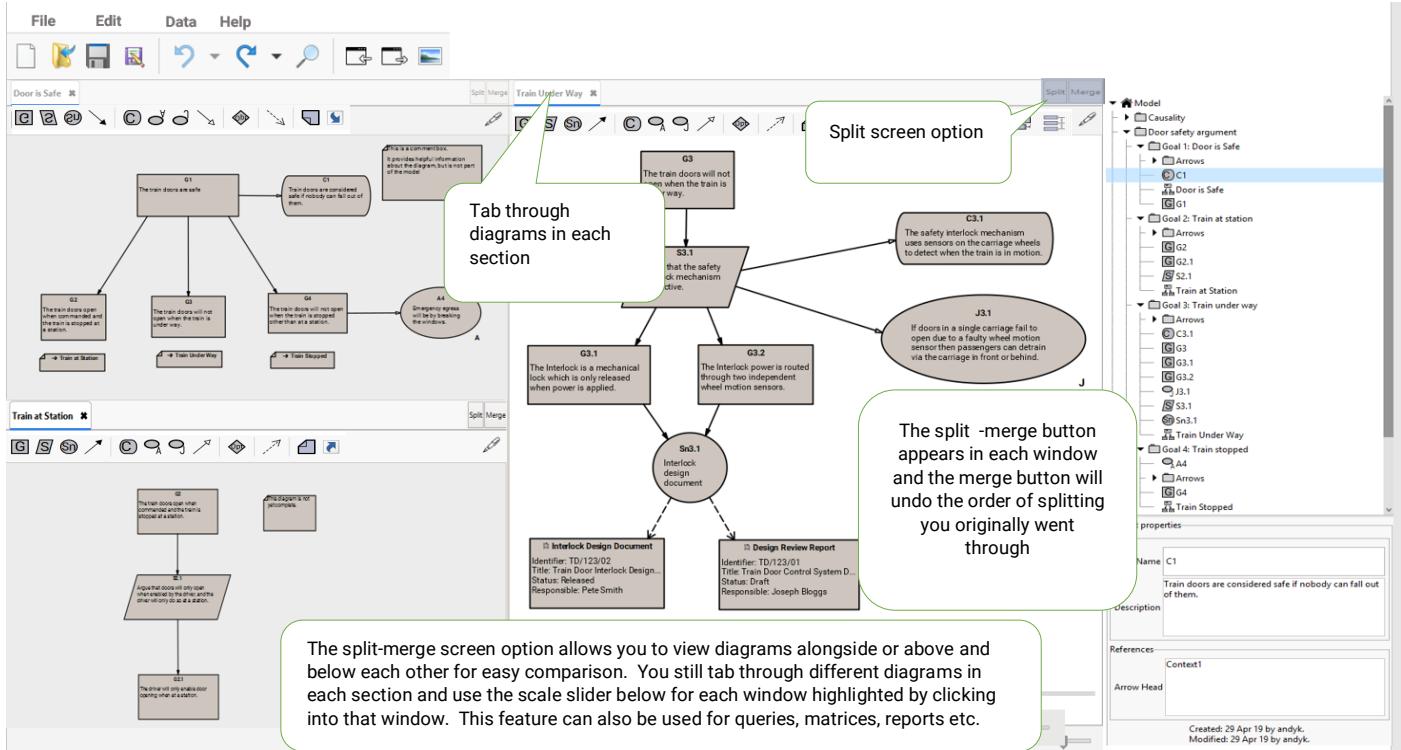


Figure 11: Splitting the Screen

Working with Entities

Diametric Software recognizes the need for customers to extend the built-in data fields to meet the individual or organizational data requirements. To that end a field extension facility has been built into the software which will allow the customer to add extension data fields to any type of entity in the model.

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 can be added.

Entity Properties

Each entity has its own set of properties, some of which are built in and other which are added by the user.

There are two kinds of property:

Fields hold simple data such as numbers or text.

References hold links to other entities. These links are always reciprocal; if a reference is added to one entity then it will also appear in the referenced entity. References are used to hold the connections between boxes and arrows, but you can add your own references too.

References are not the same thing as arrows. When you draw an arrow on a diagram it is created as a separate entity. This arrow entity has references called “Arrow-head” and “Arrow Tail” which link it to the boxes at each end.

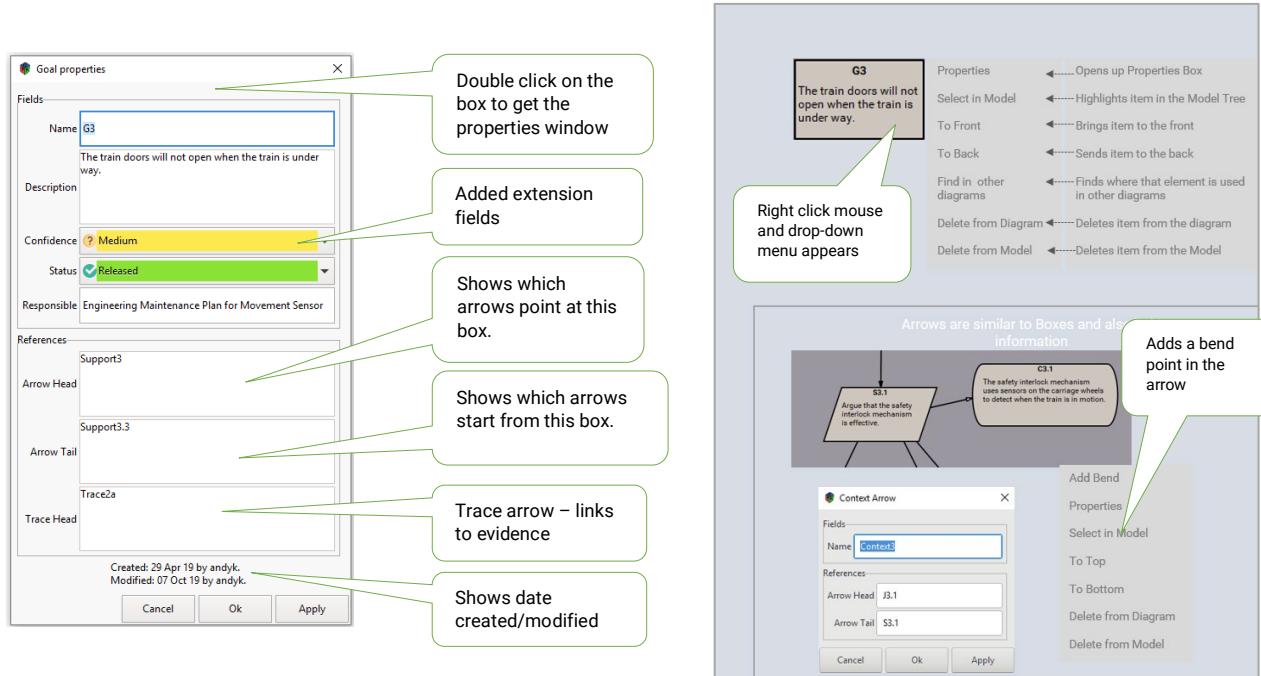


Figure 12: Working with Entities

Creating Extension Fields

The DSM allows you to create your own data fields and add them to entities as required. Click on the Data menu and select ‘Fields’ to access the Fields window. This window will show you what fields are already in the Model with columns for ‘Name’, ‘Multiplicity’ and ‘Type’.

- Multiplicity says whether the field is required or is merely optional.
- Type defines whether the field is a string, a number, a Boolean (ie “Yes” or “No”) or an enumeration (i.e. selected from a fixed list of values). It can also define “decorations”; colours and icons associated with different values

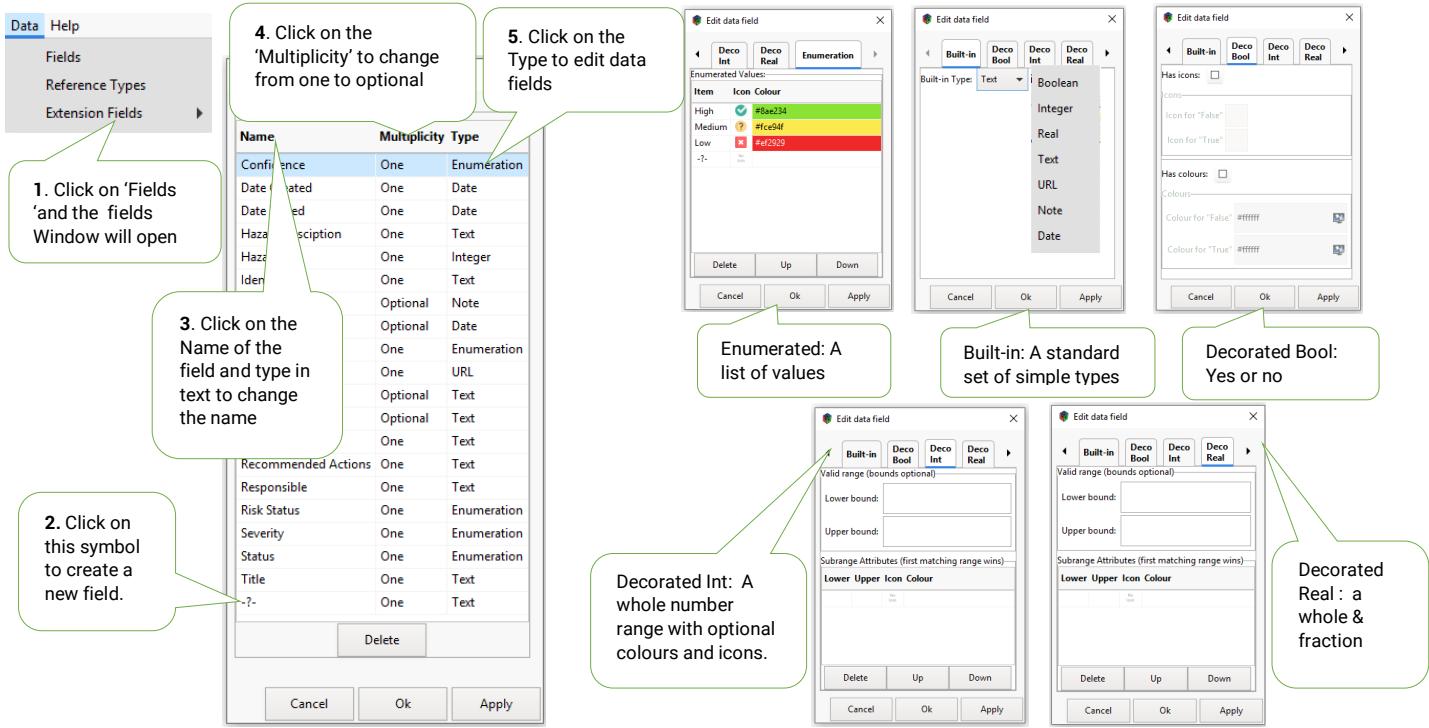


Figure 13: Editing Fields

Once you have created a new field, write the name of the field you require, chose 'one' or 'optional' and click on type to select the type of field. The following field types are available by selecting the tab at the top of the dialog. Note that some tabs are off to the right: click on the right-arrow to get to them.

Built-in – A standard set of simple types:

Boolean: A yes/no value.

Integer: A whole number, such as 42.

Real: A number that may include fractions, such as 3.14195.

Text: A short one-line piece of text, such as a name. This should not be used for anything more than two or three words because matrices will display the entire text on one line.

Date: A calendar date.

Note: Any text that is expected to be more than two or three words. It can contain multiple paragraphs.

URL: A hyperlink to a document or other thing either on the World Wide Web or your company Intranet.

Decorated Bool – Yes or No, but with icons and colours associated with each.

Enumerated – A list of values, such as "High", "Medium" and "Low". Each value can have an icon and colour associated with it.

Decorated Int – A whole number which can be restricted to a range and optionally have colours and icons associated with sub-ranges (e.g. red for 0-3, yellow for 4-7, green for 8-10).

Decorated Real – As for Decorated Int but allowing fractional numbers.

Assigning and Changing Fields

Once you have built the type of field you want you can then assign it to any of the entities and then use formulae, queries and matrices to access the data stored there. When you click on ‘Data’ then ‘Extension Fields’, a list of entities will appear for selection. Click on the required entity and the ‘Field Extension’ window will appear. As with ‘Creating New Fields’ you click on the symbol and a drop-down list of existing fields will appear for selection.

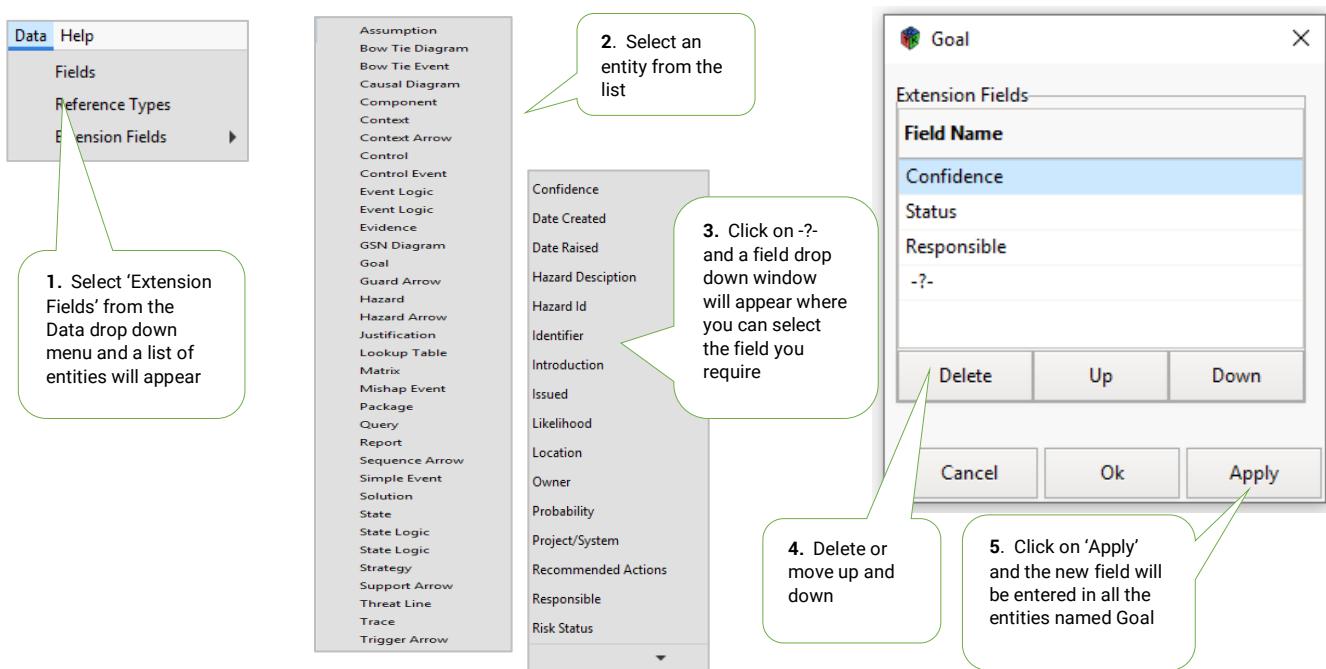


Figure 14: Adding Extension Fields

Diagram Stylesheets

When viewing entities in GSN, or Bowtie the safety case manager will find it useful to see some of the data fields sitting behind the entity. The GSN does this through Diagram Stylesheets.

Select a diagram you wish to edit (in this case a Bowtie Diagram) and click on the pen symbol at the top right-hand side of the page. A window will appear as shown below with an arrow labels selection menu and two columns. We will cover the ‘Highlights’ column later in the chapter on queries. The ‘Show Fields’ column is where you select the type of data fields you wish to see in the diagram.

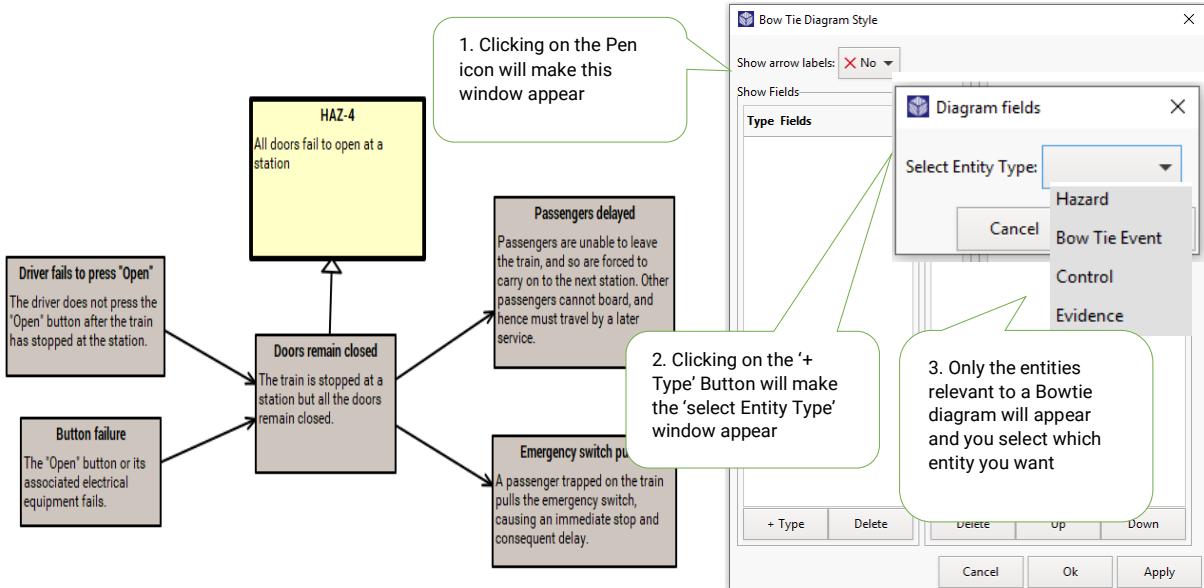


Figure 15 - Selecting the Entity to show Data Fields

Once you have selected the entity you wish to show data fields for you then go on to select which data field you want displayed.

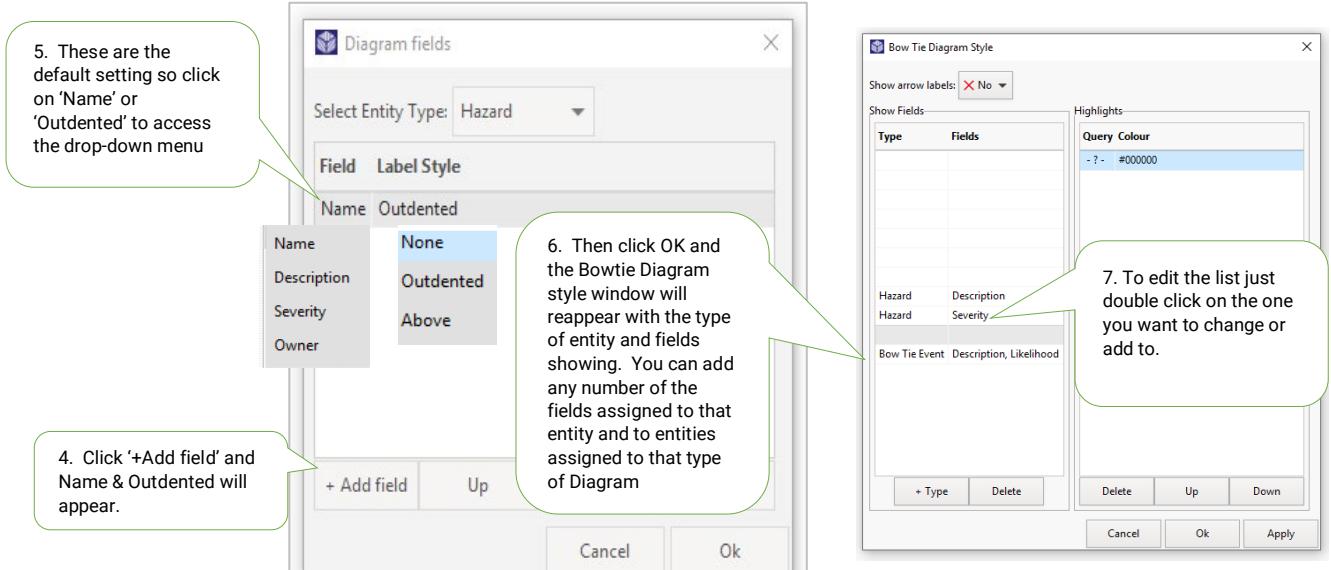


Figure 16: Adding the fields from Entities

'Outdented' means that the field name appears in bold followed by the text. **'Above'** means a horizontal line, then the field name (centered), then the field text. **'None'** just gives you the plain text without the field name.

Once you have selected the entities and fields you want, they will appear in the diagram when you click on the 'Apply' button.

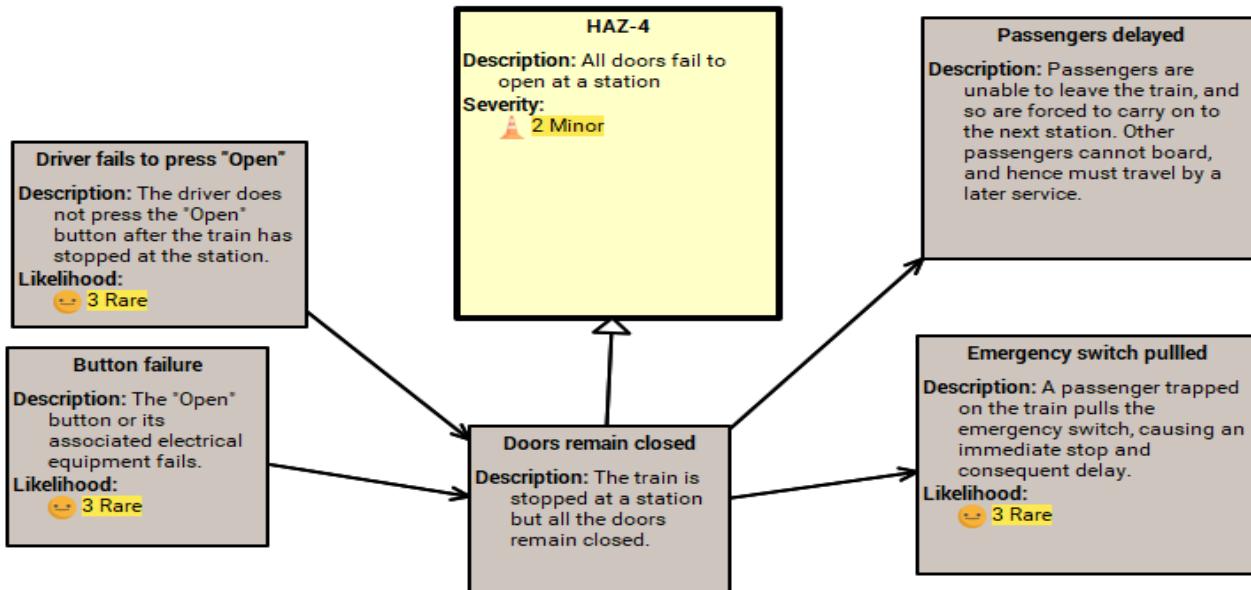


Figure 17: Fields added to the Diagram

Creating Model or Package styles in the Model Tree

If you wanted all the diagrams in a model to display the same data fields you can do this in the Model tree. Right click on the Model root and select 'Edit Diagram Style' from the drop-down menu.

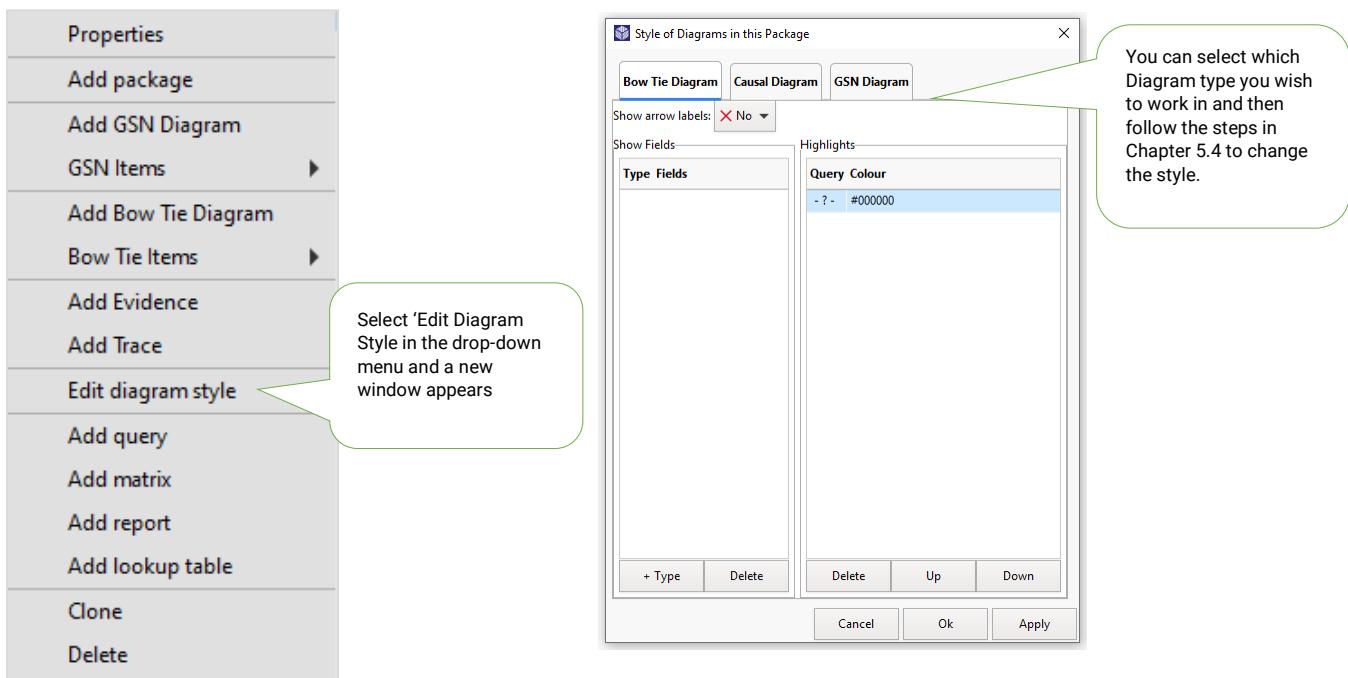


Figure 18: Changing all diagrams using the Model Tree

You can also just change the styles in a Package. Right click on the Package and select 'Edit Diagram Style' in the same way for the Model Root. If a Package style in

a lower level package has an entry for e.g. 'Evidence' then that entry overrides the style for 'Evidence' in the boxes, but nothing else.

So if you wanted to have a package of bow-tie diagrams that didn't include all of the Evidence fields you could set up a package style with just "Evidence Title, Version" and that would apply to all of the bow-tie diagrams in that package. The same applies to the diagram style dialog; it can override any of the package styles for that diagram alone.

The styles for the 3 types of diagram are independent of each other so if you change the style for evidence in bow tie diagrams, it does not change evidence in the GSN diagrams.

Extension References

Section 2.1 describes how arrows on diagrams have references to the boxes they are attached to. You can define your own references as extensions in the same way as data fields.

Start by clicking on "Reference Types" in the Data menu to get the dialog in Figure 10. Then double-click on the  symbol to create a new one.

Let's say that in order to organise your Safety Assurance Report in the company standard way you need to associate each GSN goal and each Hazard with a single diagram. Goals and hazards can appear in multiple diagrams, so this has to be a separate relationship that you define yourself.

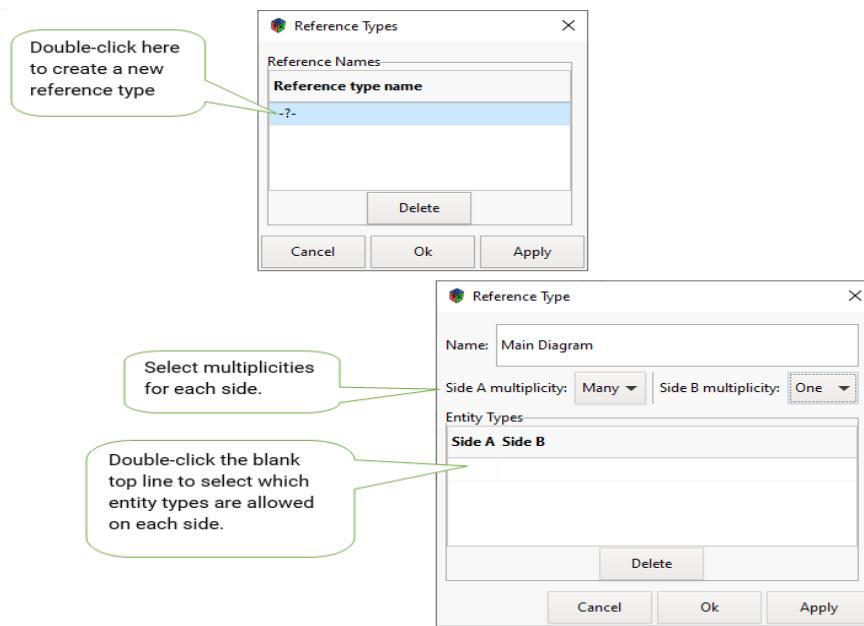


Figure 19: Extension References

In the dialog for the new reference type give it a name and decide what "multiplicity" it has; in this case, you want a diagram to reference multiple goals or hazards, but each goal or hazard should reference only one diagram. A relationship has rules about which types of entity can reference which other types. For instance, the built-in "Arrow-Head" reference type has rules like:

- You can point a GSN Context arrow at a Context box, but not at a Goal.
- You can point a GSN Support arrow at Goals, Strategies & Solutions, but not at a Context box.
- An “Arrow-Head” for an Arrow can only reference a single box (so you can’t have an arrow pointing at two things at once), but a box can have several arrows pointing at it. This is the “Multiplicity” of the reference type.

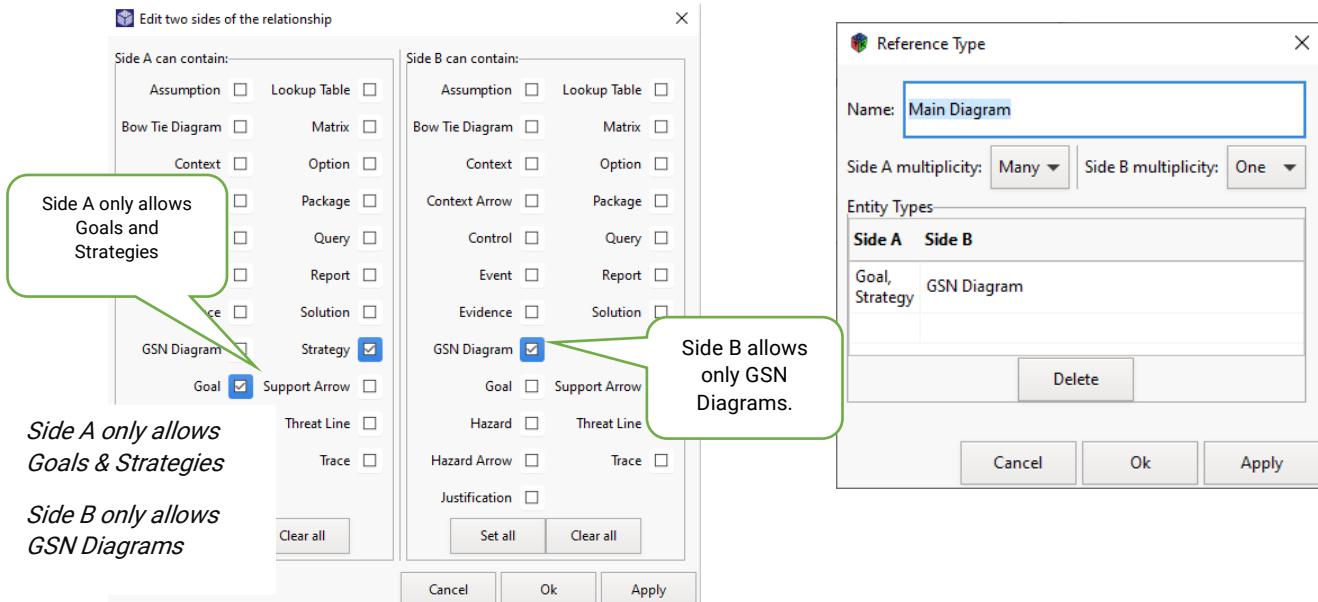


Figure 20: Adding Entity Types to a Reference Field

In the case above, we will have GSN Goals and Solutions as side A and GSN Diagrams as side B³. Double-click the blank line in the “Entity Types” table to add entity types

Now do the same for Hazards and Bow Tie diagrams:

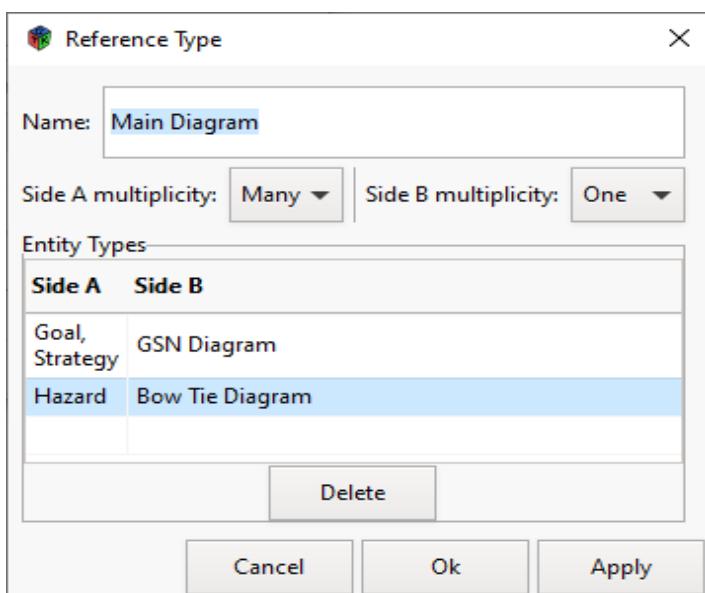


Figure 21: Reference Type with second line

³ There is nothing special about Side A versus Side B: this example would work just the same if they were reversed.

This says that you can link a Goal with a GSN diagram and a Hazard with a Bow Tie diagram, but you can't link a Goal with a Bow Tie diagram or a Hazard with a GSN diagram.

Now right click on a GSN goal to get its properties and you will see the Main Diagram listed in the references. Click on the field to get a second dialog showing the model tree with only the GSN diagrams. Select one and click OK to fill in the Main Diagram reference field. Hold the Ctrl key down while clicking to toggle the selected entry off or to select multiple entries.

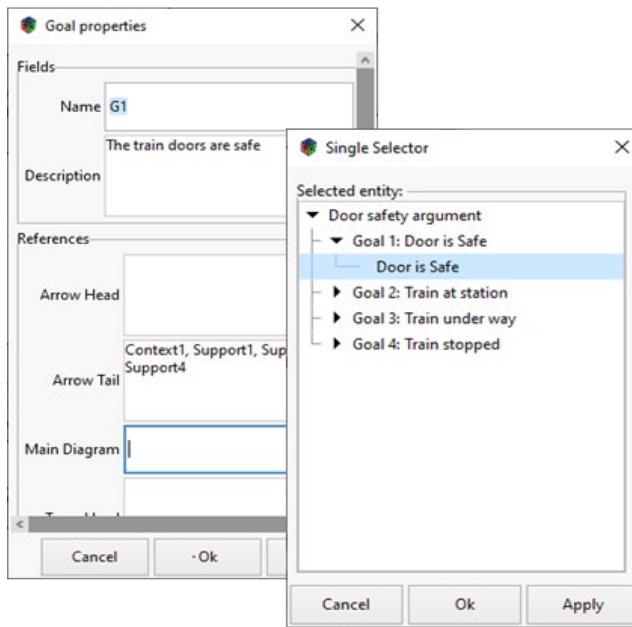


Figure 22: Editing References

Queries

Analysing the Model

The DSM has a query function 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, or you may wish to search the DSM for any event that leads to a degraded state 70% or more of the time.

If 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 for checking high level consistency. The multiple combinations make queries very powerful but also complex, so the DSM has a graphical query builder which allows you to create them in manageable blocks, test them as you progress and manage them centrally, allowing you to find them easily and re-use them elsewhere.

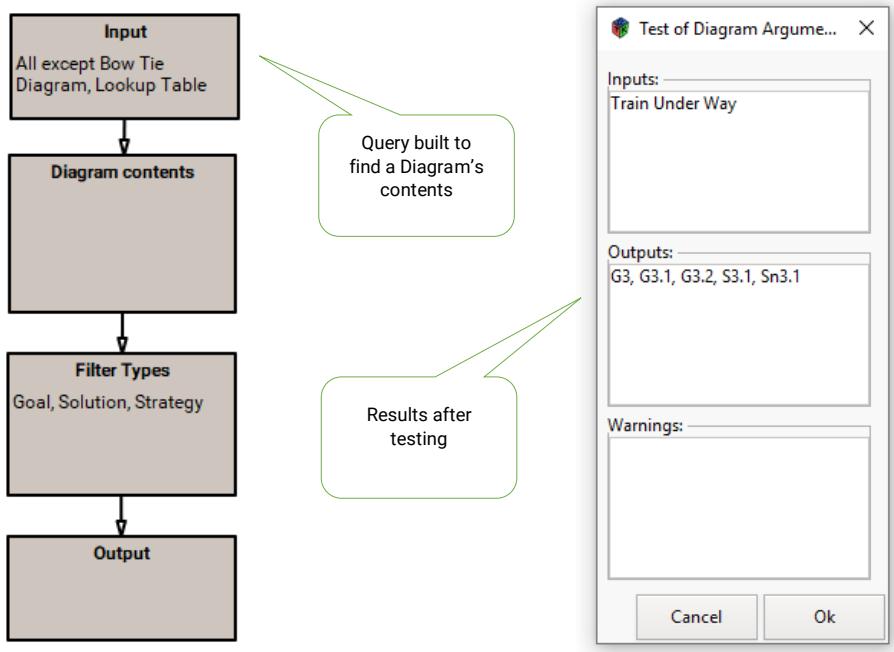


Figure 23: An example of a Query

Query Symbology and Function

The Query symbols and their meanings are detailed below. Queries are built on the desktop as a diagram using the query functions to step through the required entities and data fields. The diagrammatic format makes the building of complex queries clear and easy to understand. Once constructed the 'Multi-selector' allows you to apply them to any package or set of entities to find the required result.

Follow the arrows down through a GSN to subordinate goals and evidence		Follow Arrows	Applies a filter that only shows the selected items		Filter
Follow the arrows up through a GSN from subordinate goals and evidence to Top Level Goals		Follow Arrows Backwards	Applies a filter that shows all entities of selected types in the model, regardless of inputs		Filter Entity Type
Step up or down to identify additional information held on Arrows		Step	Gets results from another query		Sub-query
Finds all the parents of an element		Parent	Allows you to select a type or types of entity in the Model, regardless of input		Selected Type
Finds all the children of an element		Children	Allows you to select an entity or entities from the model tree		Selected Items
Finds all the entities shown in the diagram		Shown in Diagram	The starting point for a query, in the diagram, actual inputs are selected		Query Inputs

			<i>and shown in the Query Tester</i>		
Finds the diagrams that contain selected entities		Find Diagrams with	The finishing point for a query, in the diagram, actual outputs are shown in the Query Tester		Query Outputs
Joins the query elements and drives the flow of information		Joining Arrow			

Table 2: Query Symbology

Building Queries

This example follows the flow of a GSN diagram. See below:

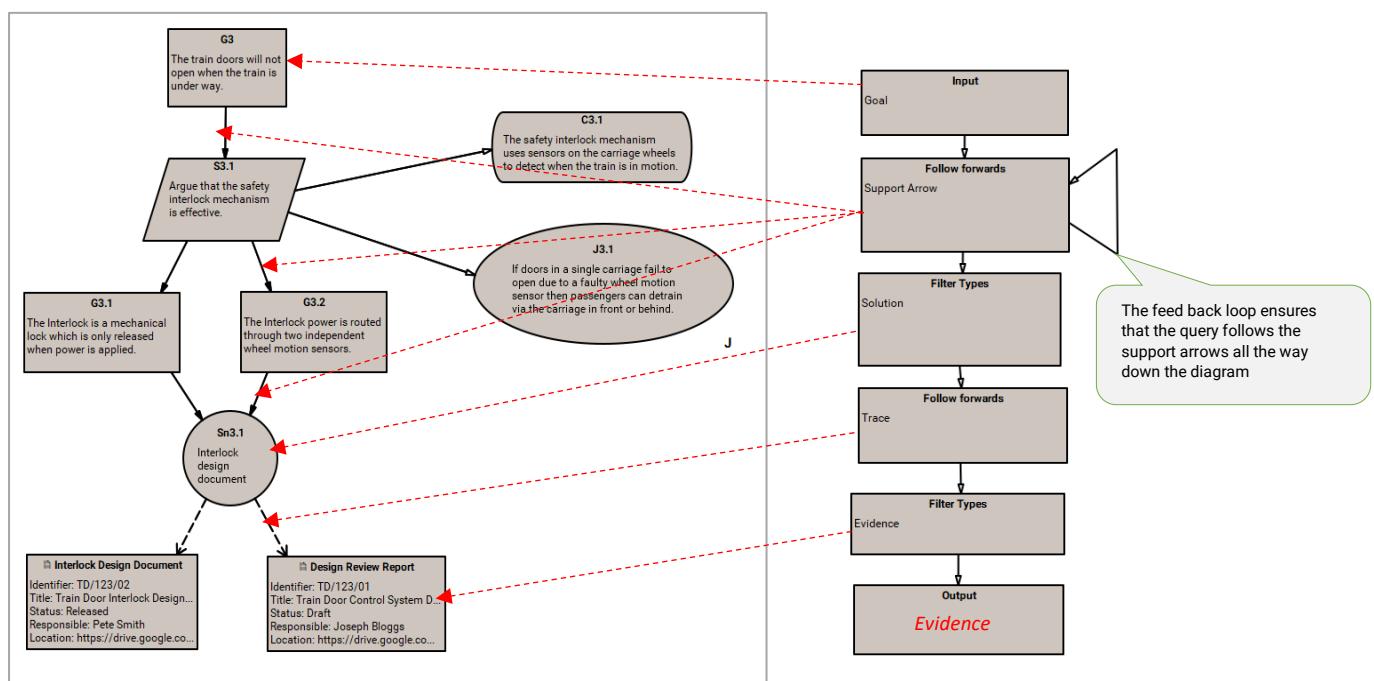


Figure 24: Query Alignment with a GSN Diagram

To create a query, right click on a package and select 'Add query' from the drop-down menu. A query properties window will appear which will allow you to add a name. Once you click 'OK' the query will appear in the Model tree under the package where you created it. Double click on the Query symbol and the Query desktop will open, giving you access to query icons and a blank page. You can then start to build your query.

To place a query symbol on the desktop simply click on the required icon and drag your mouse on the desktop and the symbol will appear (just as in a GSN diagram). To join query boxes together, click on Joining Arrow icon(\nearrow) and drag the mouse from one box to the other in the direction you wish the query to progress. The arrow will automatically connect to each box. If it does not, you can click on the arrow, select the head or the tail and drag it to the appropriate box until it does. Unlike other

diagram types the boxes and arrows in a query are not separate entities; they exist only inside the query diagram.

Queries generally begin with an ‘Input Box’ () where the starting elements can be selected and finished with an Outputs Box () which will deliver the result.

However, you can instead use the “Type” and “Value” boxes to create queries that always start from the same thing. For instance the simplest way to find all the goals in a model is just to use the “Type” box and select “Goals”.

To build a query, careful thought should be given to what you are trying to achieve, for example, if you want to identify the Goals in a Safety case through the Goal Structured Notation Network (or part of one) you will start at the package (Door Safety Argument) in this case, select the Child Entity box and link it to the inputs box and the output box using the joining arrow.

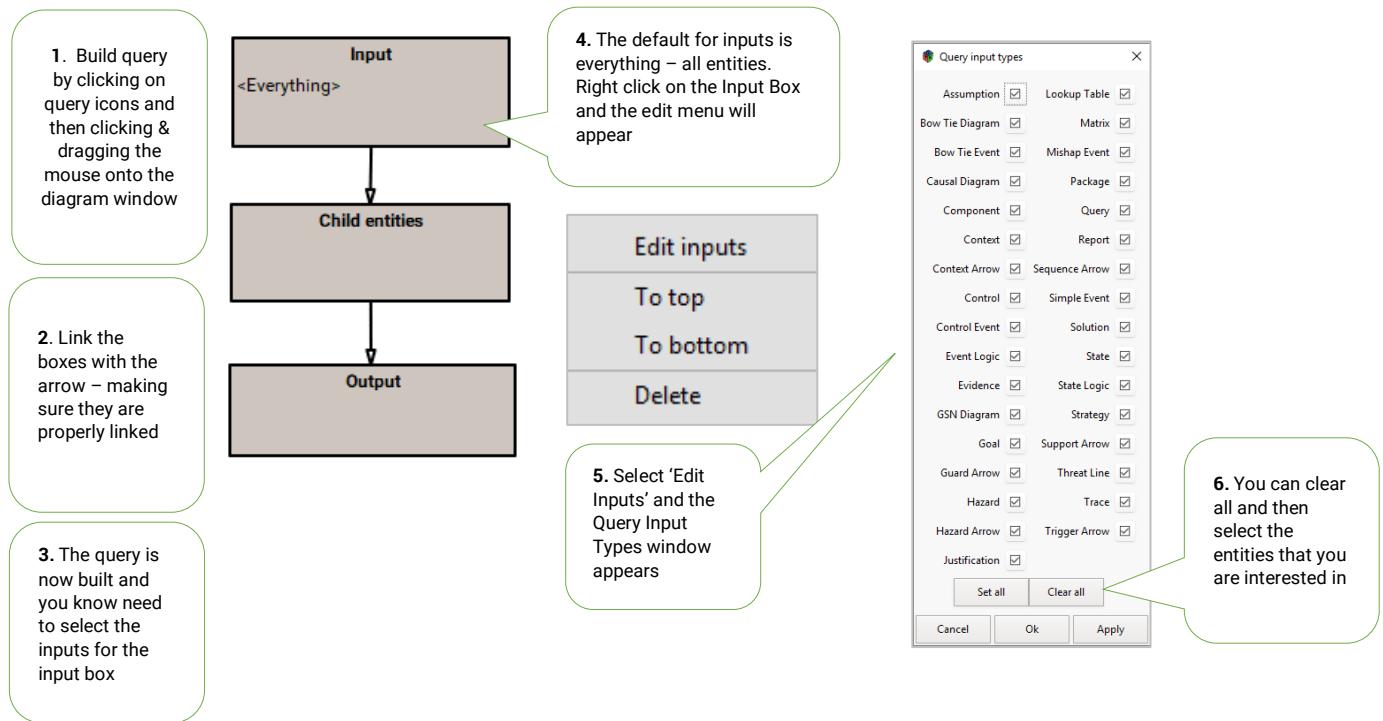


Figure 25: Building Queries

Testing Queries

You can then test the query (see diagram below) by right clicking on any blank area on the desktop and selecting the test query line. This will open the Query Test Window and by clicking into the Inputs area, the ‘Multi-selector’ appears (this allows you to select any element in the Model Tree) and the results will appear in the Outputs window. If there are problems with your query you may get a warning appear or if you have constructed it incorrectly, there will be no results.

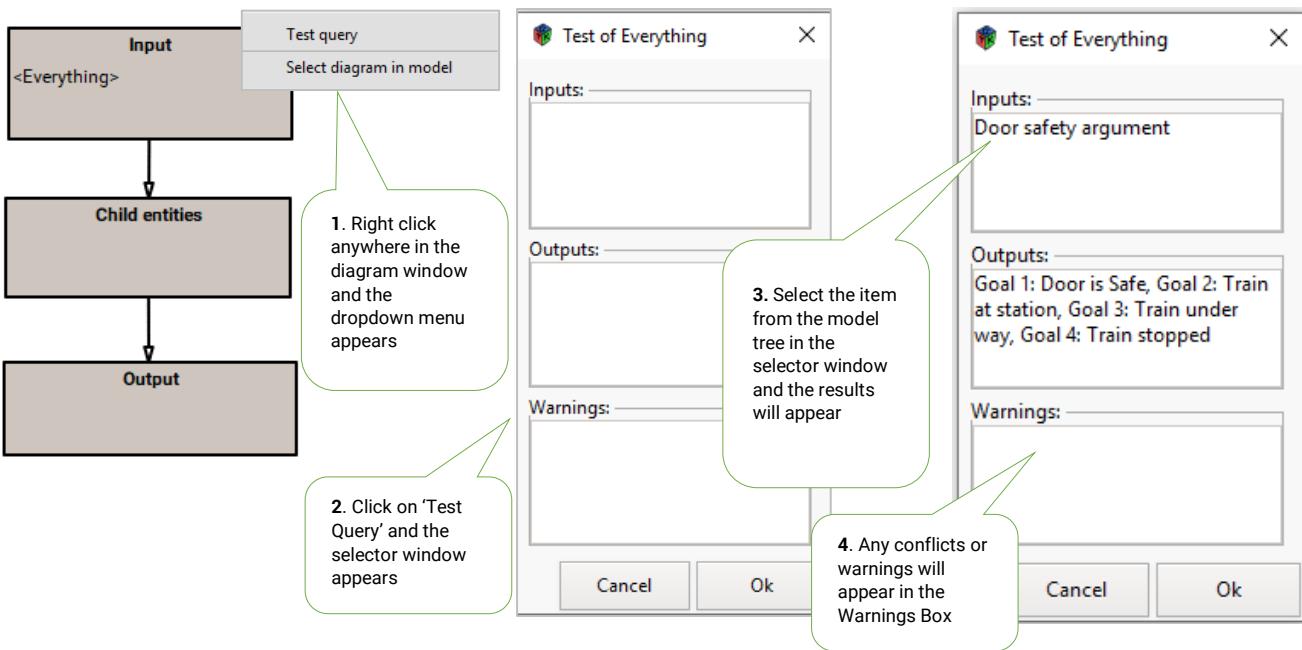


Figure 26: Testing Queries

Finding Evidence

In a slightly more complex query, you wish to follow the goals and sub-goals down to a solution and thus to the evidence that supports that solution. In this case you can follow the arrows down using the (→) icon through the GSN diagram and select the entities you wish to find, say goals, solutions, strategies using the 'Filter Types' icon. By feeding back the output of the 'Follow Forwards' box, the query will continue to follow arrows until all the sub-goals and sub-sub-goals have been reached.

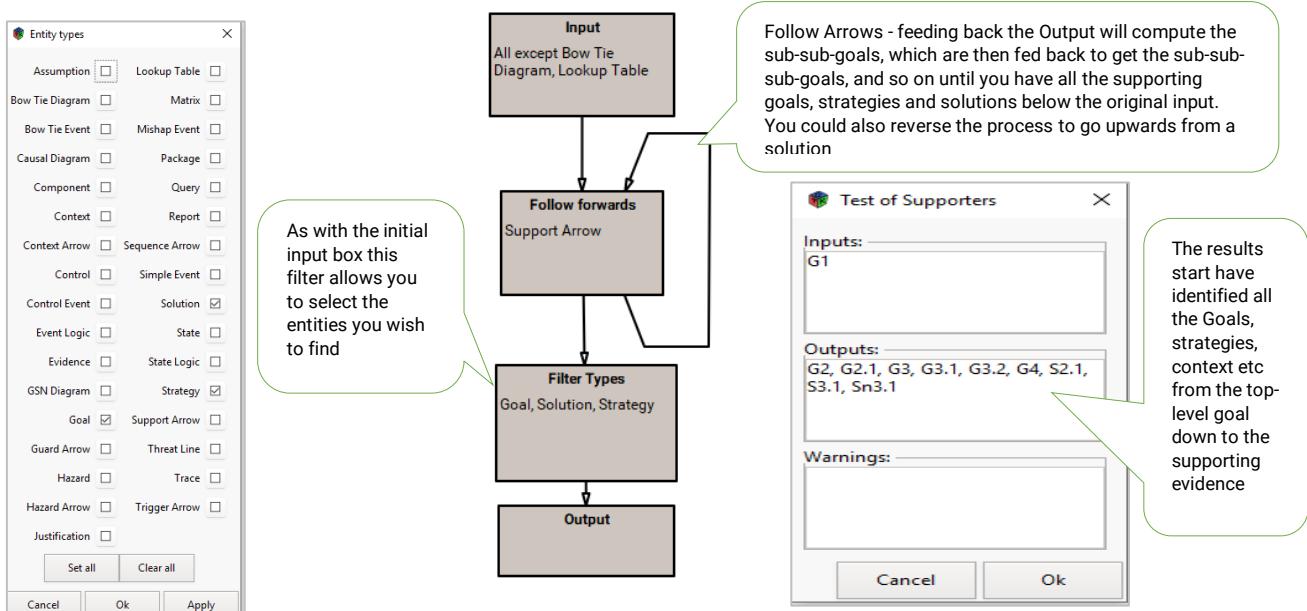


Figure 27: Finding Evidence

Working with Colours

In complex GSN structures, key areas of interest, new changes to the diagram and interdependencies can be visually difficult to identify. The DSM allows you to select areas of interest using queries so that they stand out in the GSN diagrams.

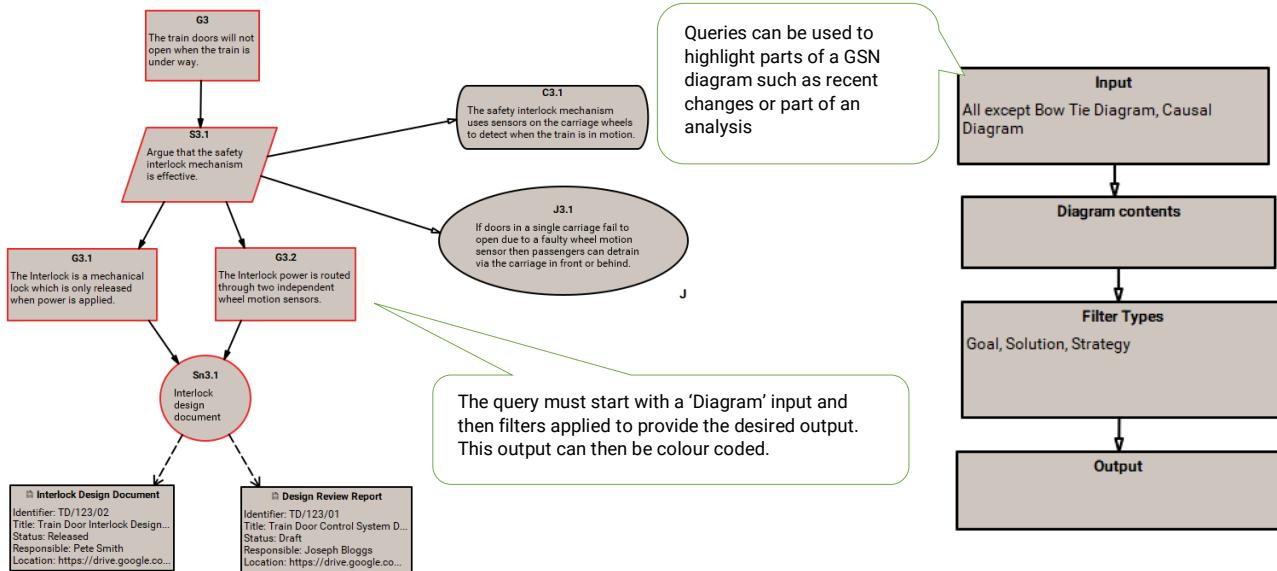


Figure 28: Building the Highlight Query

Queries are used to select the areas you wish to highlight. Each query will take the diagram as input. As the figure above shows in the query, the diagram contents have been filtered to deliver Goals, Solutions, and strategies. Once you have built your query (which can be used again and again) you select the GSN Diagram Appearance window from the pen icon (✍) and select the query you have built. In the example it is 'Interlock Goals'.

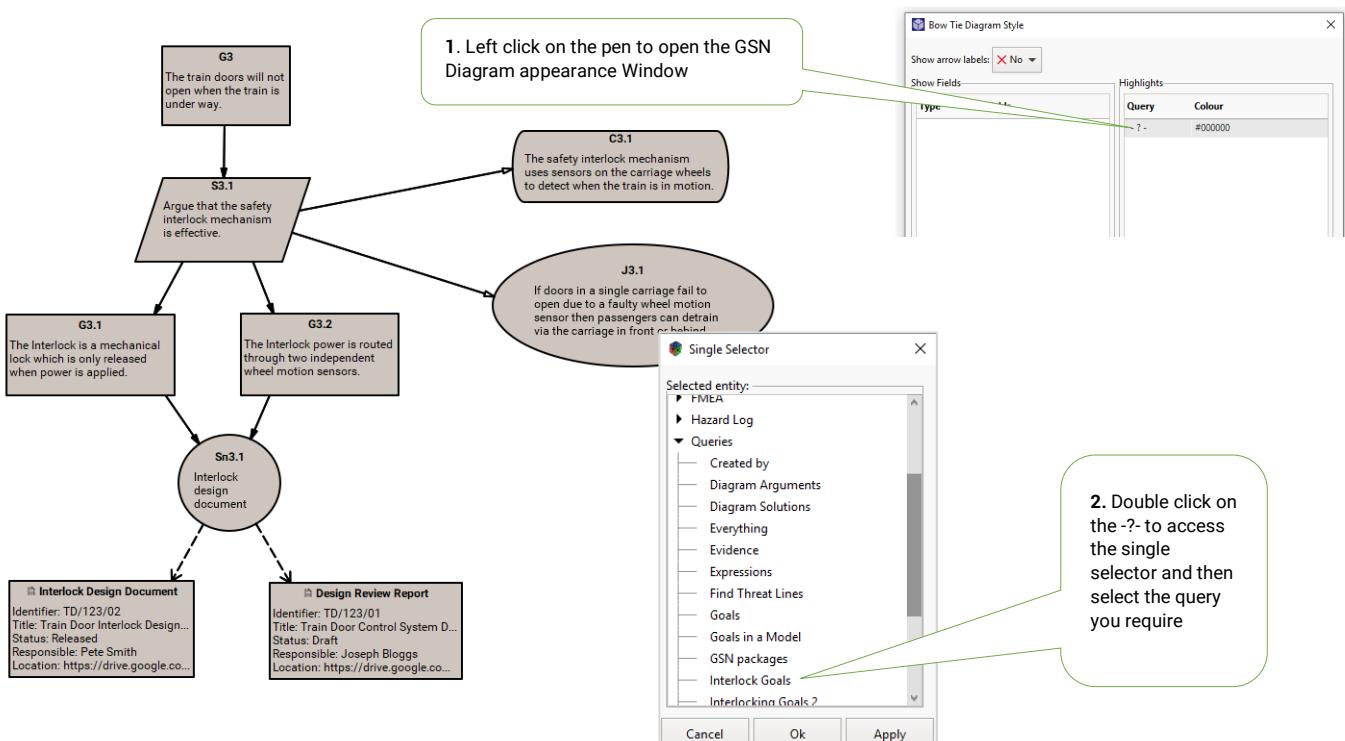


Figure 29: Using the Diagram Appearance window

You then select the colour you require the information to be highlighted in and press 'Select'. Those areas filtered by the query will be highlighted in the GSN in the colour you have selected. Using formulae (see later chapter) you could highlight changes within a timescale or by a person or key word.

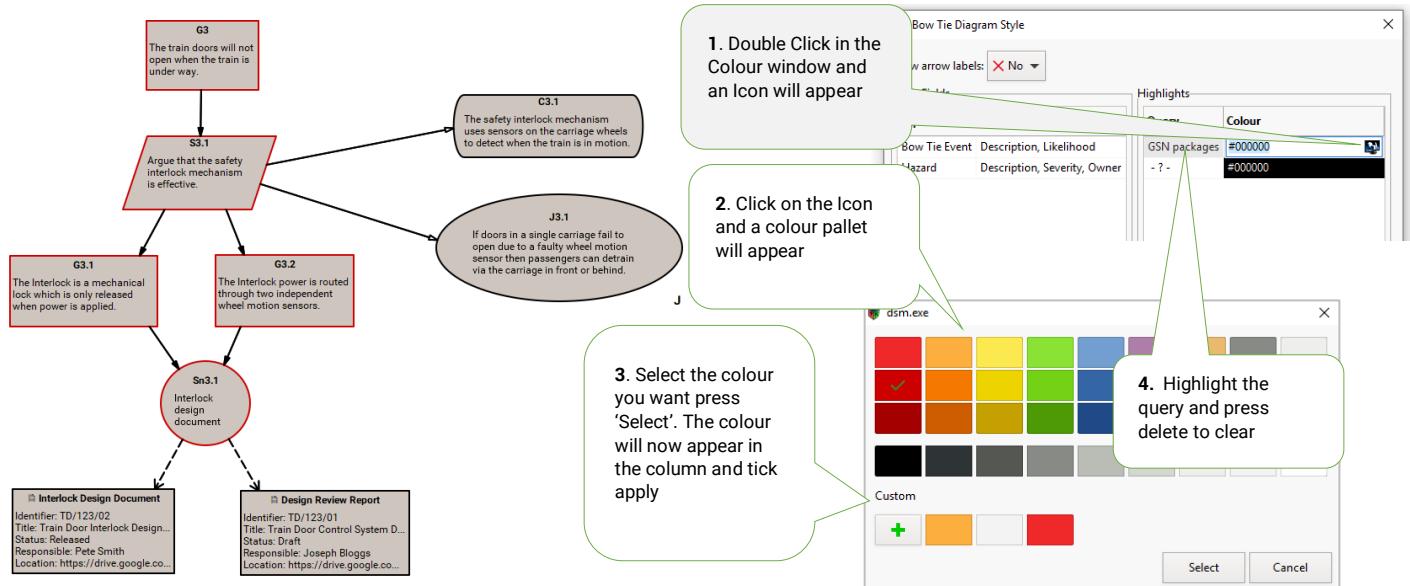


Figure 30: Using the Colour Pallet

Matrices – Presenting the Analysis

A matrix displays the result of one or more queries in a configurable table. They can be used to display results from a search on conformity for regulators, and by managers to detail progress (or the lack of it) of a safety case production.

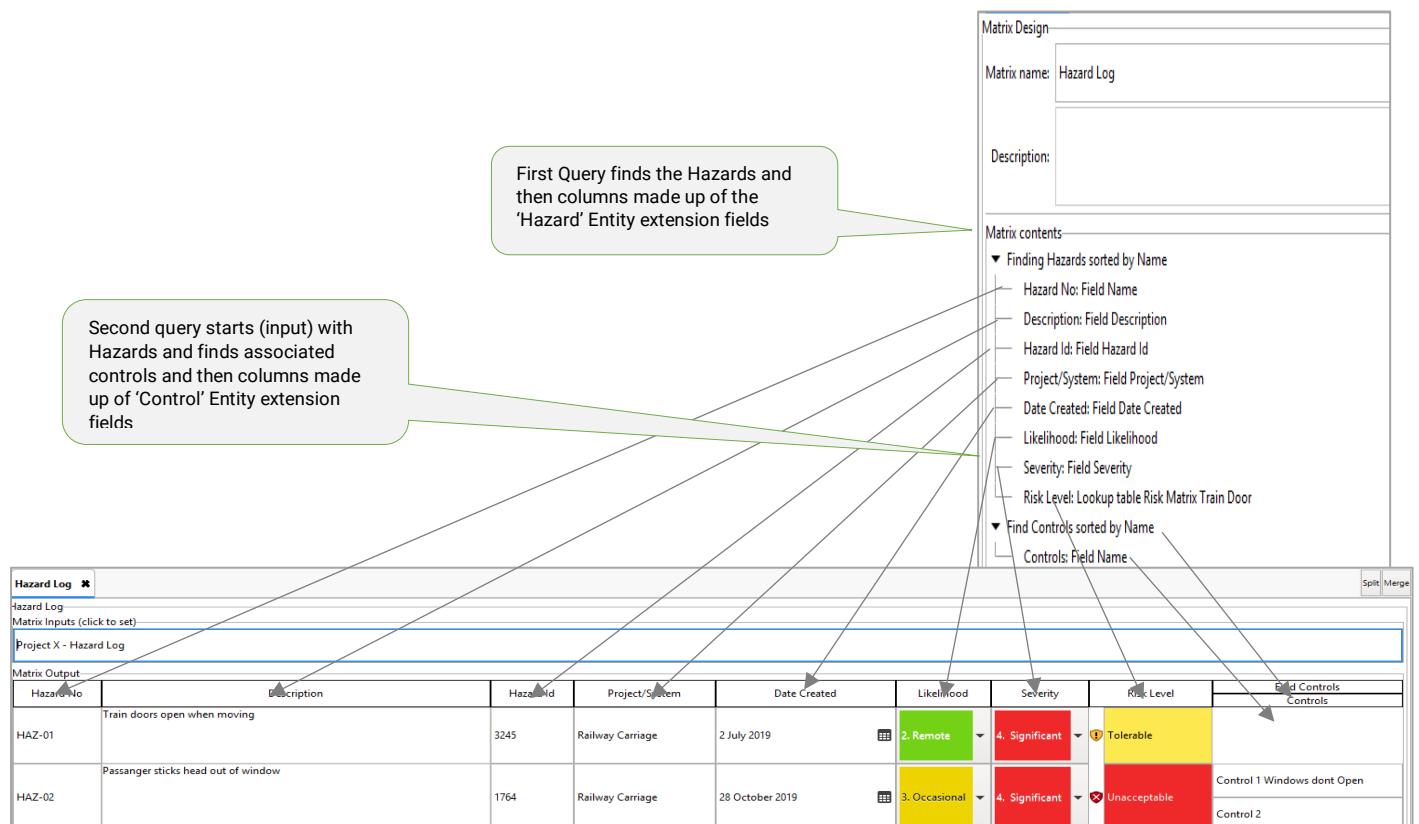


Figure 31: Hazard Log Extract Matrix & Design Window Example

Constructing a Matrix

A matrix is a configurable table that is used by the DSM to display the data required by the systems engineer. It will have a starting or subject element (Normally added to the Default Inputs: Window) and configurable rows and columns. This will display the data required in 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 one or more queries and when combined with this capability they represent a significant analytic and reporting functionality.

Every Matrix starts with a Query which will identify the entities that will form the first columns of the matrix, such as Goals, Hazards etc. In the example below the query finds the Hazards.

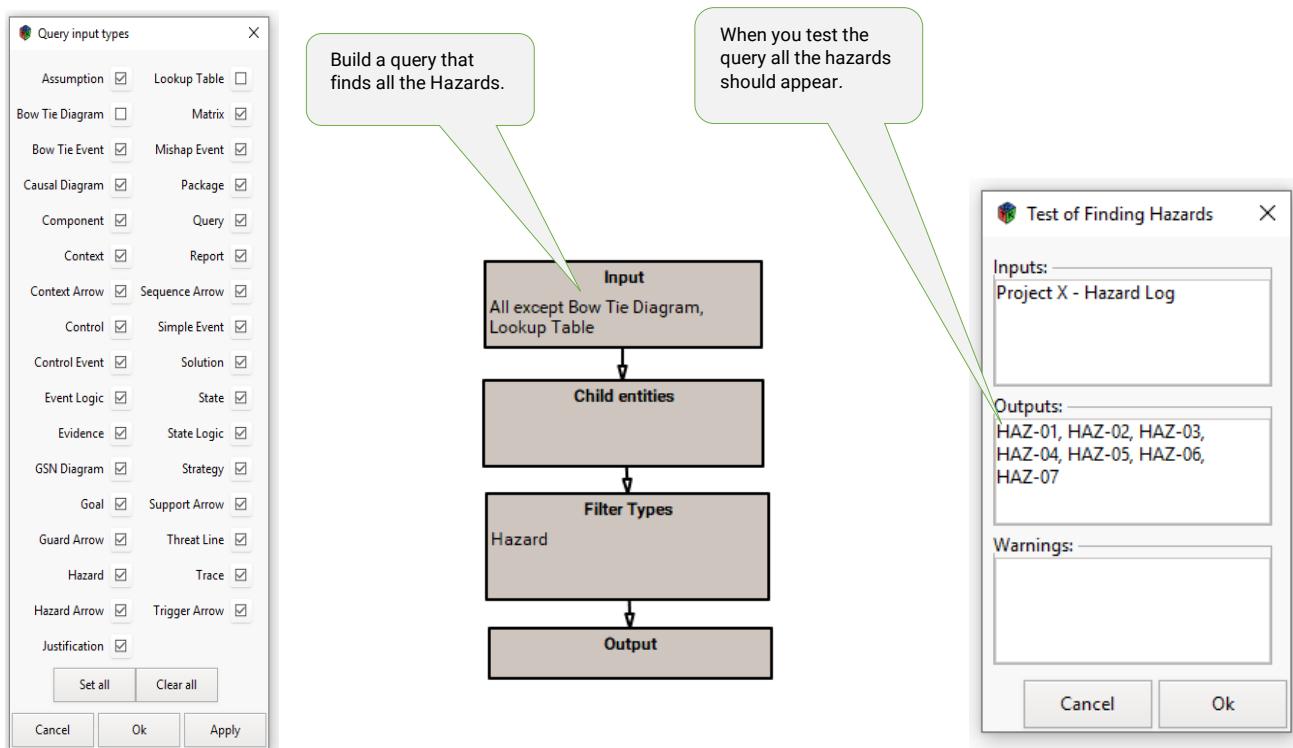


Figure 32: Hazard Query

To create a matrix you select the package in the Model Tree (or create a new package), right click and select 'Add Matrix' and the Matrix Properties window will appear. Give Matrix a name and click OK and it will appear in the model tree. You can now build the matrix by right clicking on the Matrix name and selecting 'Edit Matrix'. The Matrix Design window will now appear. As stated in 6.1, a matrix will have a starting or subject element and this is added to the Default Inputs: Window. So if the first query is looking for Hazards, the starting element will be the package in the Model Tree where Hazards are kept. This will ensure that the Matrix will run from the starting element each time.

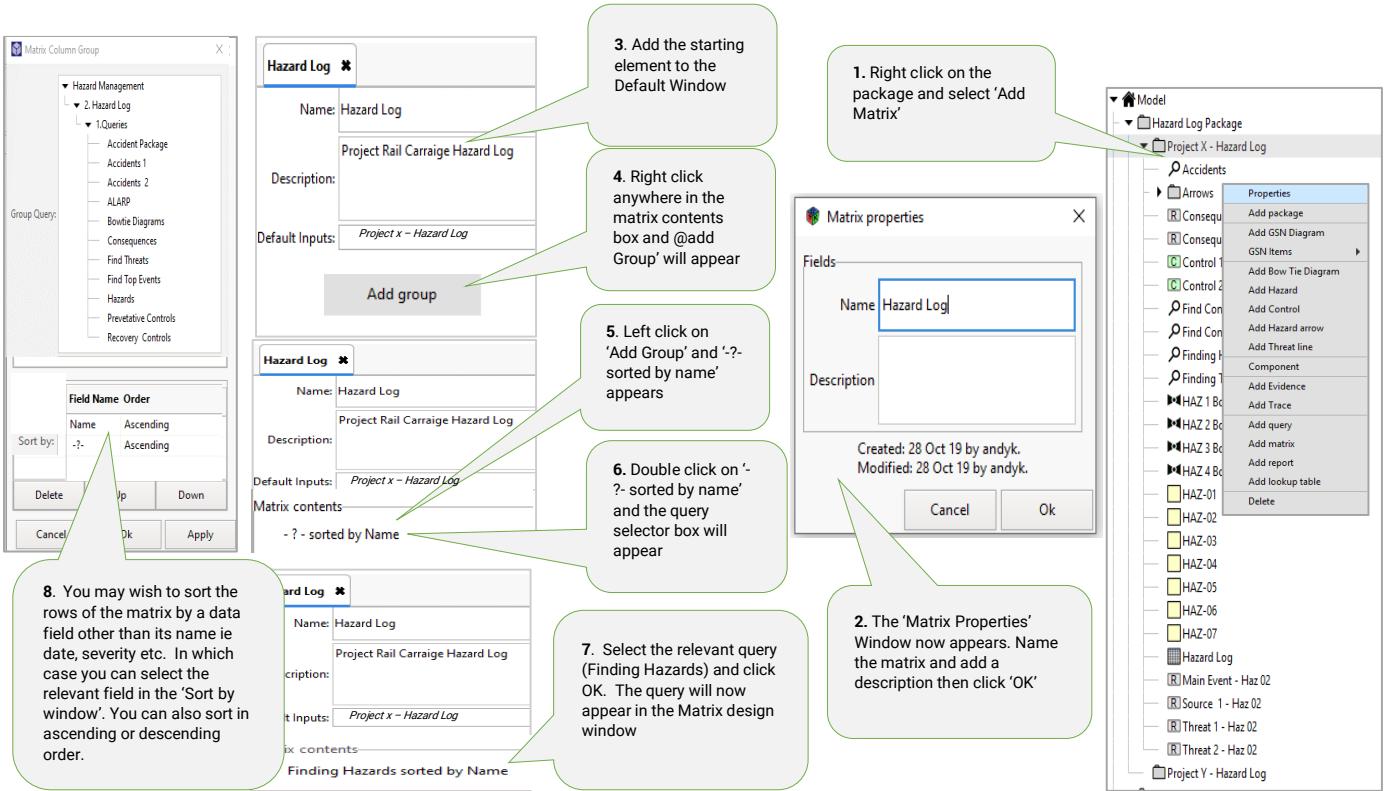


Figure 33: Adding the query to the matrix design window

Right click anywhere in the 'Matrix Contents Box' and 'Add Group' will appear. Left click on 'Add Group' and the question mark symbol will appear followed by 'sorted by name'. You can also order the query results in ascending or descending order. Sort by name is the default order and will sort the results in alphabetical order. You could also select a modification date or any other field to be sorted. The direction of ordering is indicated by a little arrow next to the query line. This is where you select the starting query which will deliver the rows of the Matrix (Goals, Hazards etc). When double click on the question mark symbol, the Matrix Column Group Selector Window will appear which will allow you to select the query you require. The Matrix contents window will remain highlighted in Pale Red. until a query has been selected. In this case it is the 'Goals' query that has been selected. You can then build the columns in the Matrix by selecting the data fields.

Adding Columns to the Matrix

After the query has dictated the row names, you add columns by clicking on the query and selecting one of the options that appears in the drop-down menu. You can add data fields, formulae, queries and lookup table as columns and each additional addition will implement a column to the right of the preceding entry.

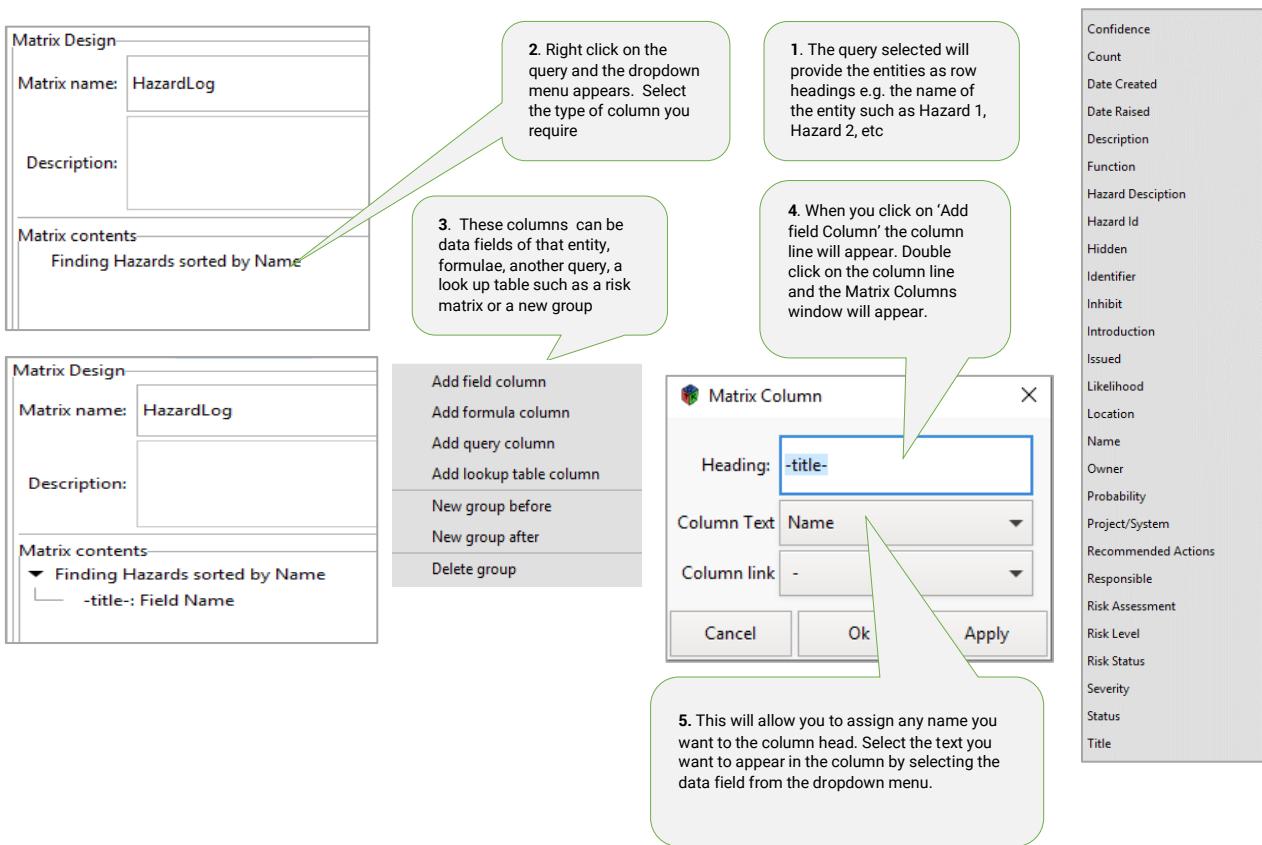


Figure 34: Adding Columns to the Matrix

Once you have the query added to the Matrix design window, you must add a name field for it to appear as the first column or nothing will show. Additional columns are added by clicking on the previous column and selecting from the dropdown menu. If you wish to change the order you can simply click and drag the entry to where you want it to be. When you add a second column a slightly different menu appears that allows you to position the second entry before or after the entry highlighted. When you insert a column query here it will only give you the entity name as a result. If you wish to add another query and use data fields from that query you must add another 'Group', remembering that the second query must start from when the first query finishes.

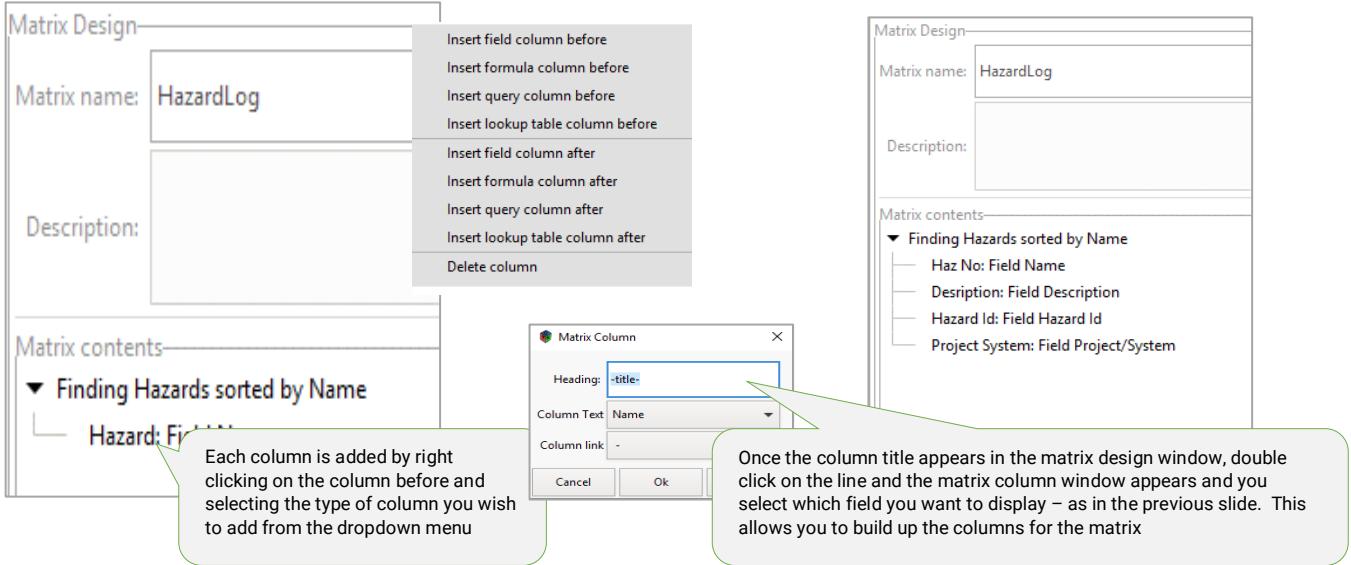


Figure 35: Adding additional columns to the Matrix

Running the Matrix

When you are ready to run the Matrix just simply right click on the matrix in the model tree and select 'Run Matrix'. The matrix structure will appear (see diagram below) showing the column headings.

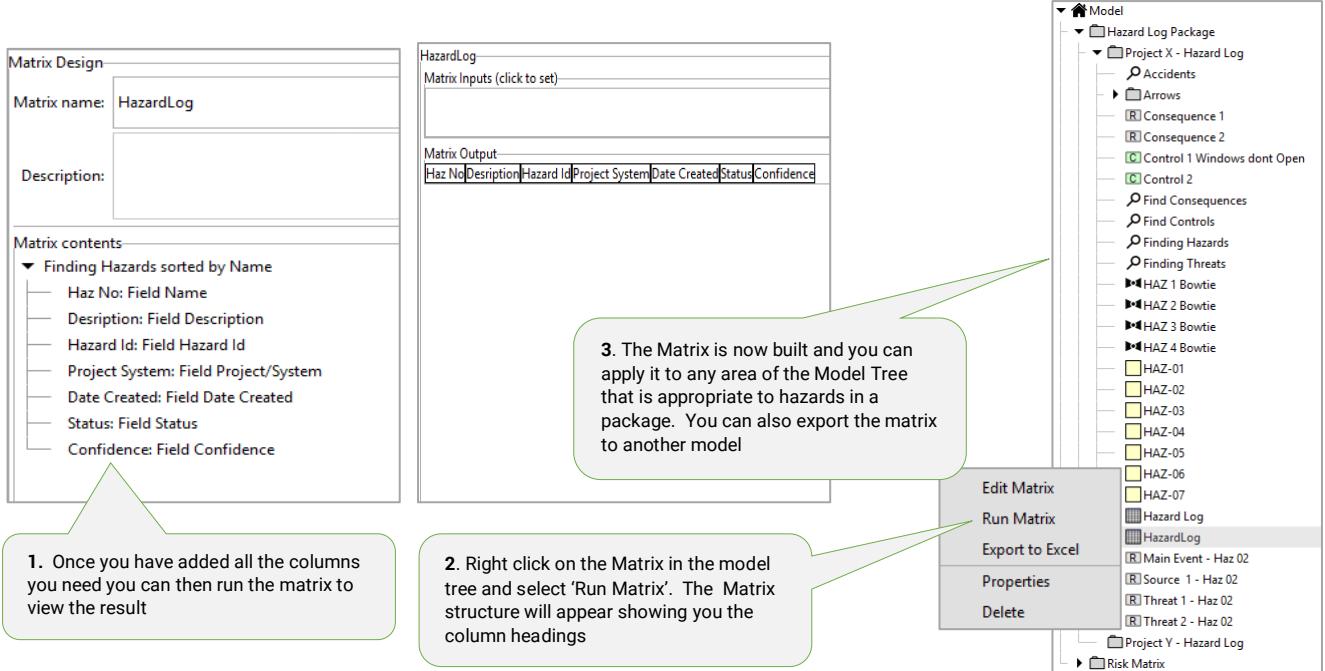


Figure 36: Running the Matrix

In the split screen mode you can see the matrix design window on the left and how the matrix will look in terms of columns on the right. Once you are happy, run the matrix, select the package you wish to run it with, and the populated matrix will appear as shown below. This matrix can be applied to any package in the Model tree that contains Goals, it can be exported into another model (See Section Exporting Selected Data & Extensions) or the populated matrix can be included in a report (See Section Adding Information into a Report) or exported to Excel (See Section Exporting from a Matrix into Microsoft Excel).

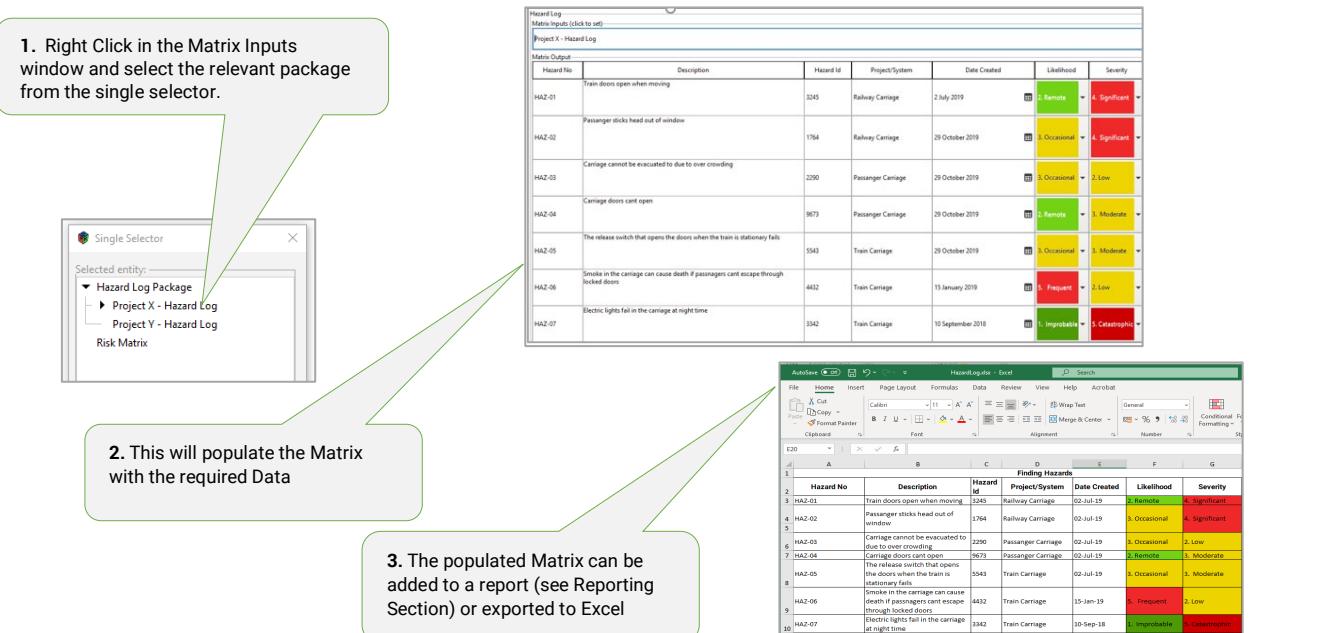


Figure 37: Populating the Matrix

If you wish to add a further column such as “Remarks” you simply go back to the Matrix design window, add another line under the last one and select “Remarks” from the drop-down box. Then re-run the matrix and it will appear as a new column.

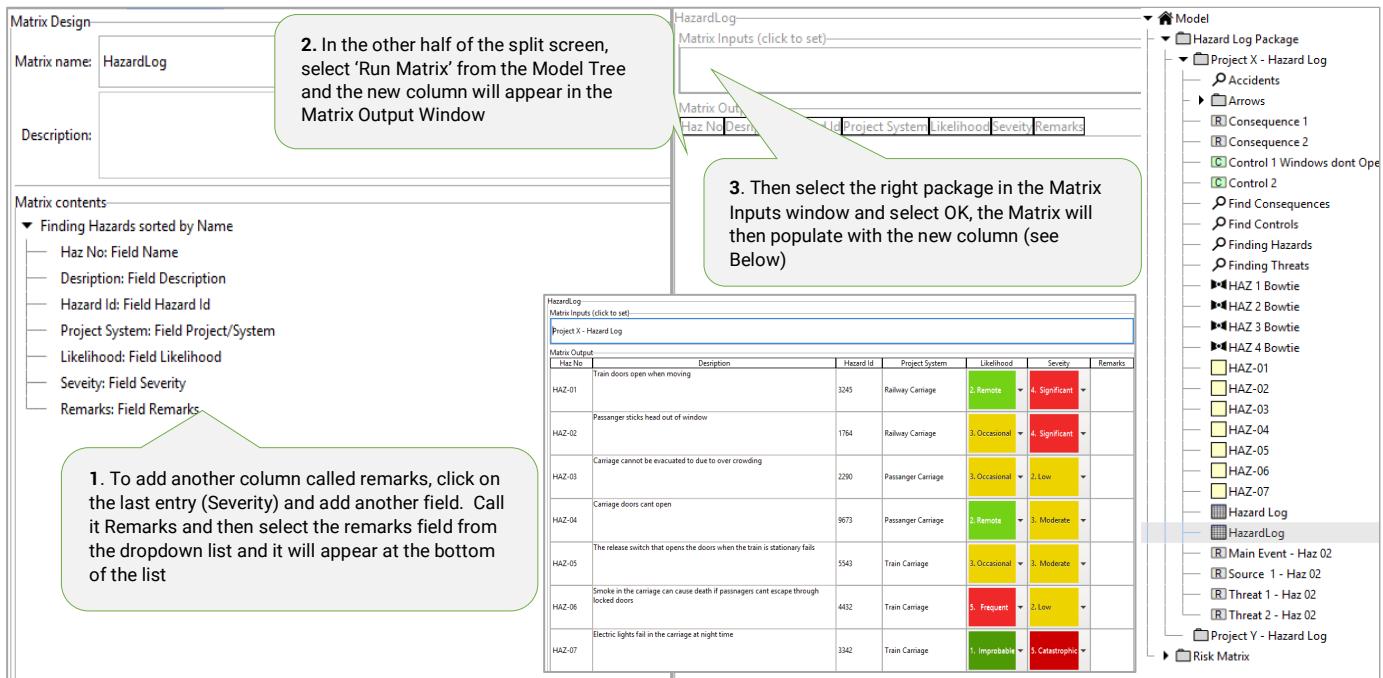


Figure 38: Adding another column

Adding Another Group to the Matrix

Adding another group to the matrix allows you to introduce additional entities and the data fields that sit within them. For example, if you wanted to show the solution to a set of Goals and then the evidence attached to those solutions, you do this through an additional group. Remember each group starts with a query, and the output of the first query is fed in to the input of the second query (see the Goal based Matrix diagram below).

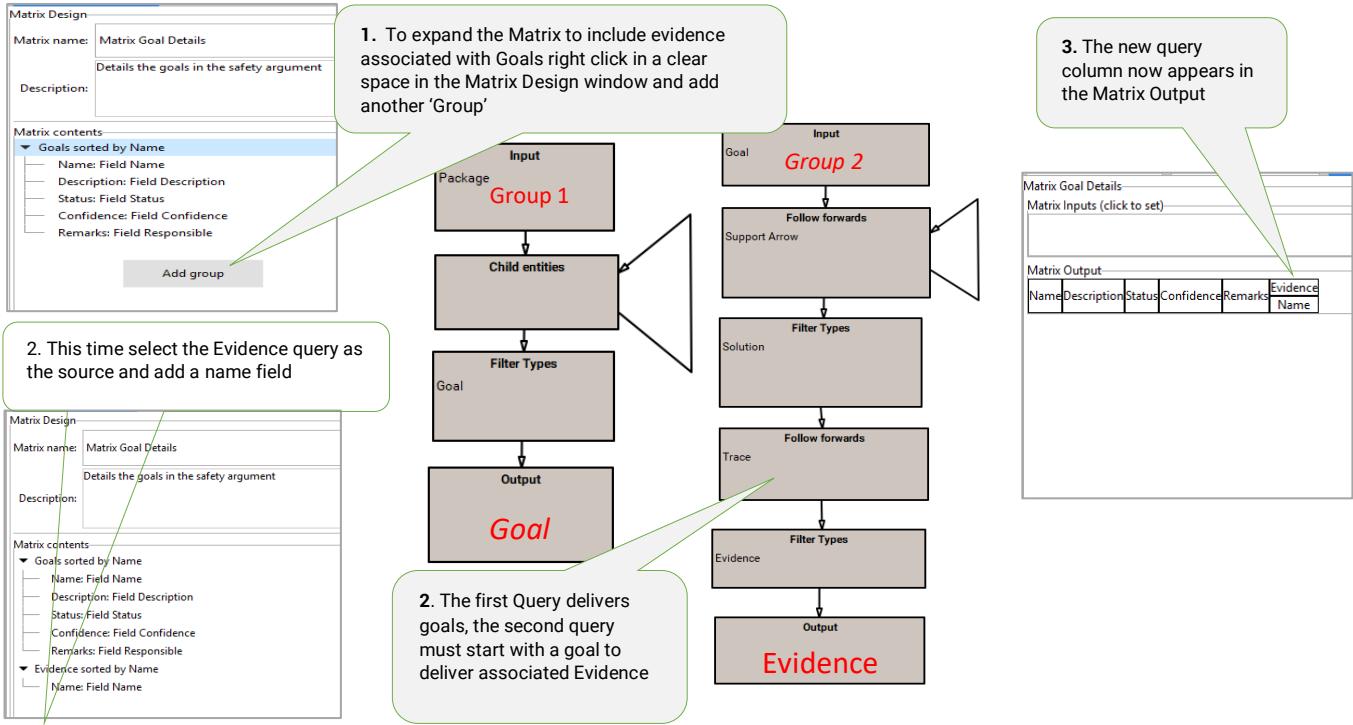


Figure 39: Adding additional Groups to a Matrix

Once this group has been added to the Matrix Designer it will appear in the matrix as additional columns. Just adding the query is not enough; you then need to select a field below that query to get it to appear in the Matrix.

Matrix Goal Details						
Matrix Inputs (click to set)						
Door safety argument						
Matrix Output						
Name	Description	Status	Confidence	Remarks	Evidence Name	
G1	The train doors are safe	Released	High	Top level Goal	Design Review Report Interlock Design Document	
G2	The train doors open when commanded and the train is stopped at a station. Testing	Released	Medium	Under Review		
G2.1	The driver will only enable door opening when at a station.	Released	High	Training objective added		
G3	The train doors will not open when the train is under way.	Released	Medium	Engineering Maintenance Plan for Movement Sensor	Design Review Report Interlock Design Document	
G3.1	The Interlock is a mechanical lock which is only released when power is applied.	Draft	High	Under review	Design Review Report Interlock Design Document	
G3.2	The Interlock power is routed through two independent wheel motion sensors.	Draft	High	SC Approval	Design Review Report Interlock Design Document	
G4	The train doors will not open when the train is stopped other than at a station.	Draft	Low	Under Review		

Figure 40: Evidence Matrix

Adding URL Links to the Matrix

You can add a URL link to a column in the DSM. To do this you must create a URL data field in the entity that you wish to link. In this example, 'Evidence' is the entity and a URL Link field is first created in the 'Fields' menu under 'Data' at the top of the page (See Section Creating Extension Fields). Once created it must be assigned to 'Evidence' in the 'Extension Fields' menu.

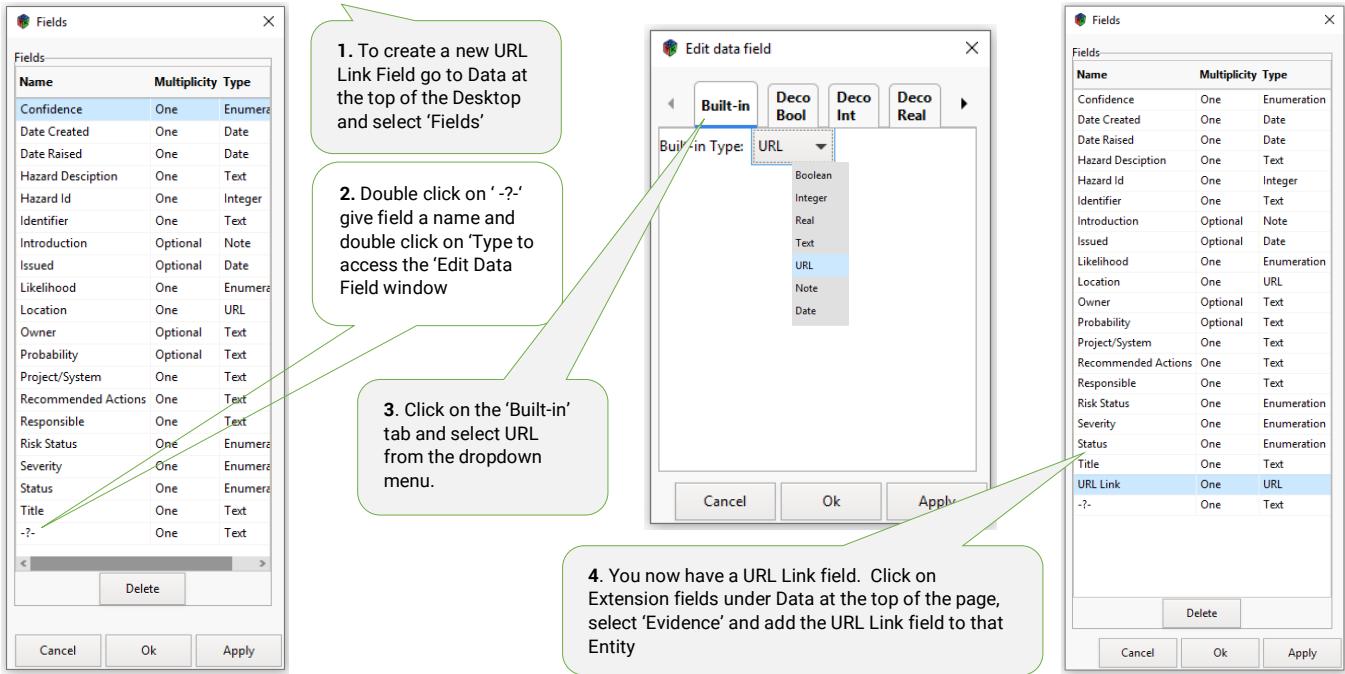


Figure 41: Building and assigning a URL Link Field

This URL field can then be added to the matrix in its own right (so you can see the URL Link details) or assigned to any data field as a column link (you will see the URL details when you hover the mouse over the link).

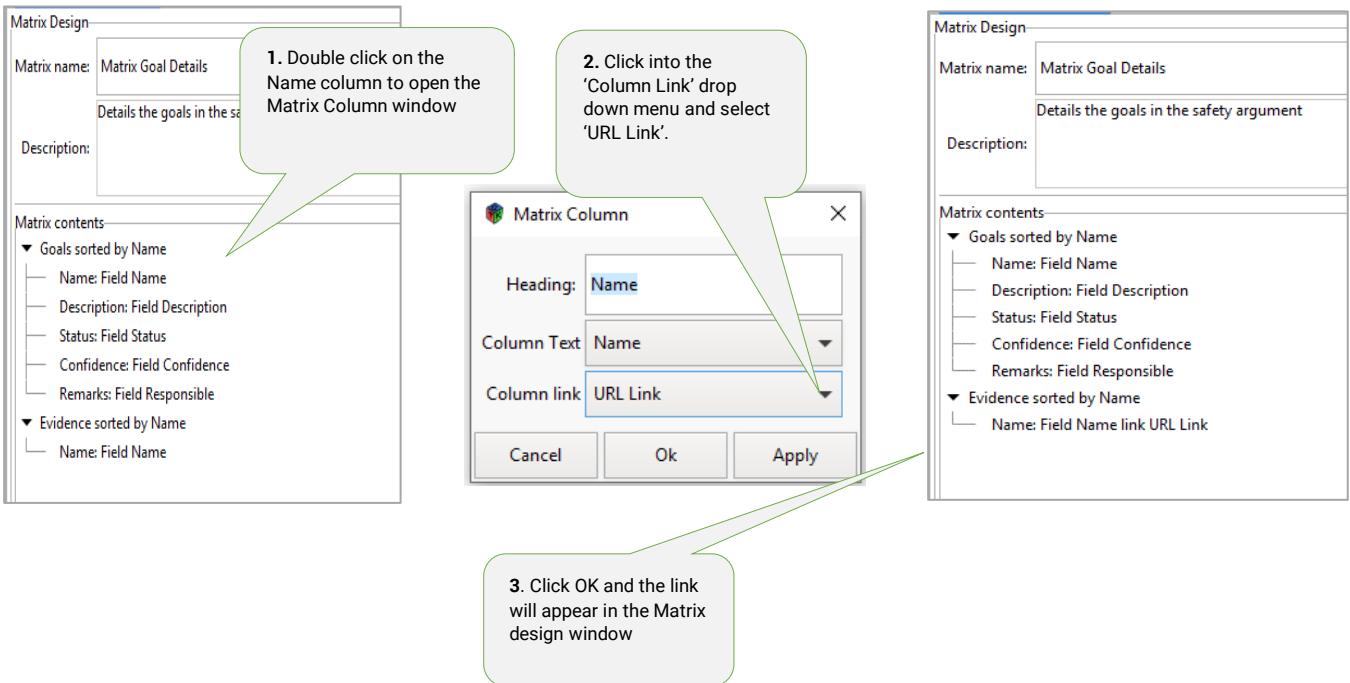


Figure 42: Linking a URL to a Column

Nothing will appear unless the URL link has been added to the 'Evidence' UFLink field in the properties window

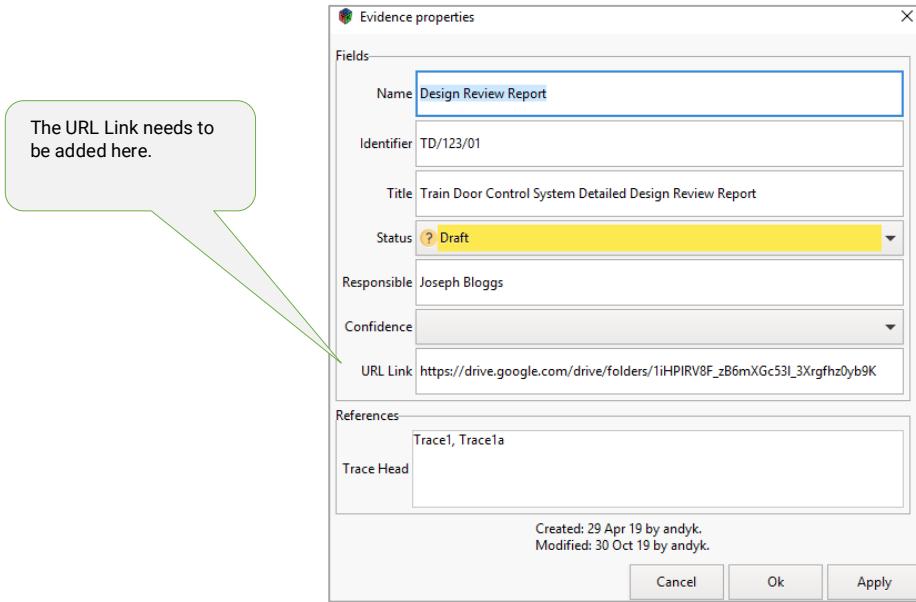


Figure 34: Adding the URL Information

Once the URL Link has been applied it will appear in the matrix as an arrow. When you hover the mouse over the link arrow the URL Link information will appear or you can add the URL Link as a column in its own right for the URL links to be permanently visible. Click on the link arrow and it will take you to the source document.

Matrix Goal Details						
Matrix Inputs (click to set)						
Door safety argument						
Matrix Output						
Name	Description	Status	Confidence	Remarks	Evidence Name	
G1	The train doors are safe	✓ Released	✓ High	Top level Goal	Design Review Report	Interlock Design Document
G2	The train doors open when commanded and the train is stopped at a station. Testing	✓ Released	? Medium	https://drive.google.com/drive/folders/1iHPIRV8F_zB6mXGc53I_3Xrgfhz0yb9K		
G2.1	The driver will only enable door opening when at a station.	✓ Released	✓ High	Training objective added		
G3	The train doors will not open when the train is under way.	✓ Released	? Medium	Engineering Maintenance Plan for Movement Sensor	Design Review Report	Interlock Design Document
G3.1	The Interlock is a mechanical lock which is only released when power is applied.	? Draft	✓ High	Under review	Design Review Report	Interlock Design Document
G3.2	The Interlock power is routed through two independent wheel motion sensors.	? Draft	✓ High	SC Approval	Design Review Report	Interlock Design Document
G4	The train doors will not open when the train is stopped other than at a station.	? Draft	✗ Low	Under Review		

Figure 44: Adding a URL Link Arrow to the Matrix

Adding Lookup Tables to Matrices

A lookup table has horizontal and vertical axes with different fields, and cells filled with values of a third type. They are used when you want to combine information from two other columns of a matrix.

Before you can use a lookup table in a matrix you have to create the following things:

- Fields for the table axes. These must also be fields in entities that appear in the matrix, so they should already exist. A field can be used as an axis for a table if it is a Boolean, an Enumeration, or a Decorated Integer with a range of 10 values or less.
- A field for the output table cells. This can be any type of field.

Once you have these fields right-click on a Package and select "Add lookup table".

Enter a name, and then double-click on the newly created  icon to open the table.

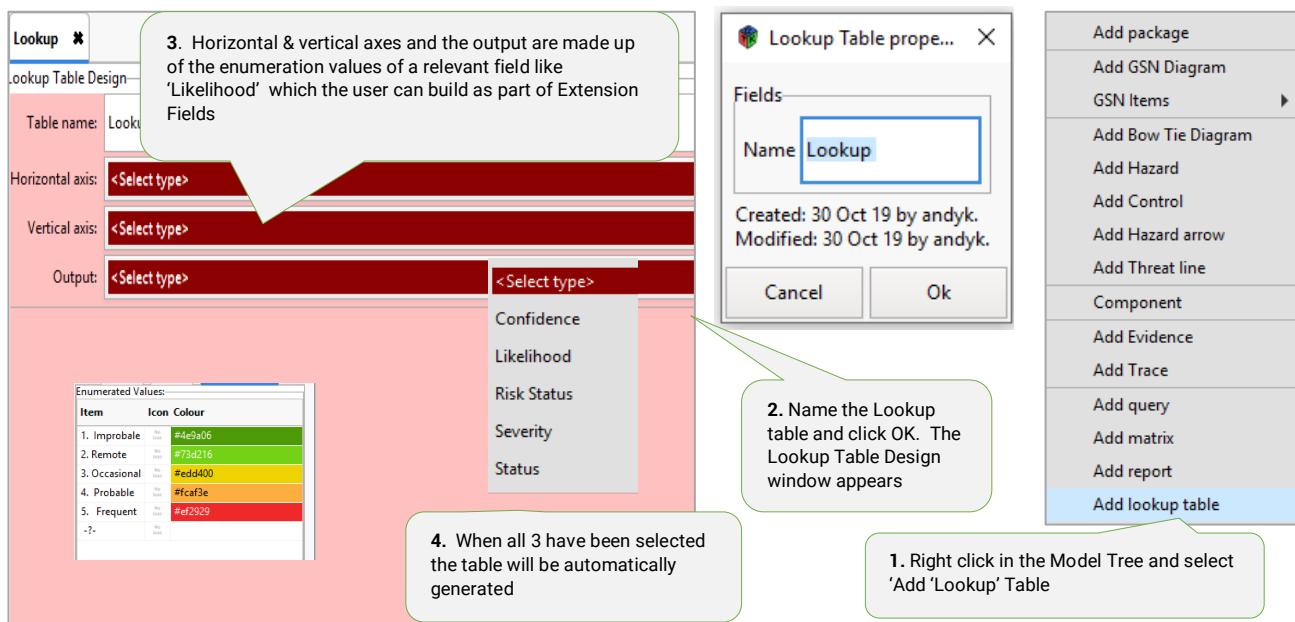


Figure 45: Adding a Lookup Table

The most common example is a risk table which has "Likelihood" and "Severity" fields as axes and "Risk Level" in the cells. Each combination of Likelihood and Severity is given a Risk Level showing how acceptable it is. Select the horizontal and vertical axes and the output field. The blank matrix will then appear below.

The screenshot shows the 'Lookup' table design interface with four stages of building a risk matrix:

- 1.** The table has now been built and can easily be amended to different axes and output using the dropdown menus.
- 2.** The required values for the matrix can then be selected in each cell to build the required Risk Levels
- 3.** Each cell is populated according to the approved risk matrix and can then be applied to Hazards and risk Matrices
- 4.** If changes to the axes or output is required, go back into the Data menu, select the relevant field and adjust the numeration values accordingly. The tables will automatically update when opened. It is very easy to build a number of risk matrices and keep them in the Model Tree.

A navigation bar on the right includes 'Data', 'Help', 'Fields', 'Reference Types', and 'Extension Fields'.

Figure 46: Building the Lookup Table

Once the table has been built it can be inserted as a column in a matrix, as shown in the diagram below.

The screenshot shows the 'Matrix Design' interface for a 'HazardLog' matrix:

- Matrix name:** HazardLog
- Description:** Project X - Hazard Log
- Matrix contents:**
 - Finding Hazards sorted by Name
 - Haz No: Field Name
 - Description: Field Description
 - Hazard Id: Field Hazard Id
 - Project System: Field Project/System
 - Likelihood: Field Likelihood
 - Severity: Field Severity
 - Risk: Lookup table Risk Matrix Train Door
- Matrix Output:** A table showing hazard details and risk levels. A callout notes: "By adding the 'Risk Matrix Train Door' lookup table as a column to the matrix builder the results will be shown in the matrix".

Figure 47: Adding the Lookup Table to the Matrix

When the matrix is run, the cells in the column are filled in with values from the lookup table cells. The DSM searches the matrix for the two axis fields starting with the current entity and then looking to the left. If it doesn't find any matching fields it leaves the cell blank. You can use 'Lookup' in a formula in a matrix or query to identify the results of a Lookup table.

The argument in brackets is the name of the lookup table. If the table is in a package then put the package names in as well, separated by "/" characters (like a file name in Windows).

The result of the Lookup function depends on the model, so this is just an example of the typical use.

Formula	Result	Type
Lookup ("Risk Register/Tables/Risk Acceptability")	Review	Text

There will be more on queries later in the Manual when we explore FMEAs, HAZOPs, Bowties and Hazard Logs.

Interacting with a Matrix

Once a Matrix has been built and run you can interact with it. You cannot change entity names but you can change fields such as 'Description'. Simply make your amendment or add additional words they will be automatically saved. If there is a drop-down selection such as' Likelihood' or 'Severity' you can change the selection simply by clicking on the drop-down arrow and selecting the category you require. If there is a look-up table in the matrix that will automatically be updated.

If you have a column with an imbedded matrix ie you have used a query in a column of the top-level matrix, you can interact with the entities it has detailed. If you right click on the name of the entity a 'Context Box' appears which will allow you open up the entity properties box or find the element in the Model Tree. If you double left click it will take you straight to the Properties Box.

In the Properties Box underneath the Model Tree you can right click on entities highlighted in the reference window to get the same context box, allowing you to look at the properties of the entity or locate it in the Model tree.

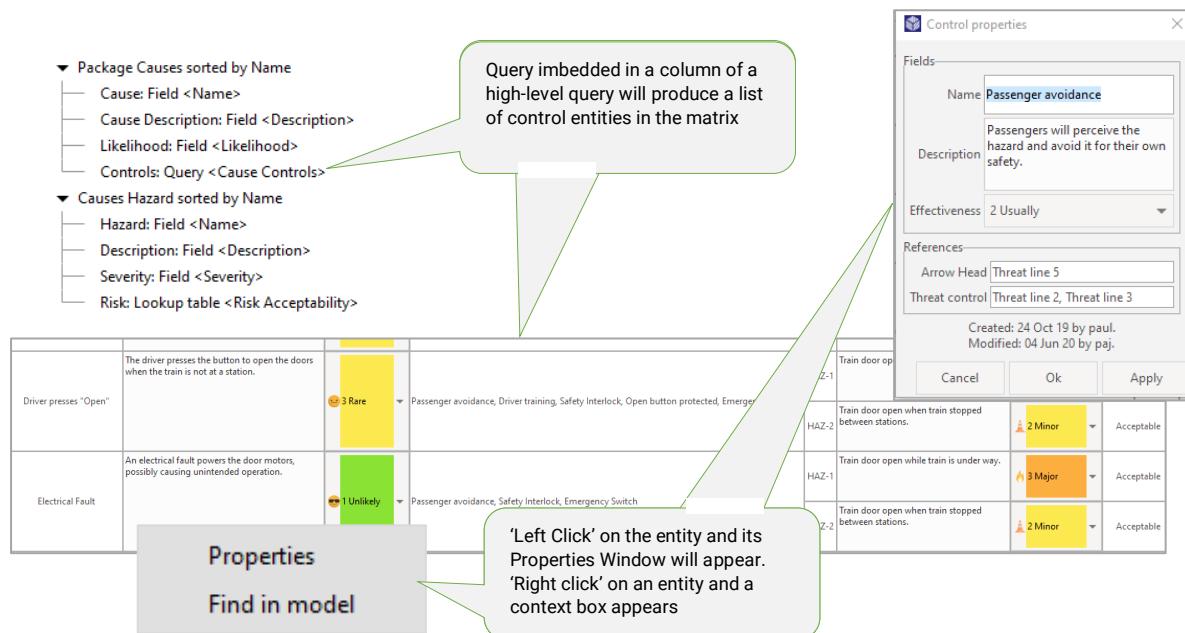


Figure 48: Interacting with Matrices

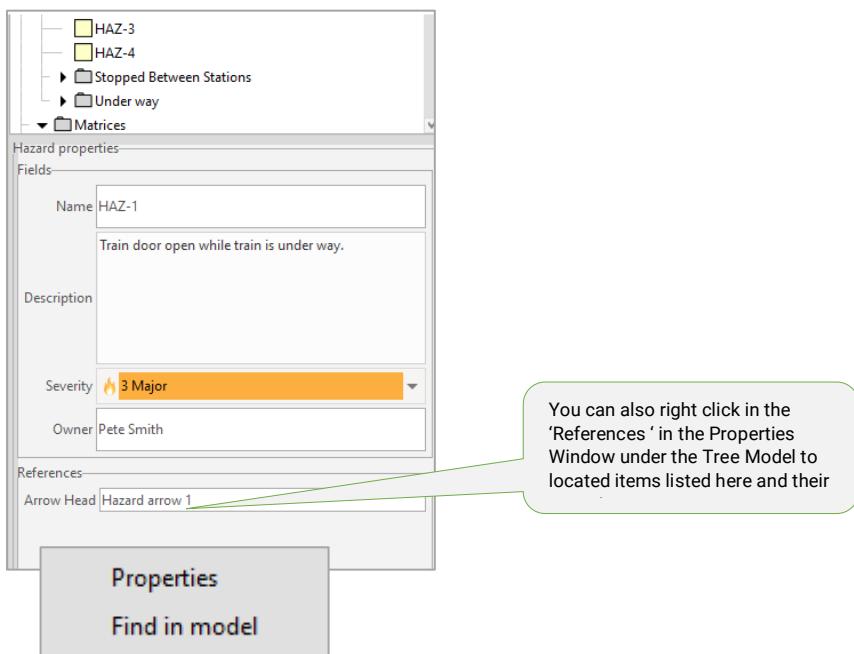


Figure 49: Interacting with References

Formulae

Formulae are key to analysing the Safety Case and presenting the data in matrices. They provide a flexible and rapid way of finding out information contained within the safety case such as:

- What has changed in the safety case over a specified period?
- Searching the safety case entities for key words that relate to a challenge or a change
- Which data fields contain certain parameters relating to GSN diagrams, risks, hazards such as owner, severity, controls etc
- Which GSN entities in the safety case are instantiated or developed

Formulae can be used in Fields, Queries and Matrices to combine information from different fields. They work very much like Excel Formulae except that they use field names instead of cell references. When adding a formula to a query you  use the "Filter" icon on the top of the Query worktop.

Useful Analytical Examples

- **Finding Key Words** – `Find("Key Words", Data Field Name)>0`

eg: `Find("SIL4",Description)>0` will find where SIL4 is used in the data field – "Description" in the Safety Case

- **Finding Updates** – Today()-Modified<=Number of days

eg: [Today\(\)-Modified<=01](#) will find all the entities in the safety case that have been modified in the last day (24 hours). By changing the number you can look back any number of days.

- **Finding Field Values** – Field name="Value"

eg: [Severity="Significant"](#) will find all the hazards with the severity "Significant"

If the file name has more than one word in its name, you need to put square brackets around the name

eg: [\[Probability Target\]="Improbable"](#) will find all the hazards with a probability target of "Improbable"

- **Finding Goals in the Safety Case that still need developing** - “! Developed”

eg: [“Developed”](#) will find all the goals in the safety case that have the ‘Developed’ box ticked

[“! Developed”](#) will find all the goals in the safety case that have the ‘Undeveloped’ box unticked ie they need more work.

- **Finding Goals that are instantiated** – “! Instantiated”

eg: [“Instantiated”](#) will find all the goals in the safety case that have the ‘Instantiated’ box ticked.

[“! Instantiated”](#) will find all the goals in the safety case that have where the ‘Instantiated’ box is not ticked – they need more actual detail

- **Finding the Results of a Look-up Table** – Lookup Table – Risk Acceptability

eg: [Lookup \(“Risk Register/Tables/Risk Acceptability”\)](#) will find all the elements in a matrix look up table with the Result you require ‘acceptable’ etc

- **Joining 2 Fields together in a Matrix** – First Field name ++ “,” ++ Second Field name

eg: [Responsible ++ “,” ++ Department](#) will join the field “Responsible with the Field “Department” to present both sets of data in a single column in the matrix.

Filter Condition

When you edit a formula, you will get an expression dialog which tells you of any problems as you type. However, it cannot tell the difference between a wrong expression and an incomplete one, so as you type you will see things like this:

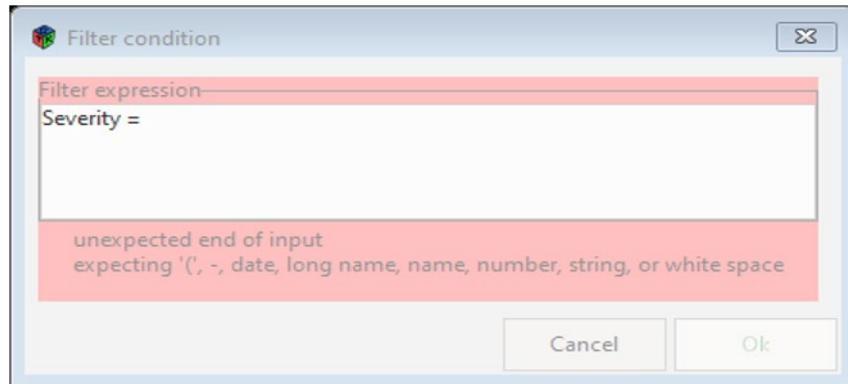


Figure 50: Error Message from partly completed formula

This is not wrong; once you complete the formula the error message will go away, and the OK button will be enabled.

Formulae in Queries and Matrices

An example of how a formula is used in the Query and a Matrix is shown below:

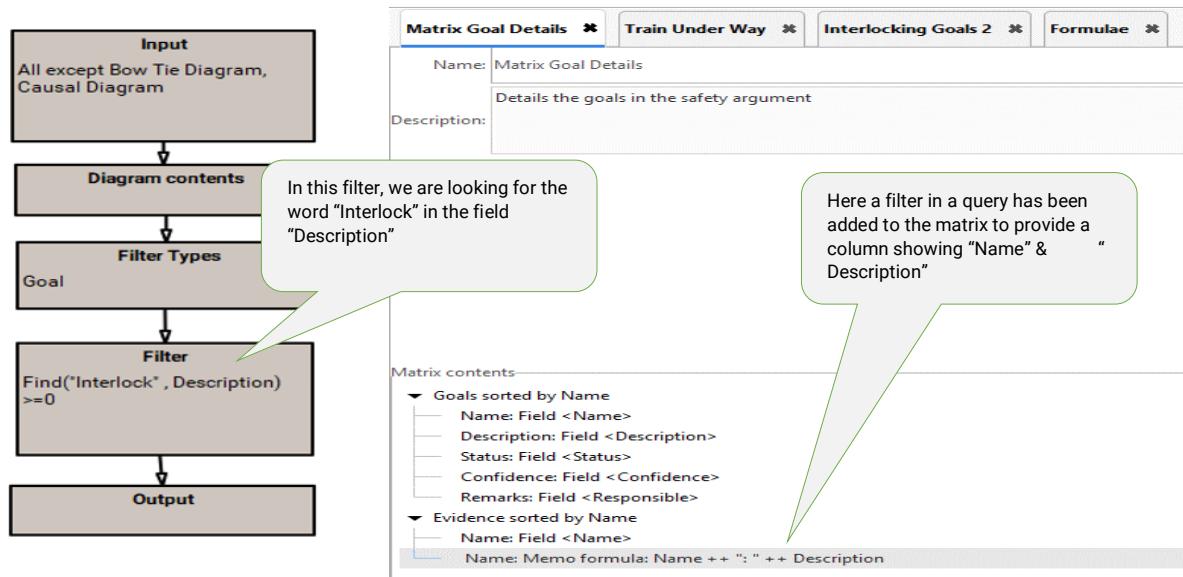


Figure 51: Formulae in Queries & Matrices

A full list of formulae functions is given in Annex A.

Reports

Generating Reports

The ability to generate reports, whether electronic or paper based, is still an important requirement in today's system engineering environment. Conventionally, the safety case is still thought of as a report and many regulatory bodies will require a paper-based report for review and filing. As new information is added to the safety cases in the DSM, reports can be automatically updated, and regulatory bodies notified. The DSM can generate reports in HTML or Microsoft Word.

Most safety reports consist of a body of text outlining the key aspects of the safety case and ending with the conclusions. The detailed safety case (GSN argument, HAZOPs etc) are then included as a set of appendices. The body of the report is therefore best produced using a word processor while the DSM is used to produce the appendices.

The DSM reporting feature can output these appendices as a stand-alone Word document. This can be appended to the main Word document as follows:

1. In Word, open up the main document and put the cursor at the end.
2. Select the "Insert" ribbon, then the "Object" pull-down menu and "Text from File..." (see image).
3. Select the DSM output Word file and click "Insert".

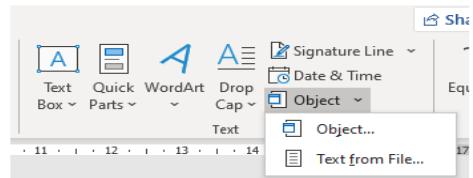
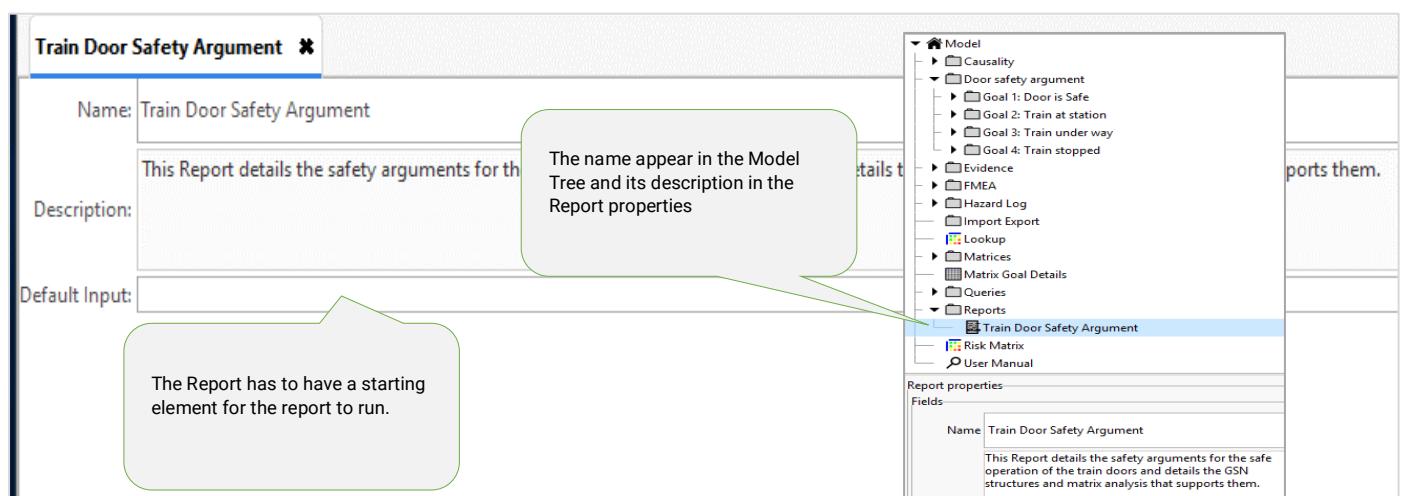


Figure 52: Importing into Word

To capture the GSN diagrams and associated Matrices a report 'Structure' is built. As with matrices a report structure uses queries to define its content. The first step is to give the Report a name that will appear in the Model Tree and any description you wish to add which is visible in the properties box.

Part 1- Giving the Report a Name & Description



The name appears in the Model Tree and its description in the Report properties

The Report has to have a starting element for the report to run.

Figure 53: Creating a Report in the Model Tree

The structure part of the window above (currently blank) is where you build the contents of the Report. Designed to be added as an Annex to a report built in a Word Processor, you can incorporate headings, sub-headings, text, diagrams and matrices that are then published as a Word Document.

When a report is run it takes an 'entity' as a starting element. This is passed as input to the query in a top-level Section element, and the contents of the Section are then run for each entity output from that query. Sections can contain sub-sections, each with its own query. This makes complex and detailed reports easy to define.

Headings are added either as a straight text entry, or as data in an entity field such as 'Name' or 'Title' etc.

As indicated above, sections allow you to add the results of a query, matrices and Lookup tables into the report.

In this example 'Goals' that support the argument must be identified. You can see them in the Model Tree: **Goal 1, Goal 2, Goal 3 etc**. A query that finds these goals is used to do this and this query has already been built and is called 'GSN Packages'.

Part 2 – Building the Structure of the Report

The first action is to add a Report Heading to the Structure window (See Figure 57: Building a Report) and then add a section inside which the query that finds the Goals (GSN Packages) and the name of those goals. (See Figure 58: Adding a Section to the Report

The figure consists of two parts. On the left is a screenshot of a software interface showing the 'Train Door Safety Argument' report structure. It includes fields for Name (Train Door Safety Argument), Description (This Report details the safety arguments for the safe operation of the train doors and details the GSN structures and matrix analysis that supports them.), and Default Input (Door Safety Argument). A callout box points from the 'Default Input' field to a text box containing the note: 'If the Report were published now it would appear like this, listing the Goals that provide the argument'. On the right is the resulting report output, which is a document titled '1 Door safety argument'. The document contains the text: 'The top level argument that the doors are safe.' followed by a list of four goals: 'Goal 1: Door is Safe', 'Goal 2: Train at station', 'Goal 3: Train under way', and 'Goal 4: Train stopped'.

Figure 54: Using a query to bring Goal entities

The second action is to add another section, inside the first section that uses a query to find the actual diagrams contained under these goals. Like matrices, the second query in a report must start from the results of the first query (See Figure 59: Adding Queries to a Section)

Train Door Safety Argument *

Name: Train Door Safety Argument

This Report details the safety arguments for the safe operation of the train doors and details the GSN structures and matrix analysis that supports them.

Description:

Default Input: Door Safety Argument

Structure

Heading 1: <Name>

<Introduction>

▼ Section: GSN packages

- > <Name>
- > ▼ Section: Package Diagrams
- > Diagram

The GSN diagrams now appear in the Report when published

The second section is added inside the first section

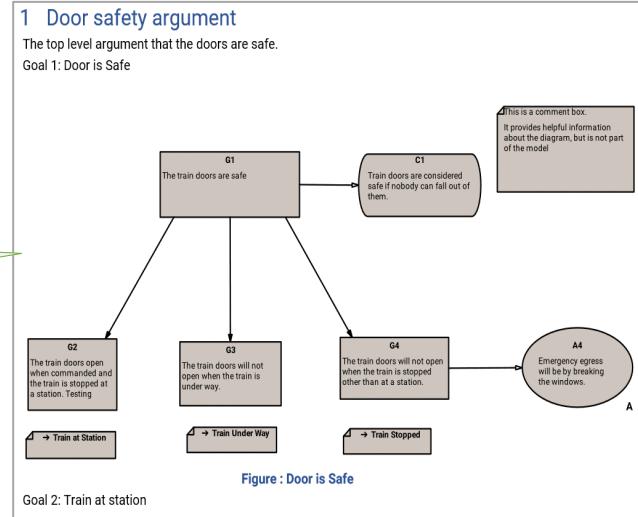


Figure 55: Using a second query to bring in GSN diagrams

If I now want to add a matrix that includes the Evidence details for a Goal, add another line under diagrams that captures the Matrix – ‘Evidence’ from the Model tree. The matrix will be applied to all the goals and will appear in the published report

Train Door Safety Argument *

Name: Train Door Safety Argument

This Report details the safety arguments for the safe operation of the train doors and details the GSN structures and matrix analysis that supports them.

Description:

Default Input: Door Safety Argument

Structure

Heading 1: <Name>

<Introduction>

▼ Section: GSN packages

- > <Name>
- > ▼ Section: Package Diagrams
- > Diagram
- > Matrix: Evidence

The evidence table now appears in the report

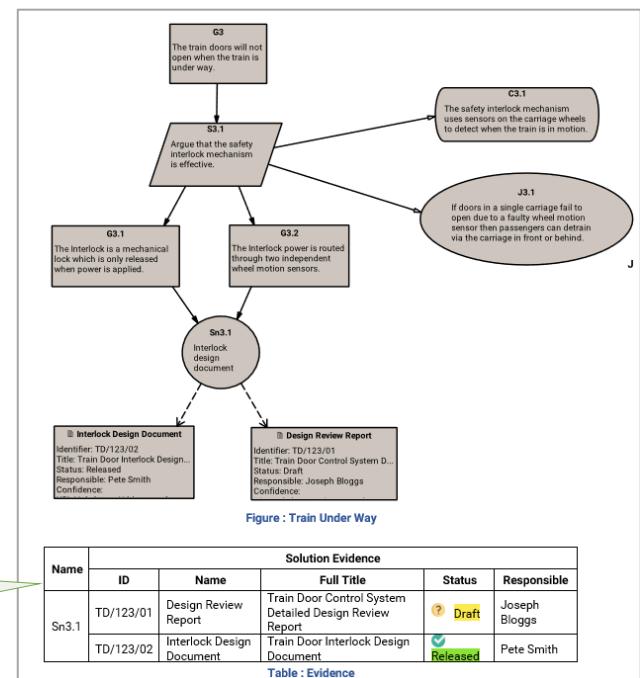


Figure 56: Using a Matrix to bring in additional data

Creating a Report

As with queries and matrices, reports are created in the Model Tree by right clicking on a Package and selecting ‘Add Report’. Once the report has been named and appears in the Model Tree, right click on the Report symbol and select ‘Edit Report’. See the Diagram below. The Edit Report window will appear with a blank Structure panel. Right click in this empty panel and a drop-down list will appear with the type of report formats you can select.

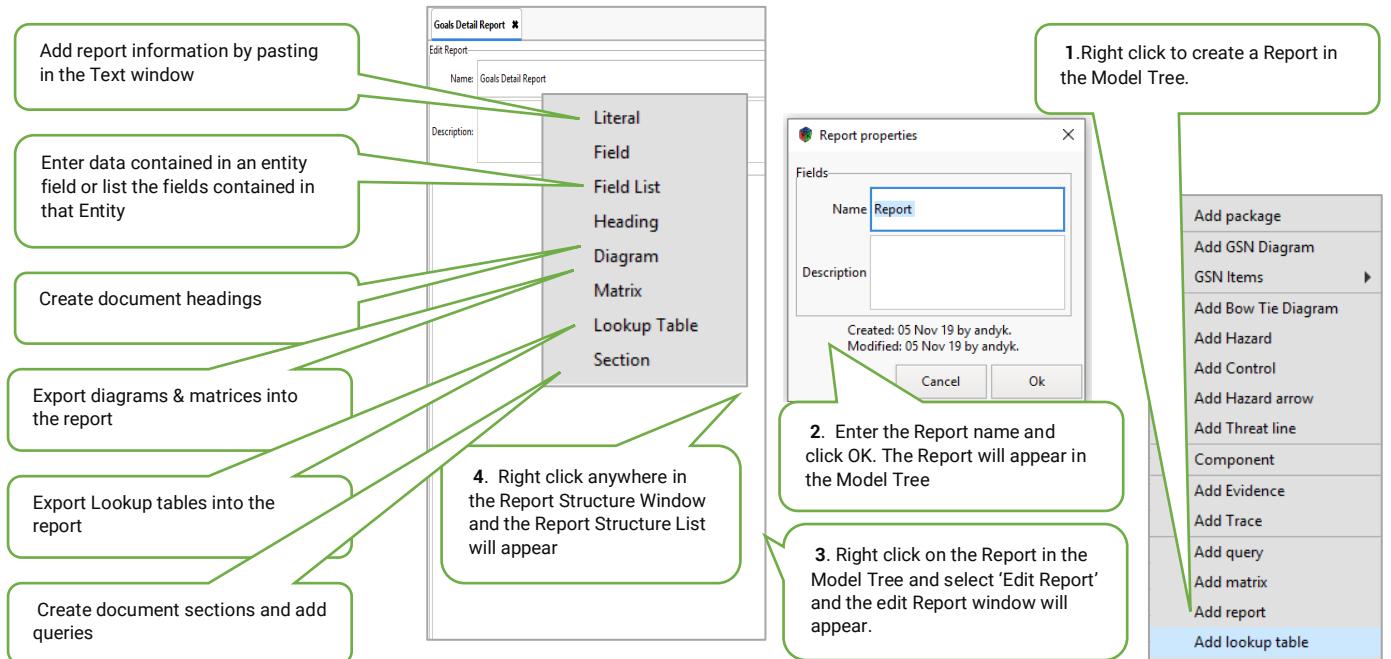


Figure 57: Anatomy of a Report

Adding Information into a Report

A report, like a matrix, is designed to analyse and report information from within the model. A report is designed as a tree in which each “leaf” contributes an element to the final report. To insert a new element then right-click on either the background or an existing element. Then choose

where the new element is to be inserted and what it is to be. The tree of report elements can be rearranged by clicking and dragging items, but only Section items can have children.

Some of these elements use the “current entity”. At the top level this will be the input entity. Within a Section element the contents of the Section will be run once for each output of its query, so the “current entity” will be one of the query outputs.

The following elements are available:

Literal: Text that is inserted into the report without change every time

Field: The contents of a field from the current entity. This is inserted into the report in-line, so you could include a field between two literals and it will be output as a single paragraph.

Field List: One or more fields from the current entity inserted as a definition list (i.e. formatted like this one).

Heading: Text and/or a field of the current entity that are to be inserted as a chapter heading within the report.

Diagram: If the current entity is a diagram then it will be inserted with its name as a caption. Otherwise this does nothing.

Matrix: Runs a matrix with the current entity as input and inserts the result as a table with the matrix name and current entity name as caption.

Lookup table: Inserts the lookup table as a table.

Section: Runs a query with the current entity as input. Sections can have elements as children within them, and these elements will be run for each entity that the query outputs. These outputs can be sorted by ascending or descending order and like Matrices, a small arrow will show the direction of ordering.

If you select ‘Heading’ by double clicking on the heading line a ‘Heading Window’ will appear and you can enter text. You can also select the Heading hierarchy for each heading by selecting levels 1 – 5. After each heading you then select the ‘Literal Text’ field shown with quotation marks - “” - and you can add or paste text from other documents here.

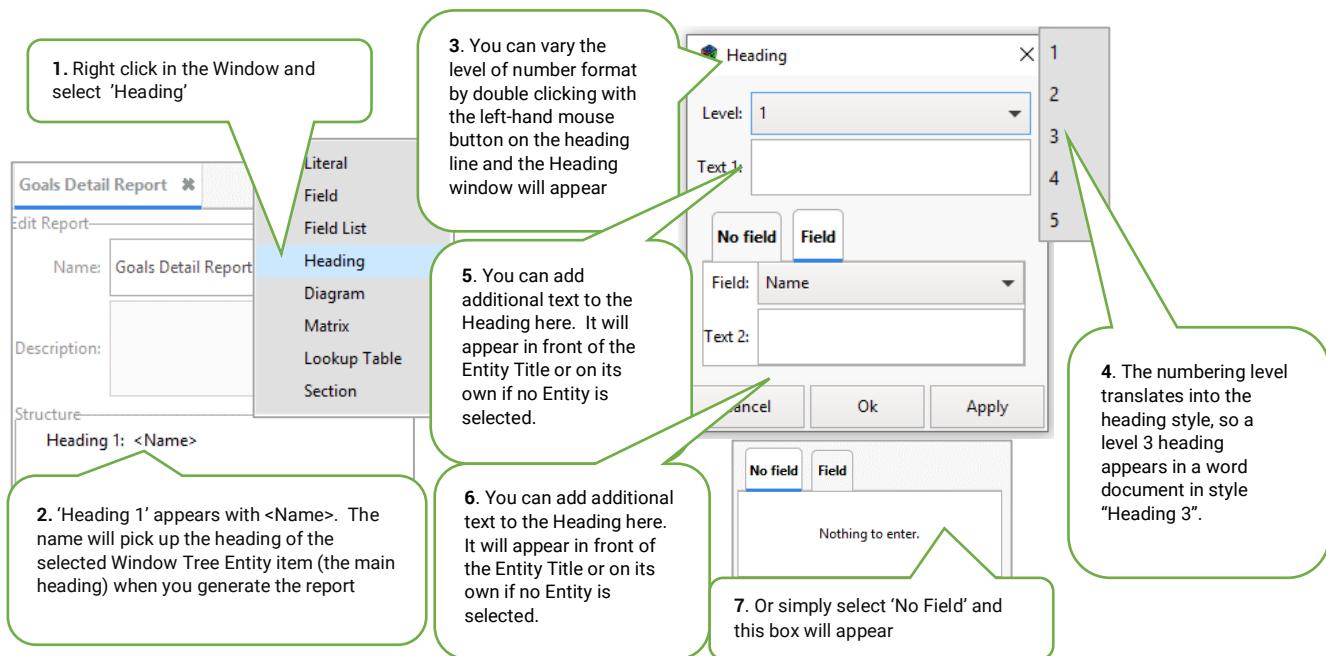


Figure 58: Building a Report

To add GSN diagrams to a report, add a section and use a query that finds the required diagrams select ‘Section’ from the Edit Report window and ‘Section’ now appears in the report structure as ‘**Section <Not Set>**’. Double click on this line and the Select Query window will appear. Click into the query box and a query selector will show you all the queries you have built – in this case you will be looking for the queries that find your diagrams. Insert fields and diagrams inside the Section by right-clicking and using “Add inside” from the drop-down menu.

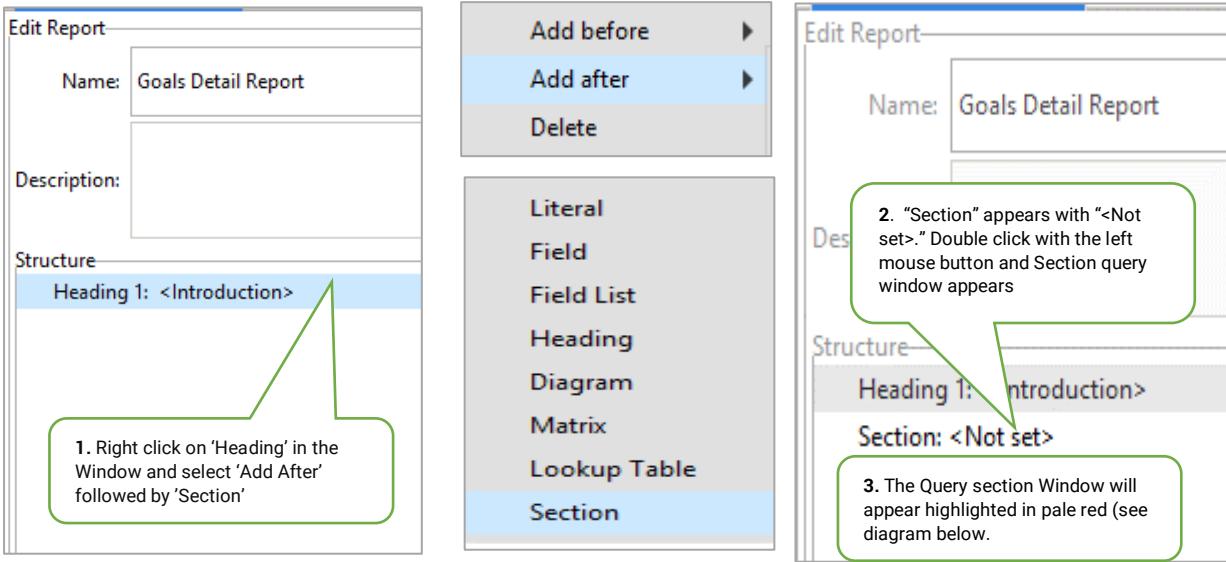


Figure 59: Adding a Section to the Report

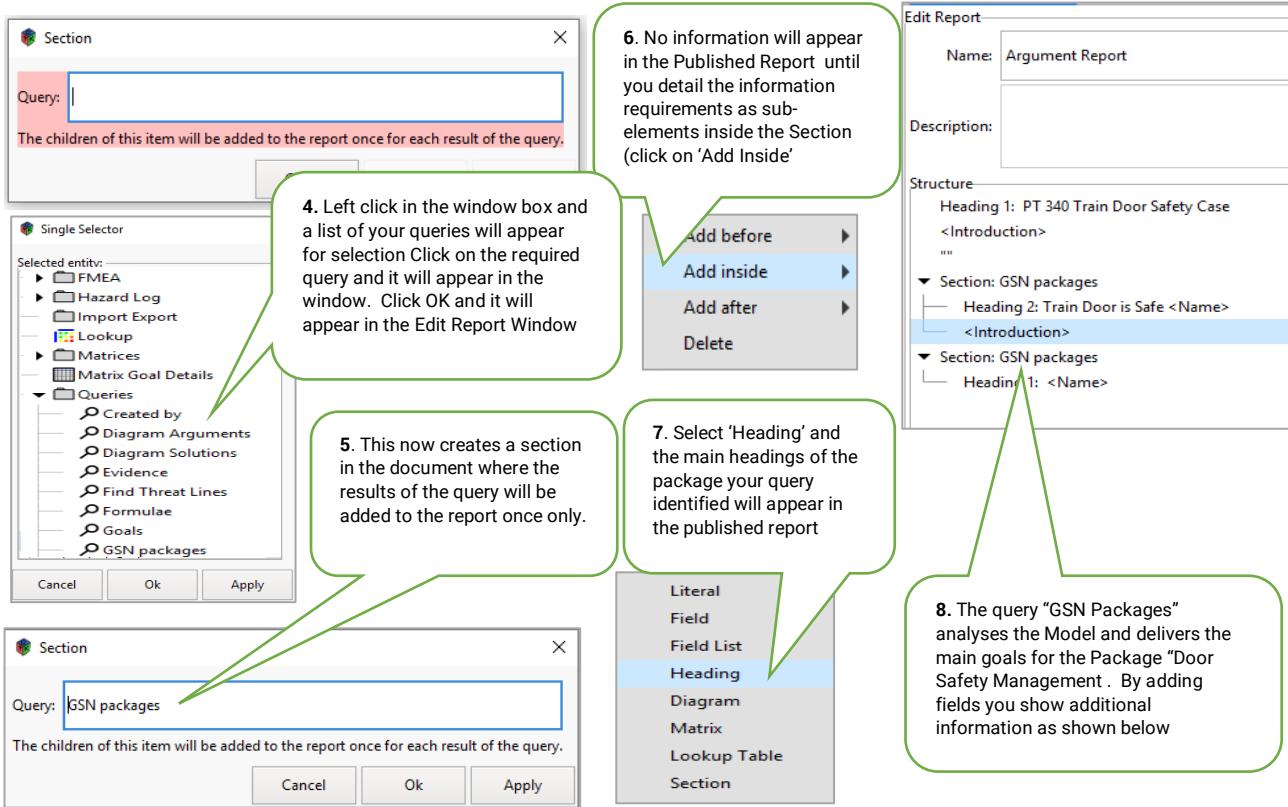


Figure 60: Adding Queries to a Section

The figure below shows how GSN diagrams and analytical matrices can be added to the report in any combination and number to produce a comprehensive Safety Case Report.

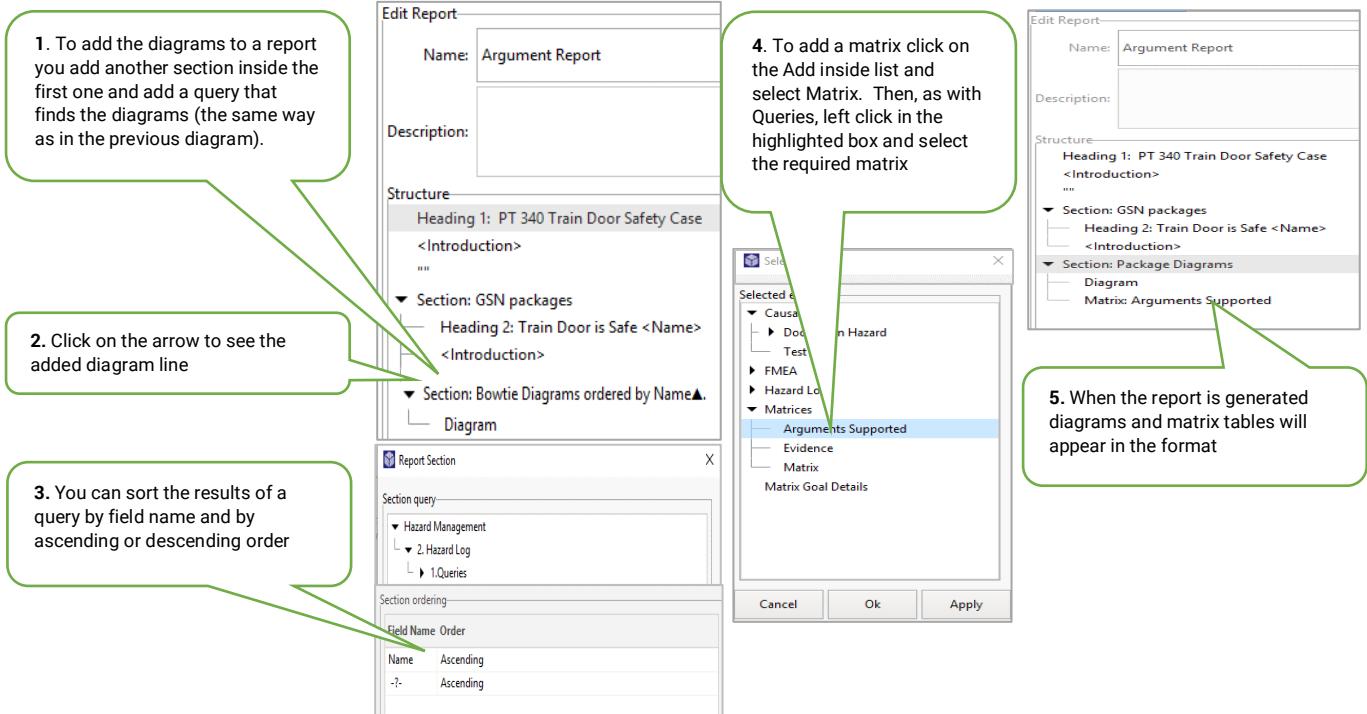


Figure 61: Adding Diagrams and Matrices to a Section

Previewing Reports

When you are building a report you can preview how it looks by using the preview entry in the Context menu. This exports the report to a temporary HTML file and activates the web browser automatically.

Publishing Reports

When you want to publish the report, click on the report icon and select 'Run Report'. You can select the output format – DocX for Word or HTML for the Web – and the report will be generated and saved in your file system - see the diagram below. To edit the report click on the report icon once more, double click on the line you wish to change and the edit window will appear. Then run the report and save it or change the version number in the file title to create an additional copy.

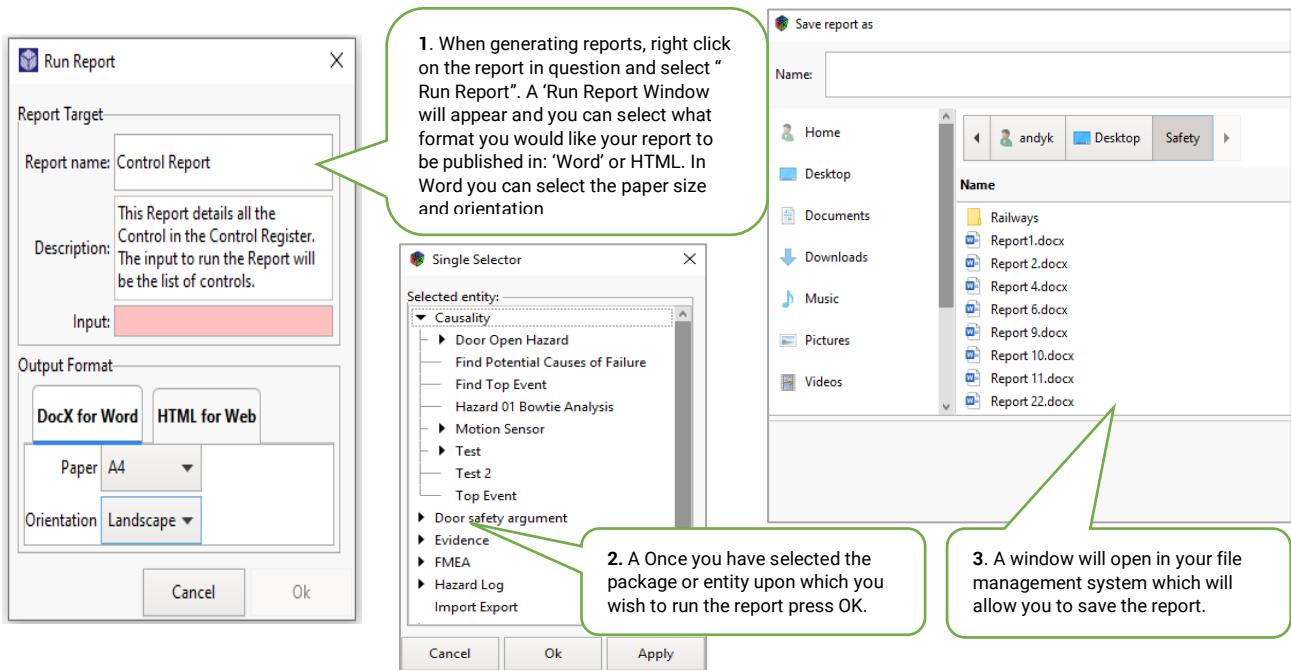


Figure 62: Publishing a Report

Cloning Entities

Entities can be cloned or duplicated to speed up safety case construction. For example, a Matrix or a Report can be cloned and amended, rather than building a similar matrix or report which will take time.

Each entity in the Model Tree now has a Clone entry in their context menu. When selected a duplicate entity appears with the extension 'clone-1' added to the title. This duplicate can then be amended as required and saved with a new title.

Importing & Exporting

The DSM has the following import and export capabilities.

- Export selected packages with subordinate entities and associated extensions.
- Export diagrams as PDF, SVG or PNG files.
- Export matrices into Microsoft Excel.
- Import previously exported packages.
- Import from a Microsoft Excel spreadsheet to create or update entities.

Exporting Selected Data & Extensions

To export data from the model for import into another, just click on the export button (). A dialog will appear with the model tree and an option to export the extensions. Select the packages you wish to export in the dialog (ctrl-click to select multiple entities) and decide whether you want to include the extensions or not.

The “Export Extensions” box controls the export of the definitions of the extension fields and references (i.e. the things found under the “Data” menu). If the box is ticked then all the extension field and reference definitions for the model will be exported along with the data. The contents of those fields in the entities will be exported regardless.

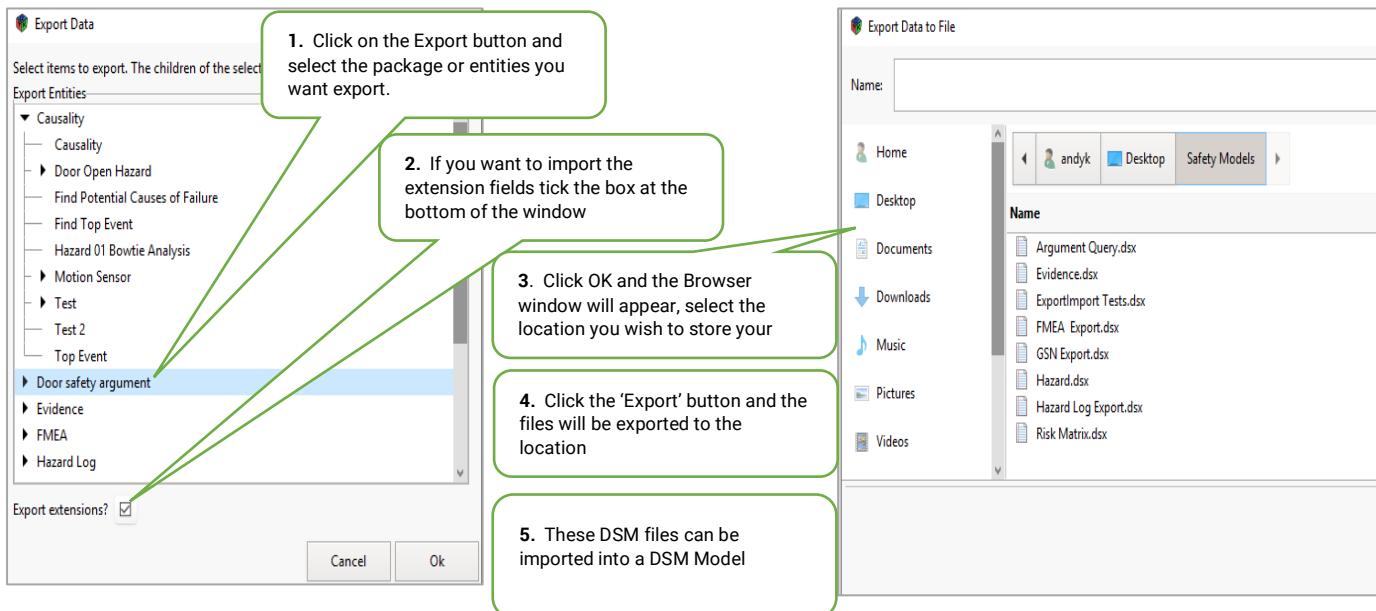


Figure 63: Exporting selected data & Extensions

Once you have selected the entities to export click “OK”. A file dialog will appear for you to select the export location. The DSM will export the data in the format of a DSM file which can be quickly imported into another model. Reports, matrices, queries and lookup tables can all be copied from one safety case model to another.

Exporting from a Matrix into Microsoft Excel

Matrices are at the heart of the DSM and can be quickly exported in a spreadsheet to aid distribution and feedback.

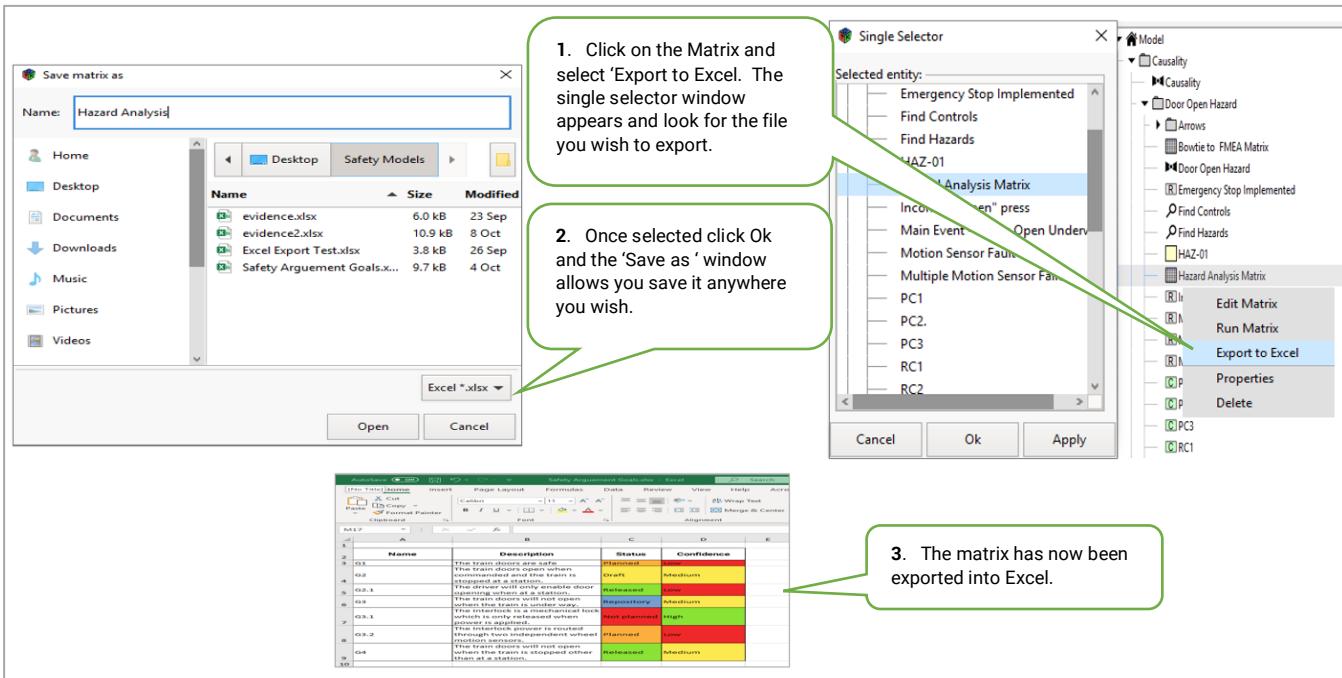


Figure 64: Exporting from a Matrix to Excel

Exporting Diagrams

Open the diagram you want to export in the diagram editor and click the Diagram Export button . A file save dialog will appear with a menu for the type of image file to generate. The options are:

SVG: Vector graphic format suitable for importing into modern versions of MS Office.

PNG: Pixel image format suitable for older versions of MS Office.

PDF: Stand-alone document format.

PS: Postscript. Obsolete for document sharing but still sometimes useful.

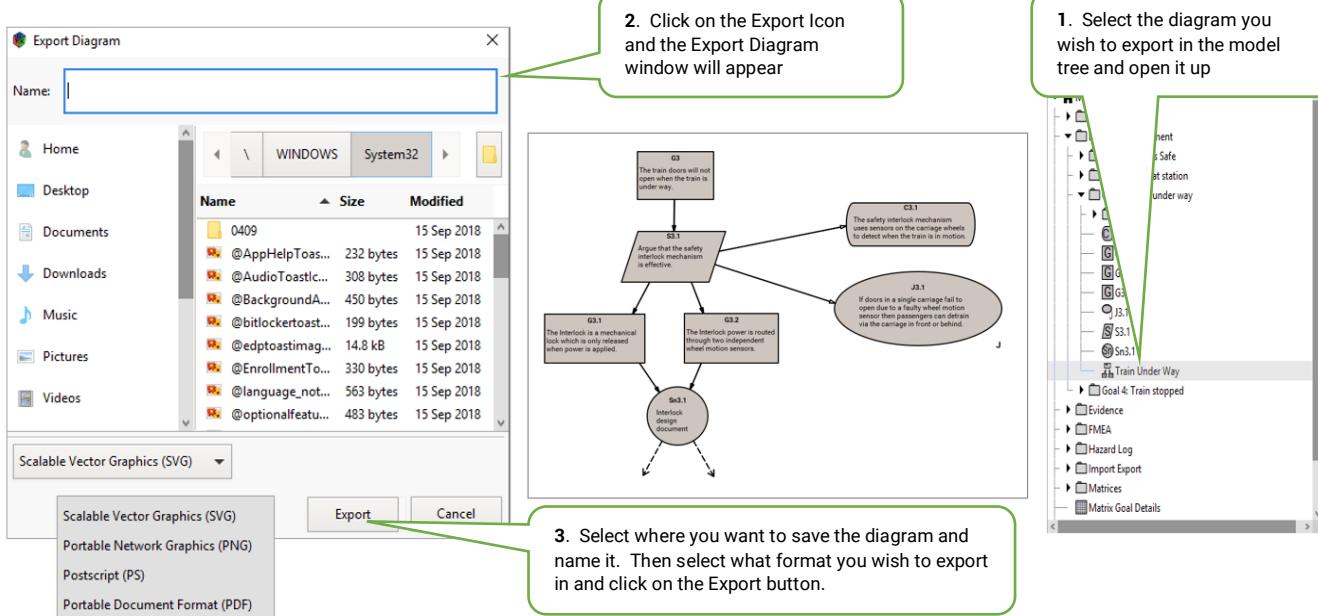


Figure 65: Exporting Diagrams

Importing Selected Data & Extensions

To import material previously exported from another DSM model, click on the “Import” button at the top of the page, select the file to be imported, select the location you want to import to (you may need to create a holding package for this), decide whether you want to import any field extensions, click OK, and the import will take place. If you tick the “Import extensions” box, then any extension data fields in the imported file will be added to the ones already existing. If an imported extension field has the same name as an existing one then the existing field definition will be overwritten.

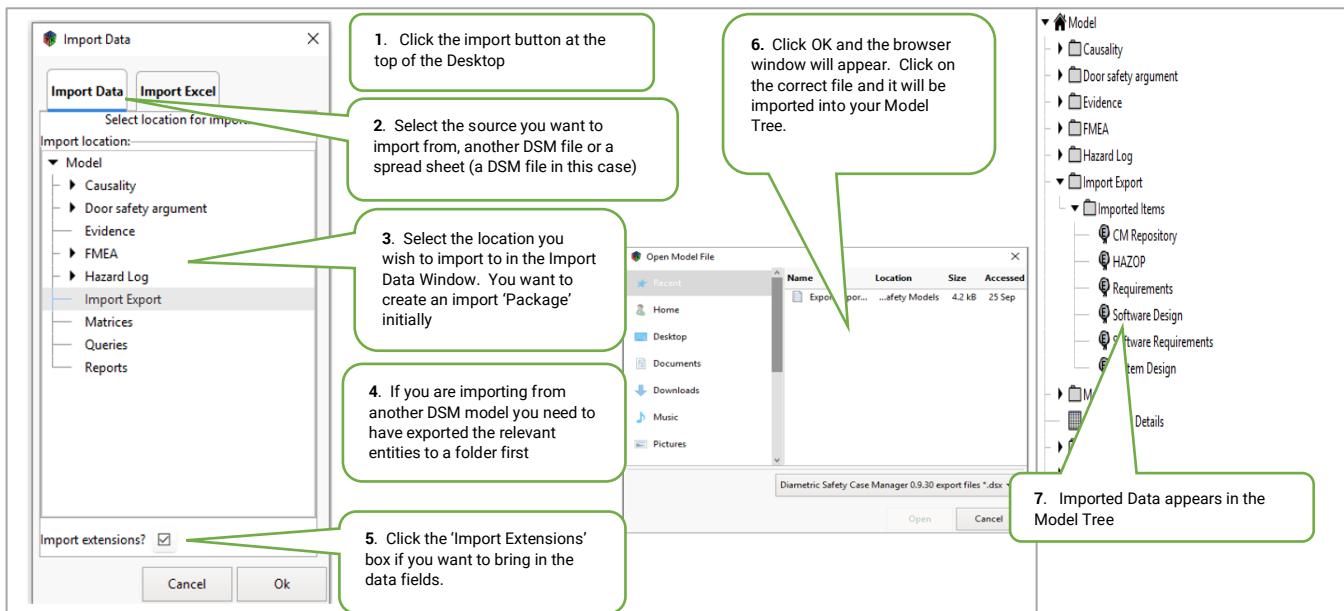


Figure 66: Importing selected Data and Extensions

Importing Data from an Excel File

When importing from a Spreadsheet the rows of the Excel Spreadsheet are the entities in the DSM and the columns are the data fields. All the imported entities will be of the type selected in the import dialog. The columns in the spreadsheet must have headings that match the data fields in the entity type for the import to work properly (the column order does not matter). You may need to add extension fields to the DSM entity type before importing the data. The DSM will automatically align the data in the Excel columns with the data fields in the entity.

Caution

It is important when importing from a spreadsheet to make sure the column headings in the spreadsheet match exactly the title of the data fields that you are importing into. Moreover there should be no gaps or additional blank rows above the first row. The import will not work otherwise.

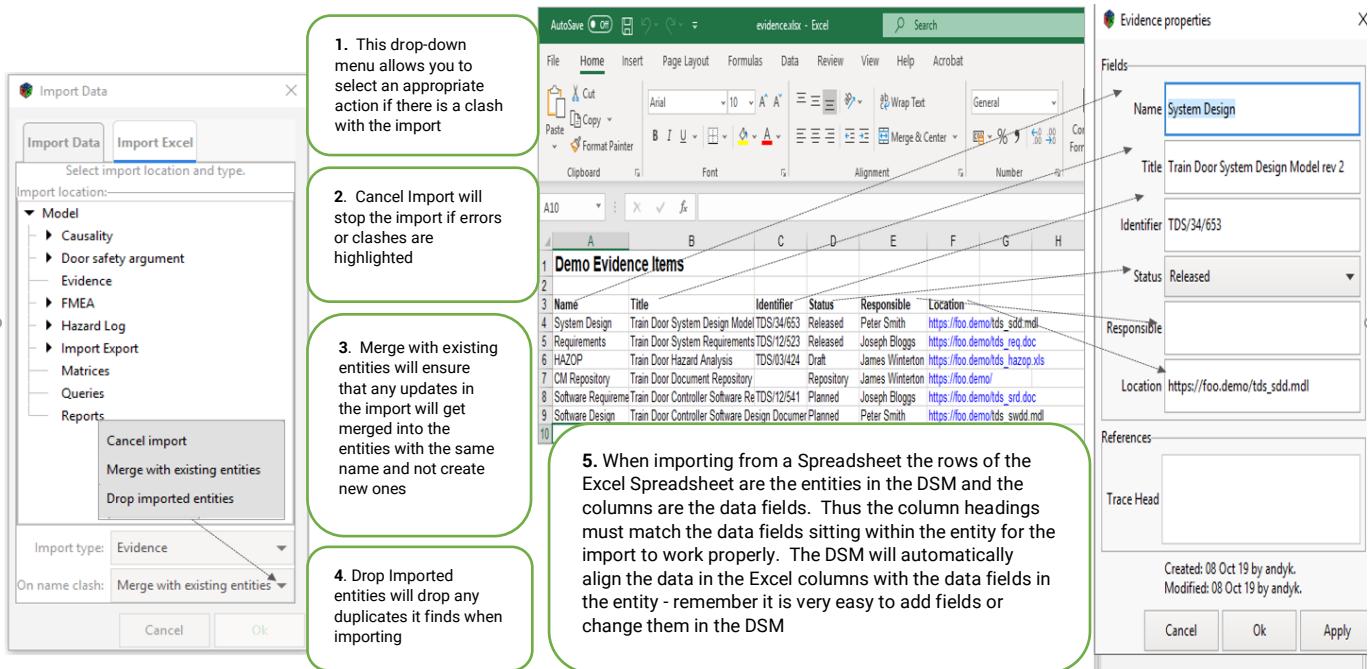


Figure 67: Importing selected Data from a Spreadsheet

Bowtie

Bowtie is used for risk assessment, risk management and risk communication. Its methodology is designed to give a better overview of the situation in which certain risks and helps people understand the relationship between the risks and organizational events. It is a graphical tool to illustrate an accident scenario, starting from accident causes and ending with its consequences.

Bowtie Functionality

The DSM uses the Bowtie functionality to provide clear a diagrammatic representation and the following functionality is delivered in the Diagram Editor.

Icon	Entity Type
	Model Tree Icon for a Bowtie Diagram
	Bowtie Event – Source, Main event or consequence in a Bowtie Diagram
	Hazard – An object, situation or behaviour that has the potential to cause injury
	Control or Barrier: Prevents or reduces the likelihood of a threat
	Hazard Arrow – references the Hazard from the top event
	Threat Line – the line that leads from the source to the top event and to the consequences
	Trace Line – links entities to evidence such as reports or a hazard log

Figure 68: Entity Type

When you select a Bowtie Diagram from the Model Tree, this functionality is automatically made available in the diagram editor.

Bowtie Diagrams

Bowtie Diagrams originated as a technique for developing a safety case in the Oil & Gas Industry, post the Piper Alpha Incident in 1988. By linking hazards and consequences to an event, it is possible to develop the relationship to include the causes or threats and the prevention and recovery controls or barriers to prevent them.

A Hazard will have sources, a top event or potential accident, consequences and threat lines that link threat sources to the top event and the top event to consequences. These entities can be created in the diagram editor and by selecting a Bowtie Diagram in the Model tree, a Bowtie Desktop is made available. Events, Hazards, controls, threat lines, hazard lines and trace lines are used to create an effective Bowtie structure. The top event (accident), the sources (or threats) to that event and the consequences are all Bowtie Events in the DSM. Threat lines will link these together and controls will sit along the threat lines to prevent the accident happening or to effect rapid recovery and minimum effect when the accident does happen.

Building the Bowtie

In the Bowtie Diagram editor create the events, add the necessary data to the fields sitting behind these events and join threats to the accident and to the consequences, as shown below:

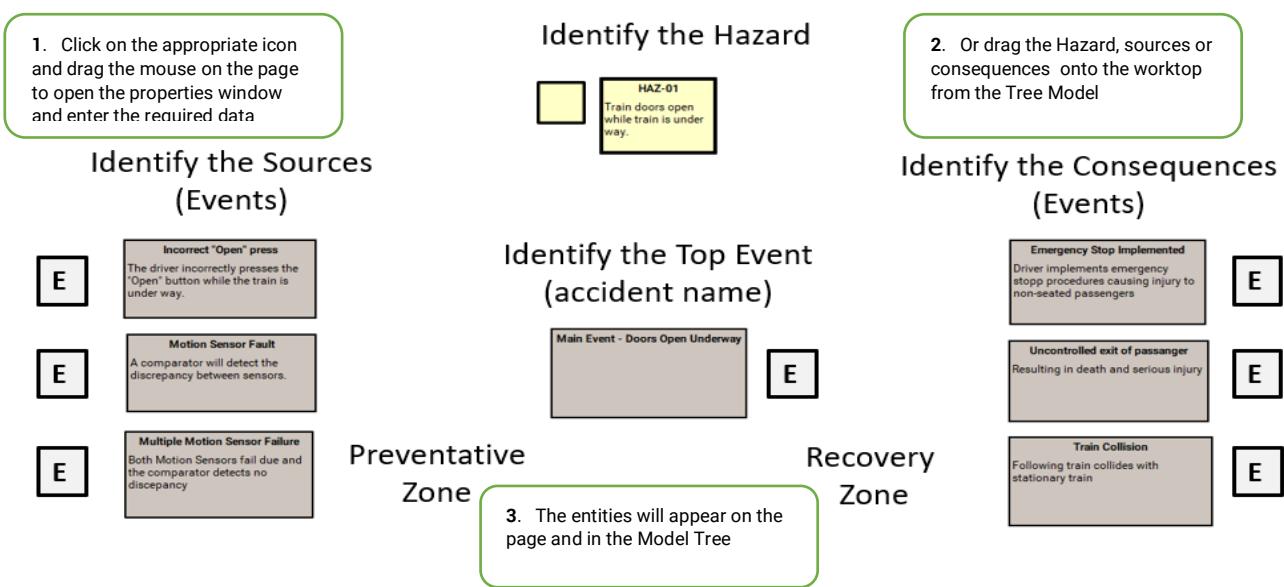


Figure 69: Building the Bowtie

Linking the Bowtie Entities

Linking accident sources and accident consequences to the top event and thus to the Hazard will provide the basis for assigning barriers or controls in the preventative or recovery zones and allow detailed analysis through queries. "What are the sources of an accident? What are the barriers that prevent them etc.

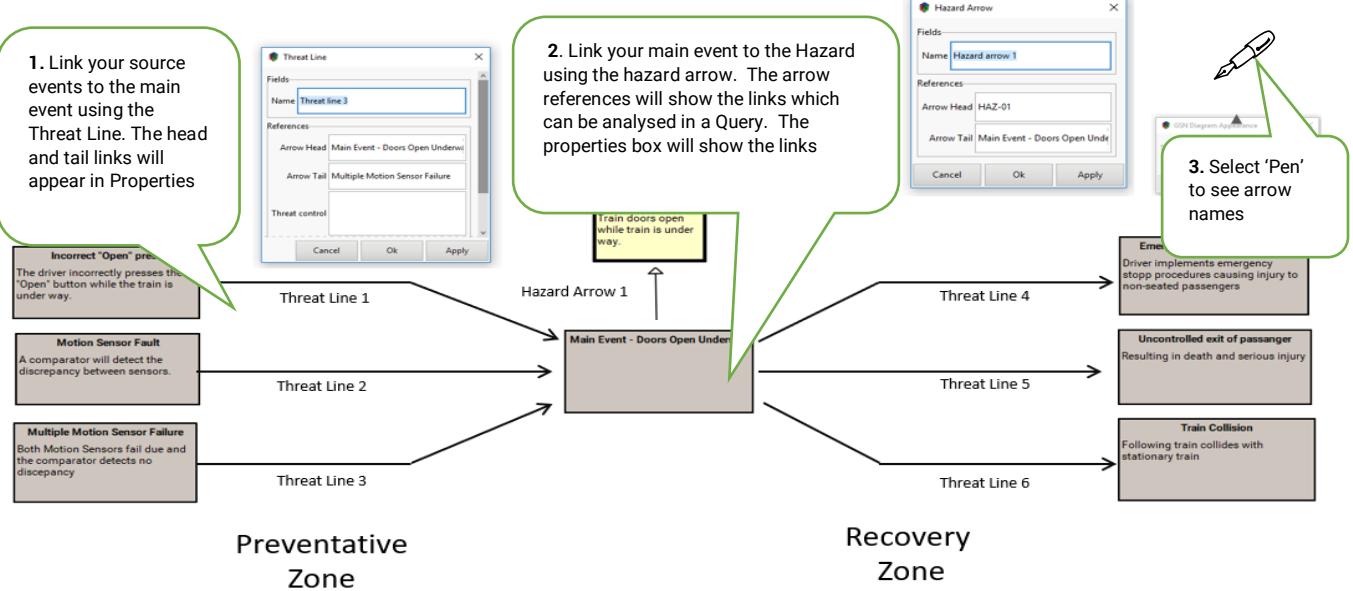


Figure 70: Linking the Entities

Creating Controls

In the DSM, barriers and controls are the same entity and are detailed by the **C** icon. With multiple controls to apply to a single threat line, the Control entity can be shrunk to just its title and or a single threat line joining a source to a main event can be displayed. Queries will pick up the necessary information no matter how it is displayed.

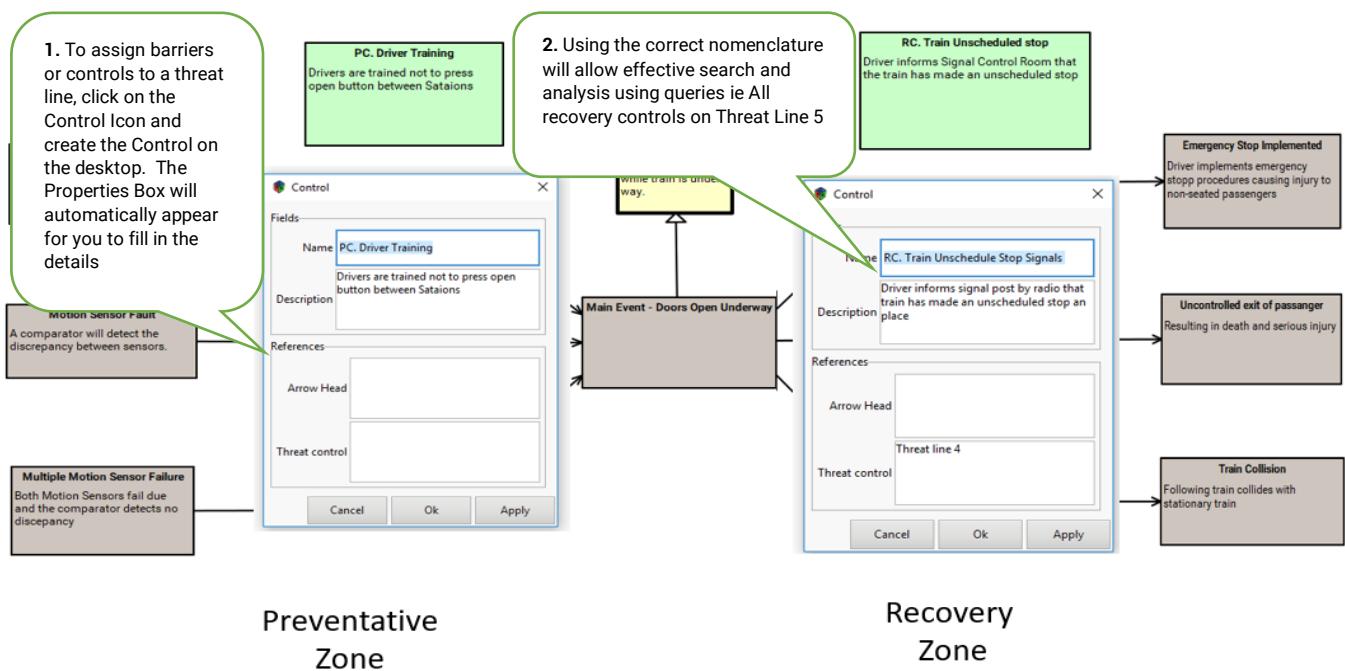


Figure 71: Creating Controls

Assigning Controls

To assign controls to a threat line it is simply a matter of dragging the 'Control' onto the relevant threat line and the link will automatically be made and shown in the 'Reference Fields' of the 'Threat Line'.

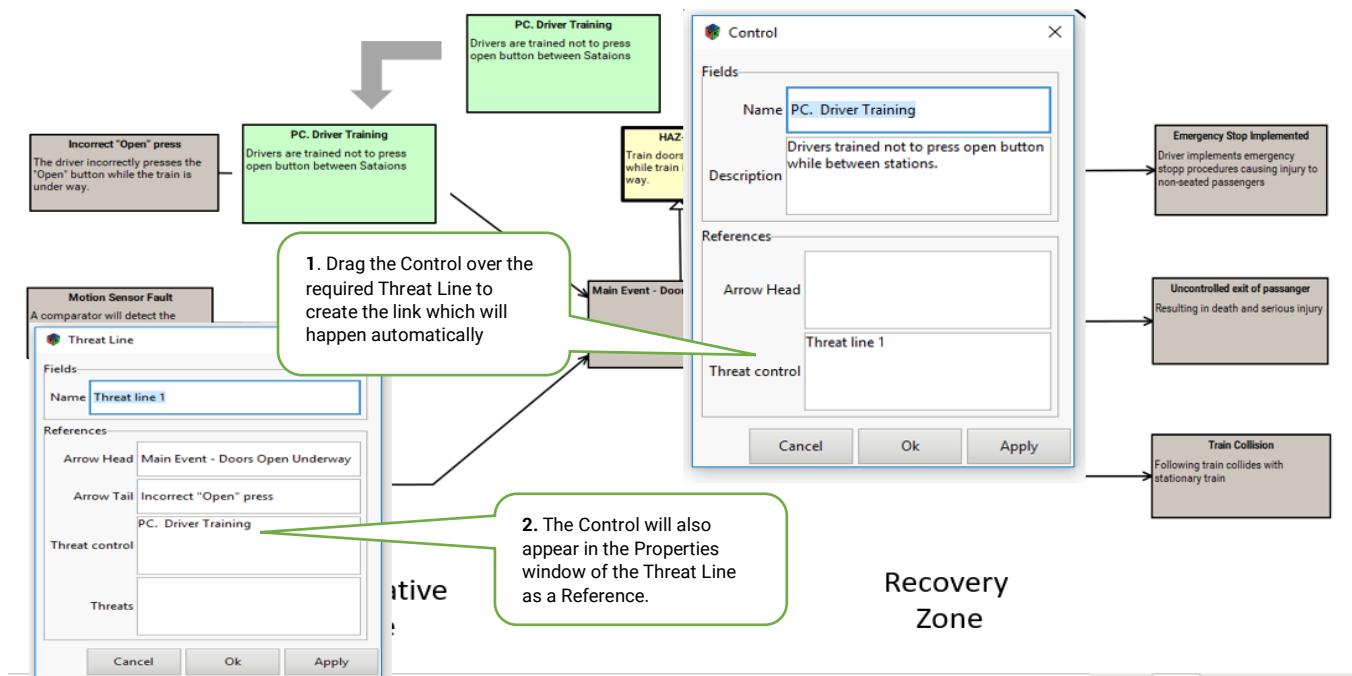


Figure 72: Assigning Controls to a Threat Line

Assigning Evidence

Once the Bowtie has been built, you can use the trace arrow to link to any evidential documents or control registers.

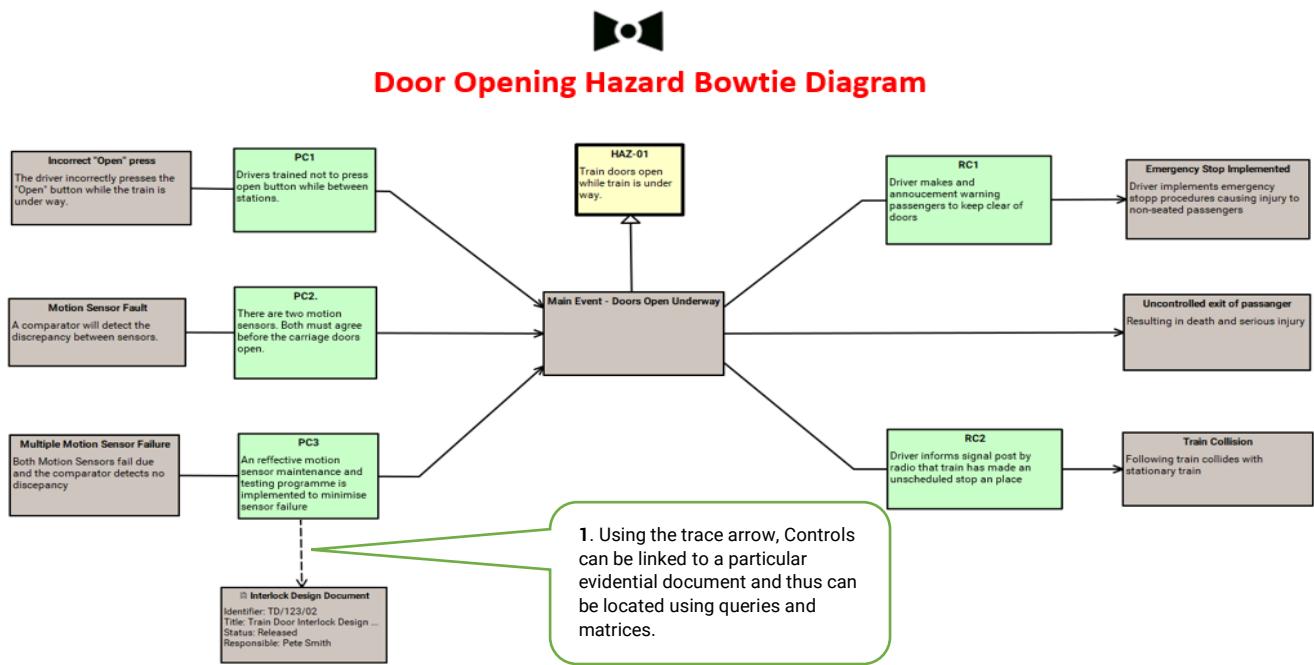


Figure 73: Linking to Evidence

Generating the Output

Once you have added all the controls and are happy with the Bowtie diagram you can generate a report which includes the diagram and produce a matrix showing the Bowtie relationships in tabular form.

To capture the output of a Bowtie Analysis you need to find which controls or barriers have been placed on the threat lines to prevent the source from happening or to recover once the event has happened. This is done using queries to find the information, matrices to group the information and reports to publish the information.

Building the Queries

Queries are the heart of the Matrix output and dictate which entities are searched for to deliver a comprehensive breakdown of the Bowtie process. As always, the diagram shows us the way with the hazard as the key entity. From the hazard we can find the accident (top event), the related threats & consequences and the controls that have been assigned. The first query – Finding the Hazard is shown below:

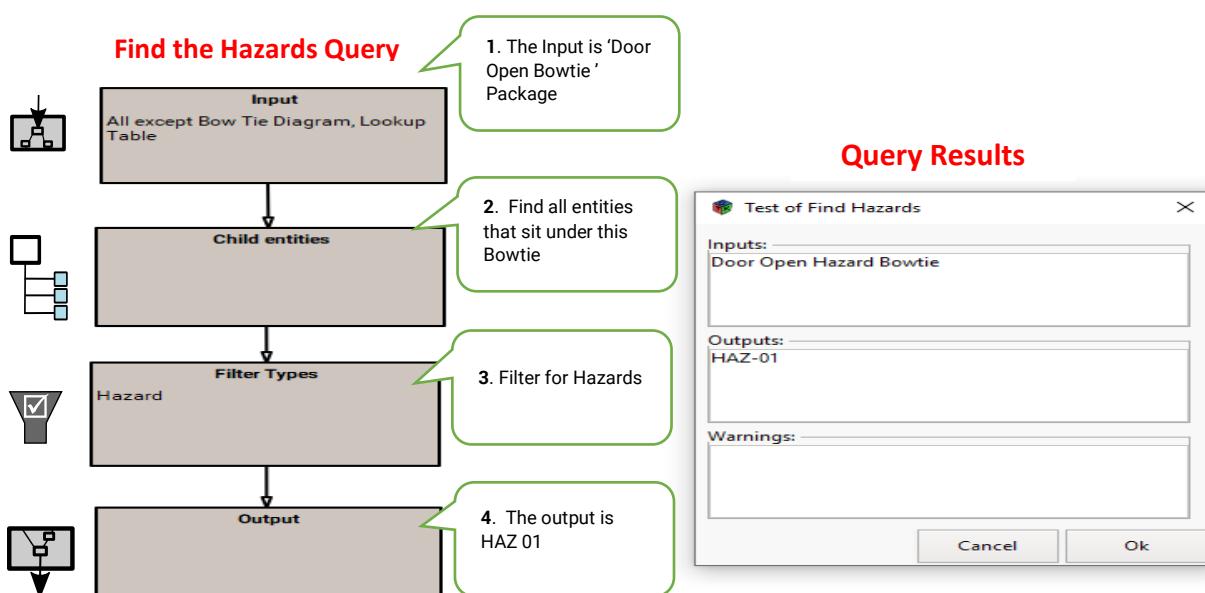


Figure 74: Finding the Hazards Query

To find the controls assigned to the Hazard, follow the diagram back from the Hazard to the top event and then step down onto the threat lines and again step down into the Threat Line Reference field 'Threat Control'. When the controls were dragged onto the Threat Lines, this relationship was automatically created.

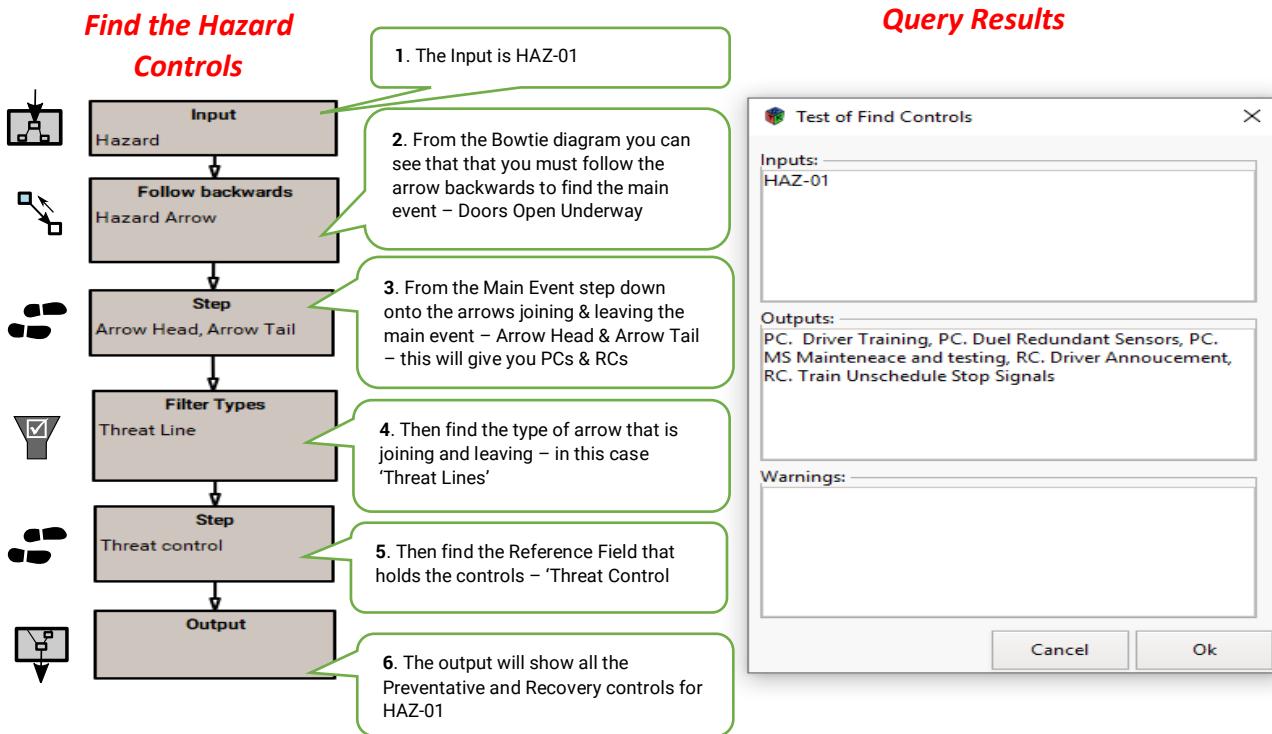


Figure 75: Finding the Controls Query

Building the Matrix

As with all matrices, you need to identify the starting query which will give you the columns you require. In this case it is the Hazard – always refer to the diagram – and you can select which fields you want to display in the Hazard Entity. To incorporate the controls, add a second query (to the right, not below the Hazard query) and add any fields you wish to show from the 'Control' entity. The matrix is now built and by selecting 'Run Matrix' from the Model tree matrix symbol you can generate the matrix for review and amendment (See diagram below). You can then publish the matrix to store in your file and version control system.

Matrix Design

Matrix name: Hazard Analysis Matrix

Description:

Matrix contents

- ▼ Find Hazards sorted by Name
 - Hazard: Field Name
 - Hazard Id: Field Hazard Id
 - Description: Field Description
 - Project/System: Field Project/System
 - Date Created: Field Date Created
 - Severity: Field Severity
 - Controls: Query Find

1. What is this Matrix called?

2. Matrices run off Queries – in this case the Query 'Find Hazards'

3. What fields from the HAZ-01 do I want to show? In this case the column heading will be 'Hazard' and this column will contain all the Hazards my query finds – using a field called 'Name'

4. The next field I want to show is the 'Hazard Id' so click on the green plus sign. I call this second Column heading 'Hazard Id' and select that field from the drop-down box

5. The next field I want to show is 'Description' so I click the green plus sign etc, etc

6. I don't have a reference field called 'Controls' but I can use my 'Find Controls' query to do the same thing

7. I simply click on the 'Query' tab, click in the Query window and select the query from the list

Matrix contents

- ▼ Find Hazards sorted by Name
 - Hazard: Field Name
 - Hazard Id: Field Hazard Id
 - Description: Field Description
 - Project/System: Field Project/System
 - Date Created: Field Date Created
 - Severity: Field Severity
 - Controls: Query Find Controls

8. I call this column 'Controls'

9. The Matrix is now built and you can run it to see the result

Figure 76: Building a Bowtie Matrix

Matrix Output

The inbuilt queries will automatically pick any new hazards and control and add them to the list, providing they are within your Bowtie Package, as shown on the right-hand side in the diagram above.

Matrix Output						
Hazard	Hazard Id	Description	Project/System	Date Created	Severity	Controls
HAZ-01	14567	Train doors open while train is under way.	Train Door Upgrade	24/4/2019	2	PC1, PC2., PC3, RC1, RC2

Figure 77: Bowtie Matrix

The Matrix above is just one configuration of a Bowtie and it is easy to add additional columns (such as date and responsible Person) or the order in which they appear.

Failure Mode & Effects Analysis (FMEA)

The FMEA objective is to determine the effect on system reliability from component failures, but the technique can be extended to determine the effect on safety. FMEA methodology is designed to identify potential failure modes for process, assess the risk associated with these failure modes and prioritize issues for corrective action and identify and carry out corrective actions to address the most serious concerns.

In the DSM, you can add the required FMEA fields to the entities to produce a structured FMEA worksheet that can be quickly adjusted and formatted to meet the differing needs of the organisation. It is recognised that there are many FMEA formats and all can be built in the DSM but only one example is detailed below.

FMEA Diagram

In the DSM the FMEA worksheet will be produced using a Matrix. However, to fully understand the interactions between the FMEA entities it is better to use the Bowtie

diagram editor which has been specifically designed to show the relationships between the FMEA elements.

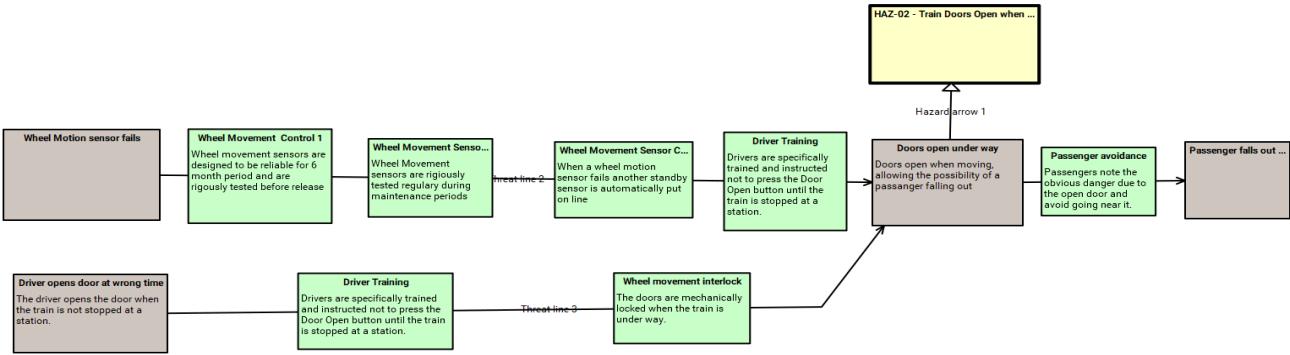


Figure 78: An example of an FMEA Diagram

The entities in the DSM are aligned with the entities required in an FMEA and the relationships are easily seen in the diagram above.

Aligning the FMES with DSM Entities

The required information groups are added to the DSM entities through field extensions (see Section 4.2 - Creating Extension Fields)

- Item, Function, failure mode, Severity, responsible person, and recommended actions are all fields in the Hazard entity.
- Causes and effects of failure are fields in the Bowtie Event Entity
- Controls are added using the DSM 'Control' entity and can be assigned to a 'Threat line' between the Potential causes of a failure and the potential effects of a failure

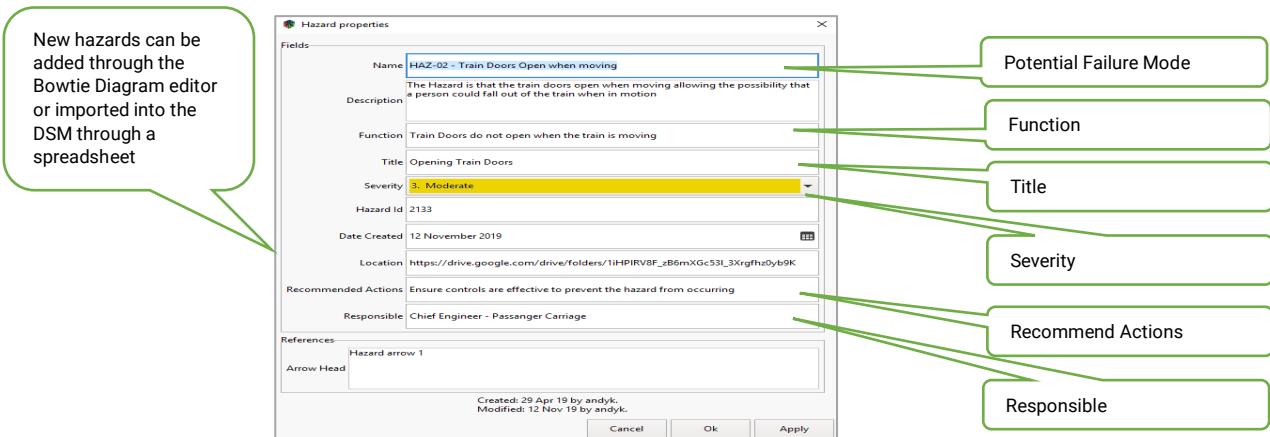


Figure 79: Aligning DSM Entities with FMEA Fields(1)

Event Properties

Fields

Name	Wheel Motion sensor fails
Description	The Wheel motion sensor fails and the train door opens when the train is moving
Responsible	Chief Engineer
Recommended Actions	Design High reliability of Wheel Motion sensor
References	
Threats	

Created: 02 Sep 19 by andyk.
Modified: 12 Nov 19 by andyk.

Cancel Ok Apply

Event Properties

Fields

Name	Doors open under way
Description	Doors open when moving, allowing the possibility of a passenger falling out
Responsible	Chief Engineer
Recommended Actions	Install Door opening Alarm when train in motion
References	
Threats	

Created: 02 Sep 19 by andyk.
Modified: 12 Nov 19 by andyk.

Cancel Ok Apply

Figure 80: Aligning DSM Entities with FMEA Fields (2)

Control properties

Fields

Name	Wheel Movement Control 1
Description	Wheel movement sensors are designed to be reliable for 6 month period and are rigorously tested before release
Title	Design Control
Responsible	Chief Design Officer
Recommended Actions	Yearly Design Review
References	
Arrow Head	
Threat control	Threat line 1, Threat line 2

Created: 29 Apr 19 by andyk.
Modified: 12 Sep 19 by paul.

Cancel Ok Apply

Figure 81: Aligning DSM Entities with FMEA Fields (3)

The diagram in Figure xx shows where the Controls have been added to prevent the potential effects of failure happening (the main event in a Bowtie). The assignment of controls in the DSM is quite easy.

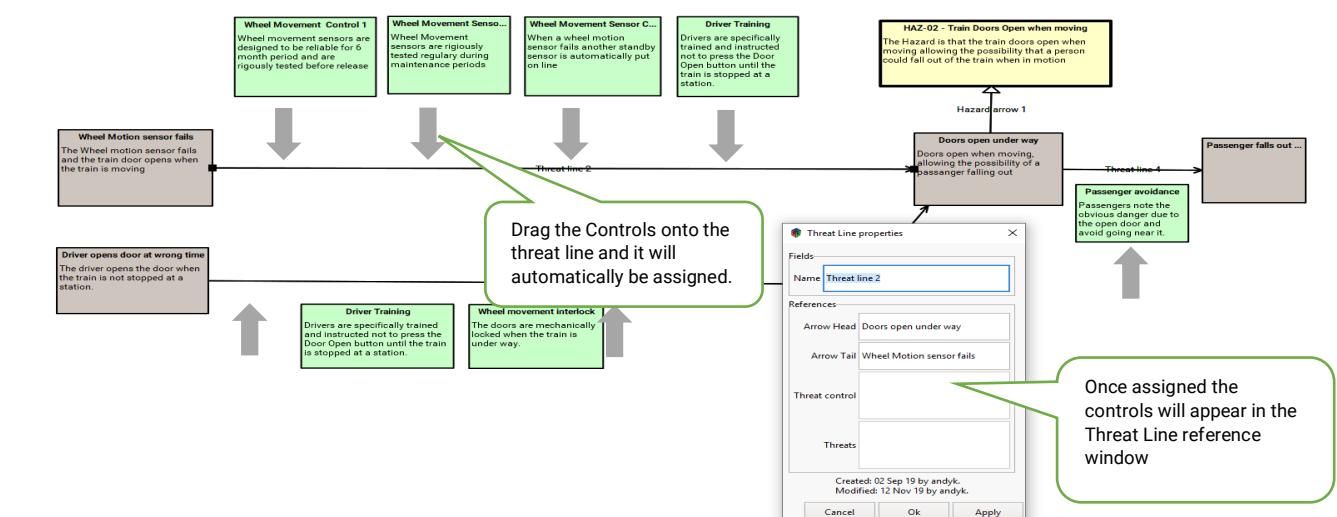


Figure 82: Assigning Controls to Threat Lines

The controls are dragged onto to the diagram from the Tree Model newly created and then dragged over the ‘threat line’ where they are automatically assigned to that threat line.

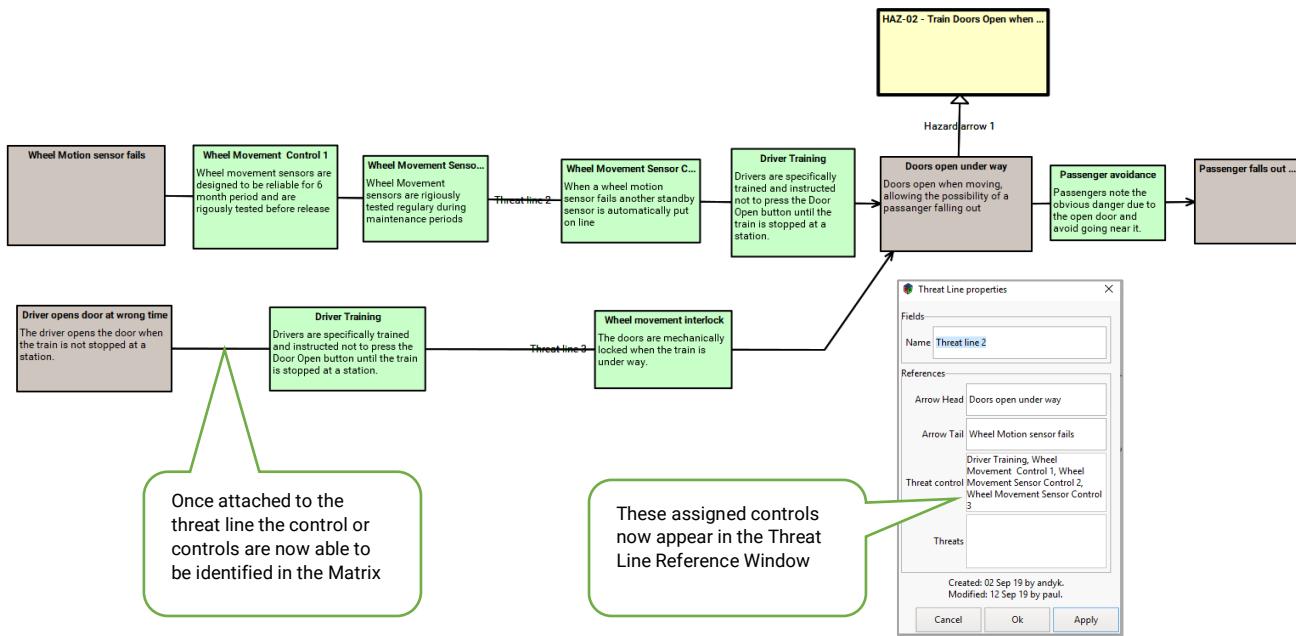


Figure 83: Assigned Controls in an FMEA Diagram

Building the FMEA Matrix

With the correct fields built and populated and the relationships created, the FMEA matrix can now be built that will deliver the FMEA worksheet. Once built, the FMEA Matrix can be applied to any FMEA package (multiple use) and be edited directly.

To build the FMEA Worksheet you need to produce queries that will provide you with the right results and use the fields of those results to build the other columns (See Building a Matrix).

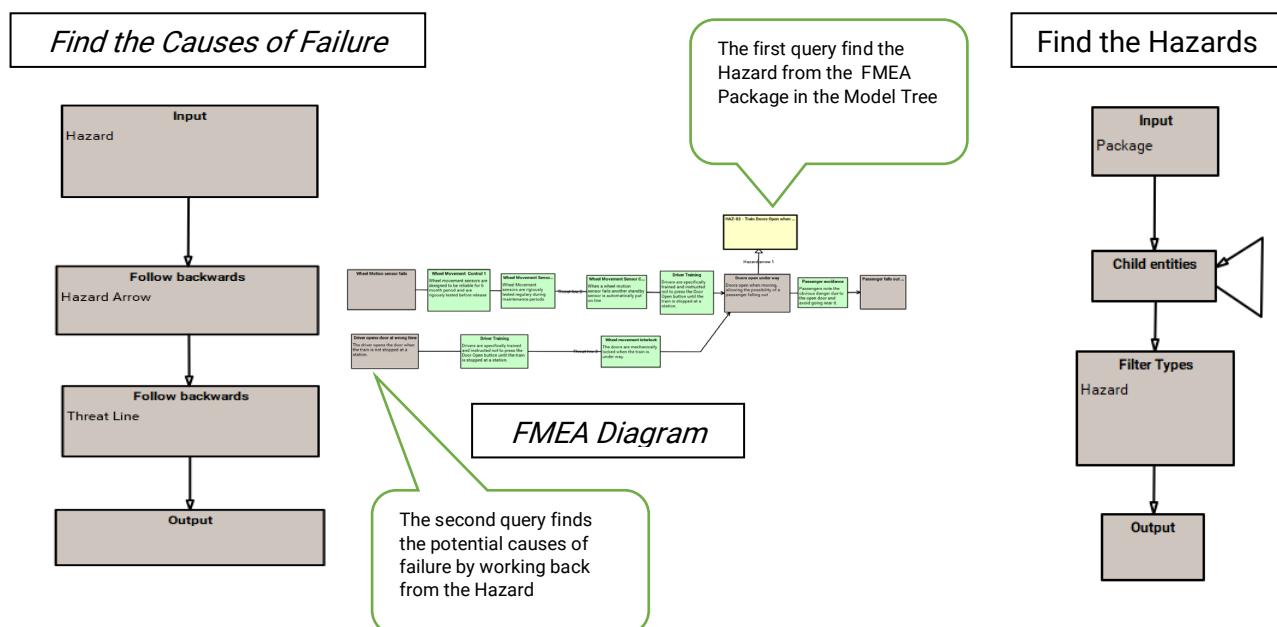


Figure 84: Queries for the FMEA Matrix

From the queries above, the Matrix can now be built and run. It can be applied to any FMEA format and will pick up new information when you run it each time.

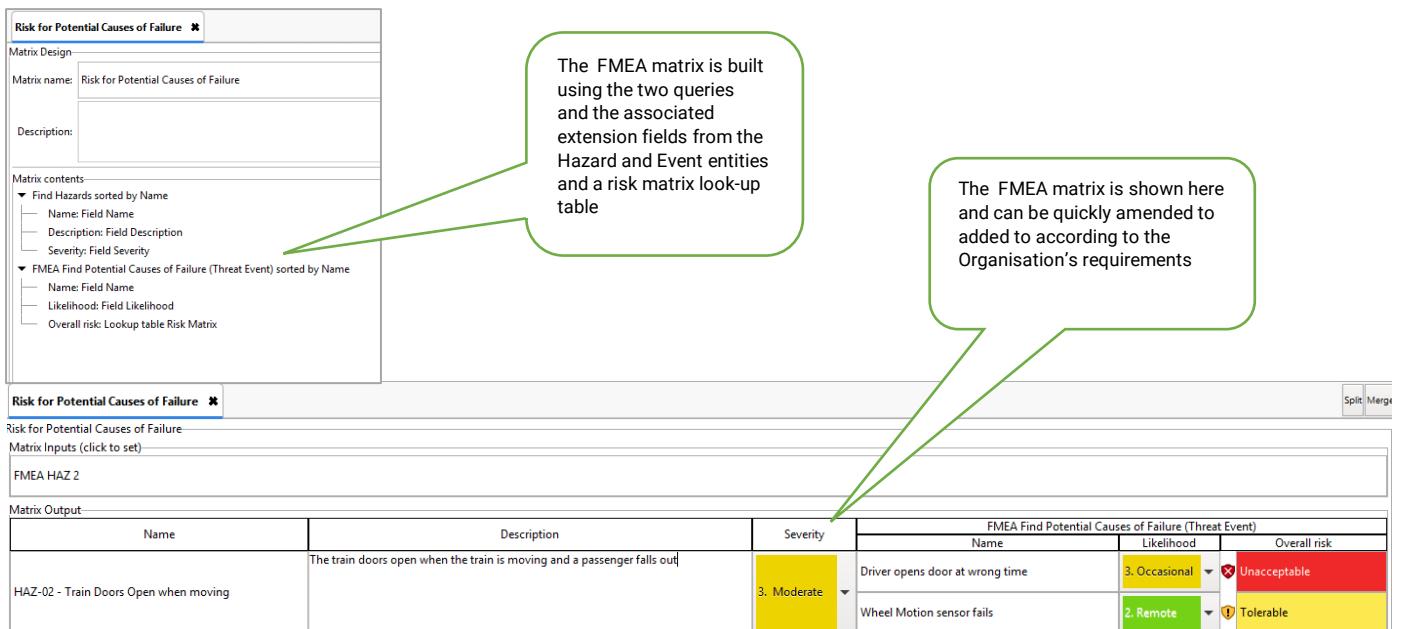


Figure 85: FMEA Matrix

Hazard and Operability (HAZOP) Analysis

The fundamental difference between FMEA and HAZOP is HAZOP uses guide words to stimulate the participants to identify system abnormalities, whereas FMEA uses known equipment failure modes.

HAZOP analysis is a technique for identifying and analysing Hazards and operational concerns of a system. It is a very organized and structured and methodical process for carrying out a hazard identification analysis.

As with the FMEA, the DSM can be used to conduct and capture a HAZOP by building the required Matrix. Focused on an event entity (Item) and an associated Hazard entity, a HAZOP work sheet can be quickly produced and applied during the HAZOP process.

Building HAZOP Relationships

The Hazard can be linked to several items by building the relationships in the diagram editor as shown below:

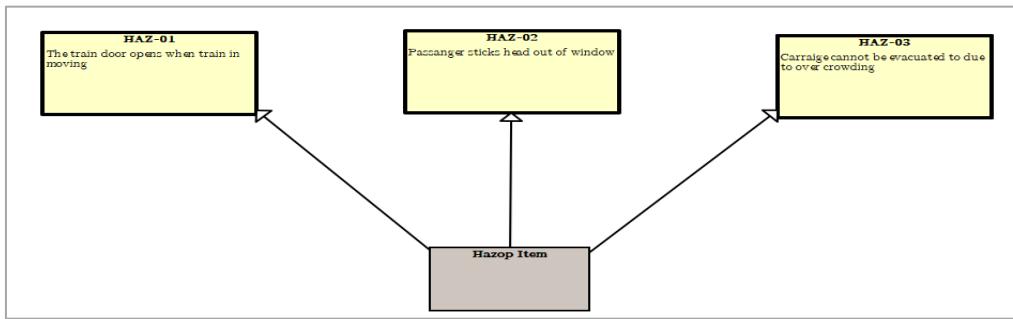


Figure 86: HAZOP Diagram

As with the FMEA, entities and fields of entities provide the columns for the HAZOP and the Matrix will capture new and amended items when it is run.

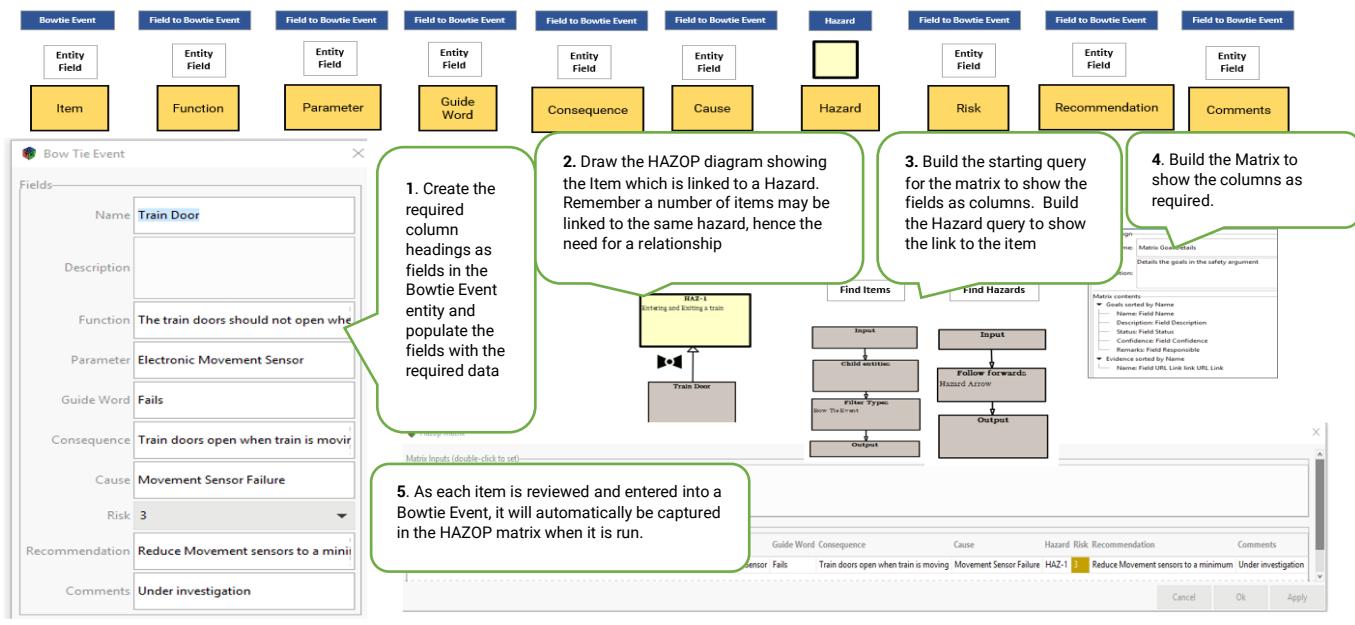


Figure 87: Capturing the HAZOP in the DSM

HAZARD Logs

A Hazard Log is a continually updated record of the hazards, accident sequences and accidents associated within a system. It includes information documenting risk management for each hazard and accident. It is a structured means of storing and referencing Safety Risk Evaluations and other information relating to an equipment or system and it is the primary means of tracking the status of all identified hazards, the decisions made and actions undertaken to reduce risks. The hazards, accident sequences and accidents recorded are those which could occur, as well as those which have already occurred. The information stored covers accidents, controls, risk evaluation and ALARP justification, as well as any data on Hazards.

In the DSM, as with FMEA and Bowtie, Hazards and controls are standalone entities but accident sources (Threats), accidents themselves (top events) and accident consequences are depicted as Bowtie events. The DSM Hazard Log is a configurable

Matrix, built from queries and data fields to provide a tabular display for Hazards and their related accident sequences and accidents themselves.

Using Bowtie

Using our Bowtie diagram, we can quickly build up a picture of the columns required and identify the queries that will deliver them to the matrix.

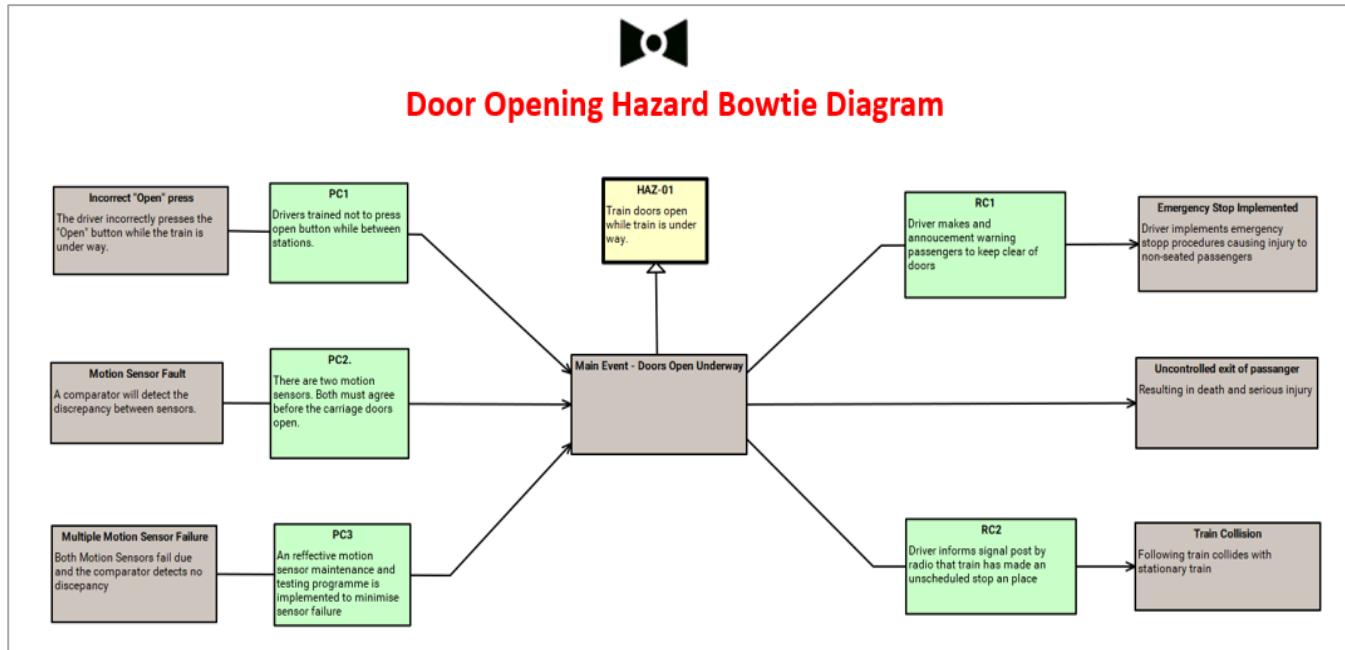


Figure 88: Building a Hazard Log using the Bowtie Diagram

Hazard Log Queries

In this version of the Model (remember that the DSM stores its models in files so you could have a number of Hazard logs with different Criteria) the Hazard Entity has a number of extended fields to meet the organisation's hazard information requirement.

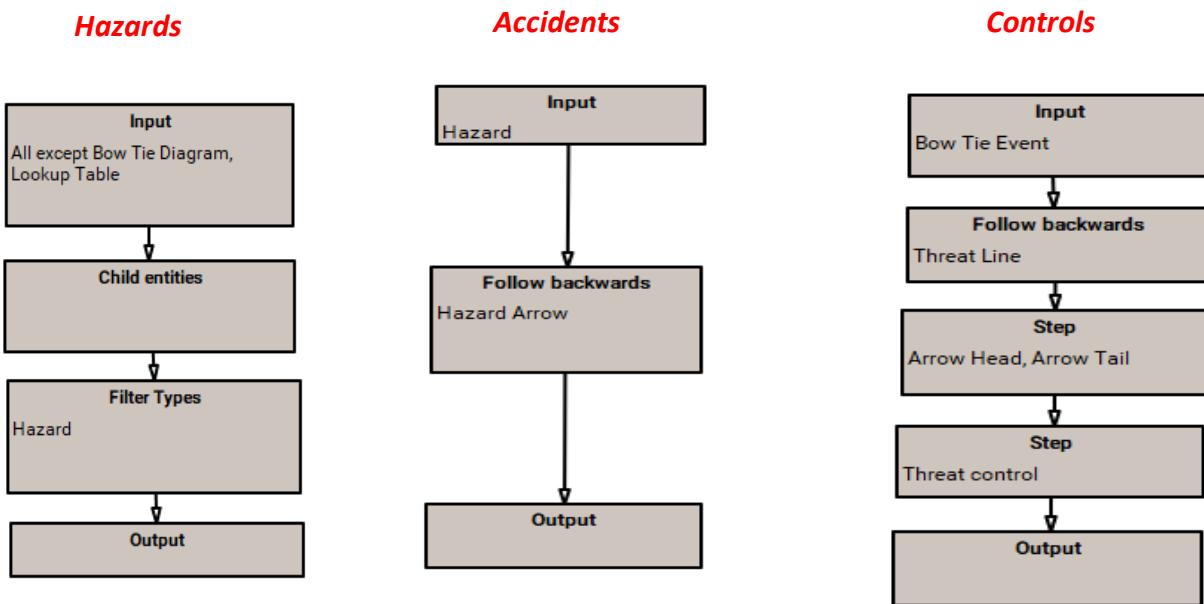


Figure 89: Hazard Log Queries

In the Hazard Log the first requirement is to identify all the Hazards and a simple query will do this. So using the Bowtie diagram, we can see that our first query is the same one we used for the Bowtie output. To find the accidents we need a query that would work back from the Hazard to the accident (main event). We then need a query that will find the controls (See Figure 82).

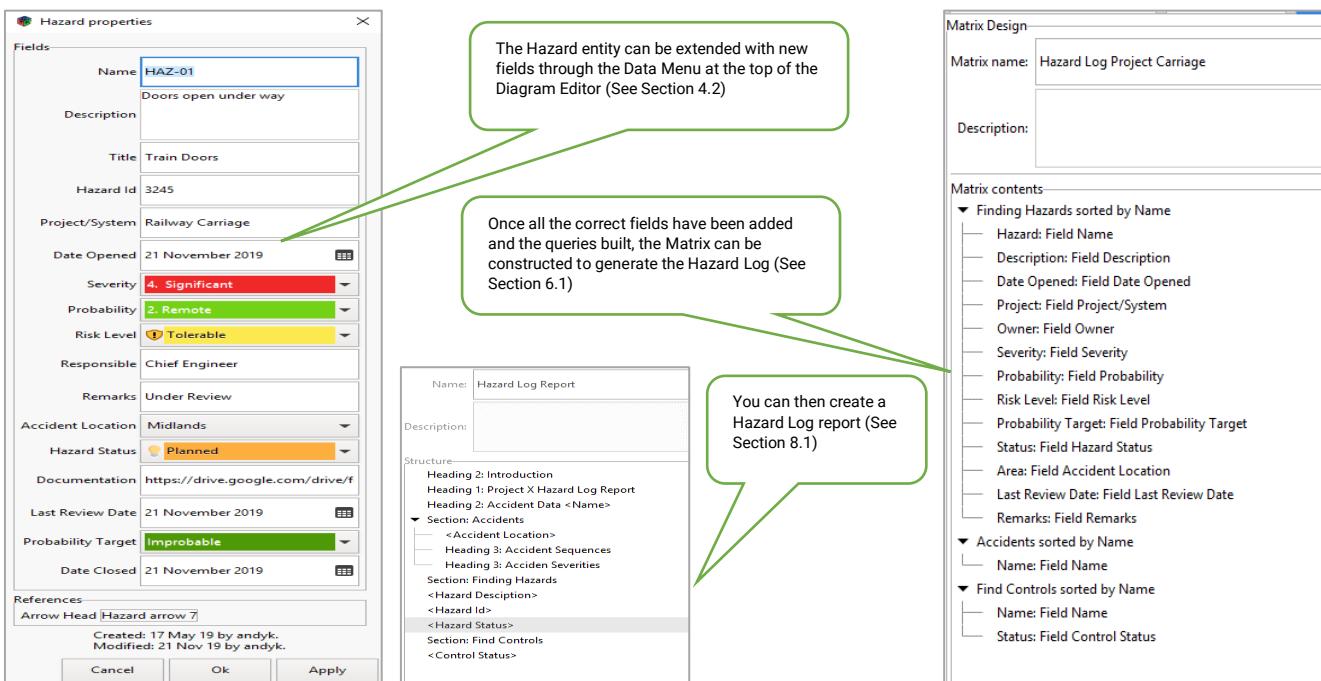


Figure 90: Hazard Log Construction

Hazard Log Matrix

You can also add a Risk Matrix using a lookup table and the Hazard Log will look like the example below. In the next version of the software, Hazard Log Matrices can be

amended directly through clicking into the right column and making any changes. You will also be able to filter columns by value.

Project X - Hazard Log																
Matrix Output																
Hazard	Description	Date Opened	Project	Owner	Severity	Probability	Risk Level	Probability Target	Status	Area	Last Review Date	Remarks	Accidents	Find Controls		
													Name	Name	Status	
HAZ-01	Doors open under way	21 November 2019	Railway Carriage		4. Significant	2. Remote	Tolerable	Improbable	Planned	Midlands	21 November 2019	Under Review	Main Event - Doors open	Driver Training	In Place	▼
														Dual Redundant Sensors	In Place	▼
														Maintenance & Testing	In Place	▼
HAZ-02	Passenger sticks head out of window	21 November 2019	Railway Carriage		4. Significant	2. Remote	Unacceptable	Improbable	Planned	Midlands	11 September 2019	Ongoing	Main Event - Passenger	Restrict Window Size	Under Consideration	▼
														Windows dont Open	In Place	▼

Figure 91: Hazard Log Matrix Extract

Modular Safety Cases

Large and complex safety cases are easier to manage when they are broken down into sub-system safety cases or modules. This helps in the identification and isolation of areas where the change applies and also allows the development of the safety case by different teams.

Creating a Template

To do this using the DSM, it is necessary to produce a template file that contains the correct data field formats required by the safety case manager. For example hazards will need to have the same data fields whether in the high-level safety case or in the sub-system safety case. So in the Modular Safety Case Template, the user can add or adjust the data fields sitting behind Hazards and other entities (See Chapter 4.2 Creating Extension Fields). Standardized queries, matrices, report structures and look-up tables(Risk etc) can also be added to the template.

Exporting and Importing sub-system Safety Cases

Once this has been achieved, this template can then be cloned and renamed. This will ensure that the entities in the file to be exported as a sub-system safety case will have their own Globally Unique Identifiers (GUIDs) and will not over write main safety case information when imported back into the safety case.

There may be several sub-system safety cases that will need to be exported and the template will need to be cloned each time.

saved under a new name (any number of times) to create a standardised DSM structure for assignment to sub-system safety case teams.

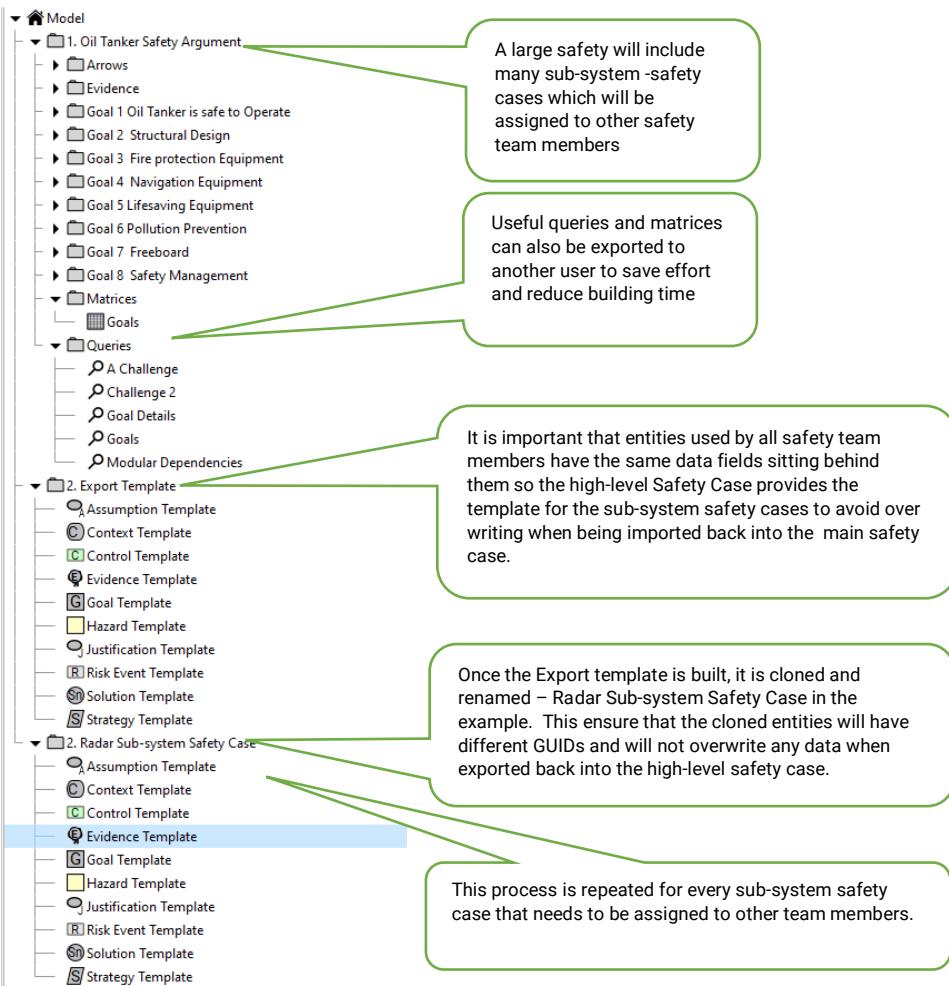


Figure 92: Modular Safety Cases

Creating standardised templates allows different safety case files to be imported into the high-level safety case without any overwriting issues (eg: one Hazard entity overwriting another hazard entity with different data fields). It ensures uniformity across the different safety cases and allows the reuse of queries, matrices, reports and look up tables. Deleting old sub-system safety cases from a package and importing the new version provides a clear update without any hidden conflicts. The next version of the DSM will be able to analyse updated versions and import only these items that have changed.

Annex A

A1 - Further Details on Formulae

Formulae are very powerful functions that can be used in Fields, Queries and Matrices. They work very much like Excel formulae except that they use property names instead of cell references.

A2 - Types of Value

Type	Function
Boolean	"Yes" or "No".
Text	Any length, possibly including multiple paragraphs.
Integer	Whole numbers of any size
Real	Numbers including fractions
Date	A calendar date (does not include the time).
No-value	Special type representing the absence of a value

A3 - DSM Formula Operators:

=	Equal to
<>	Not equal to
>	Greater than
<	Less than
>=	Greater than or equal to
<=	Less than or equal to
& (ampersand)	Joins two or more text strings in a single string
, (comma)	Used to separate arguments in functions.
+ (plus)	Addition
- (minus)	Subtraction or negation (changes the sign of the value)
* (asterisk)	Multiplication
/ (forward slash)	Division
^ (caret)	Exponential (power of)
[] (square brackets)	Used for field names that contain spaces.
! (exclamation)	Logical negation (i.e "Yes" becomes "No" and vice versa)
No-value	Special type representing the absence of a value

A4 - Handling No-values

Formulae can be applied to entities with different sets of extension values, so it is possible for a formula to refer to an extension value that doesn't exist in the current entity. In this case the formula will not find anything in the field, and will treat this as a "no value".

Rather than just giving an error the "no-value" gets handled as follows:

- Formulae that include a no-value will return a no-value. So if “Score” is a no-value then the formula (score+1) will also be a no-value.
- Text formulae that include a no-value will treat it as being an empty string. If a text value is expected then a value of any other type is converted into its text representation.

A5 - Functions

All function names are capitalised without spaces (i.e. in “CamelCase”). The function name is followed by a list of arguments in brackets. There can be spaces between the function name and the left bracket.

If a no-value is given as a function argument then the result is a no-value.

A6 - Characters

Number of characters in the string.

Formula	Result	Type
Characters (“foo. !54<>”)	10	Integer
Characters (23)	2	Integer

A7 - Words

Number of words in the string. Anything that isn’t a space is treated as part of a word. Tabs and new lines are treated as spaces.

Formula	Result	Type
Words (“foo. !54<>”)	2	Integer

A8 - Strip

Removes any leading or trailing spaces.

Formula	Result	Type
Strip (“ foo. ”)	“foo.”	Text

A9 - Find

Returns the start index of the first argument within the second, counting from zero.

Formula	Result	Type
Find (“foo”, “The foo thing has foos!”)	4	Integer
Find (“foo”, “This has none.”)	-1	Integer

A10 - Mid

Takes characters from the middle of the text. Negative numbers count from the end.

Formula	Result	Type
Mid (“This is some text.”, 5, 7)	“is some”	Text
Mid (“This is some text.”, 0, 4)	“This”	Text
Mid (“This is some text.”, -10, 4)	“some”	Text
Mid (“This is some text.”, 5, -1)	“”	Text

A11 - Left

Takes characters from the start of the text.

Formula	Result	Type
Left ("This is some text.", 4)	"This"	Text
Left ("This is some text.", -1)	""	Text

A12 - Right

Takes characters from the end of the text.

Formula	Result	Type
Right ("This is some text.", 4)	"ext."	Text
Right ("This is some text.", -1)	""	Text

A13 - LeftWords, MidWords, RightWords

Takes words from the middle of the text. As with the "Words" function anything that isn't a space is considered to be part of a word. All the words taken are returned separated by single spaces regardless of how they were separated before.

Formula	Result	Type
LeftWords ("This is some text.", 2)	"This is"	Text
MidWords ("This is some text.", 1, 2)	"is some"	Text
MidWords ("This is some text.", -2, 2)	"some text."	Text
RightWords ("This is some text.", 2)	"some text."	Text

A14 - If

Returns either the second or third arguments depending on whether the first is "Yes" or "No".

If the first argument is a non-value then the result is a non-value. If the first argument is something other than a Boolean then an error will be reported.

Formula	Result	Type
If (2 < 4, "Yes value", "No value")	"Yes value"	Text
If (4 < 2, "Yes it is", 78)	78	Integer

A15 - Round

Converts a Real number into an Integer, rounding to the nearest whole number.

Formula	Result	Type
Round (3.14159)	3	Integer
Round (-3.7)	-4	Integer

A16 - Upper, Lower

Converts a string into upper or lower case.

Formula	Result	Type
Upper ("This is text.")	"THIS IS TEXT."	Text
Lower ("This is text.")	"this is text."	Text

A17 - Day, Month, Year

These functions return the day of the month, the month number and the year number from a date.

Formula	Result	Type
Day ('5 February 2019')	5	Integer
Month ('5 February 2019')	2	Integer
Year ('5 February 2019')	2019	Integer

A18 - Weekday

Returns the day of the week as a number. Monday = 1, Sunday = 7.

Formula	Result	Type
Weekday ('5 February 2019')	2	Integer

A19 - DayName, MonthName

These functions return the name of the day and month as text.

Formula	Result	Type
DayName ('5 February 2019')	"Tuesday"	Text
MonthName ('5 February 2019')	"February"	Text

A20 - Today

Returns the current date. This is unlike all other functions because (a) it takes no arguments and (b) the result changes from one day to the next. Even though it takes no arguments the brackets are still necessary; without them the DSM will look for an extension value called "Today".

Formula	Typical Result	Type
Today ()	'5 Feb 2019'	Date

A21 - Lookup

Applies a lookup table to the current row in a matrix or the current entity in a query filter. The argument in brackets is the name of the lookup table. If the table is in a package then put the package names in as well, separated by "/" characters (like a file name in Windows).

The result of the Lookup function depends on the model, so this is just an example of the typical use.

Formula	Result	Type
Lookup ("Risk Register/Tables/Risk Acceptability")	Review	Text