ELECTRONIC SAFETY CASES

Introduction

There is a requirement to explore ways of developing and presenting Nuclear Power Plant (*NPP*) safety cases more efficiently if targeted cost savings are to be met. The capabilities of current safety case tools and methods are being challenged by many factors, including the complexity of modern NPPs, regulatory requirements and advances in industry guidance, including fault and hazard studies. Many of these challenges relate to the ability to access, link, and update the information that forms the basis of the safety case.

The use of an electronic safety case is not new as they have been implemented in the nuclear and other high-hazard industries with varying degrees of success. Modern safety cases are largely presented electronically in the form of technical reports and supporting evidence. The main challenge with the modern safety case is managing the complexity of the NPP design and presenting the safety case in a clear, concise and auditable format. These aims can be readily achieved using a suitably structured electronic safety case, which can be presented in a more logical and transparent format than traditional reports.

The purpose of this task is to provide a summary of the available tools and consider some best practices and potential pitfalls associated with the implementation of an electronic NPP safety case.

Presentation of the Safety Case

Safety cases can be presented as standard reports, structured reports or diagrammatically. While it is acknowledged that there is no single best practice approach to safety case production, it is generally accepted that the safety case should be presented in some form of Claims, Arguments and Evidence (*CAE*). Modern safety cases have moved away from the standard report approach to improve the visibility and accessibility of safety claims and supporting evidence. The CAE format can be presented in a structured report format or diagrammatically, or a combination of both.

Available Tools and Packages

There are a variety of software tools available that can be used to help produce electronic safety case documentation. These range from simple database packages for structure and control of information to programs which have been specifically designed for producing and managing safety case documentation.

The following sections consider the merits of a small number of tools available to support safety case development. Electronic tools considered include the following:

- DOORS.
- Adelard Assurance and Safety Case Environment (*ASCE*).
- Microsoft Access.
- Modelling Based System Engineering (*MBSE*).

DOORS

DOORS database software can be used to structure and manage a safety case. The database consists of a number of modules containing the raw safety case data including, but not limited to, the following:

- **Hazards Module**: The Hazards Module is the central module of the database and provides a complete listing of all initiating events identified during the relevant Hazard Identification (*HAZID*) exercises.
- **SFR Module**: The Safety Functional Requirements (*SFRs*) module provides a complete list of Safety Functions (*SFs*), Demand Safety Functional Requirements (*DSFRs*) and Specific Safety Functional Requirements (*SSFRs*).
- **SSC Module**: This module identifies all Systems, Structures and Components (*SSCs*) claimed within the safety case as providing a contribution toward maintaining nuclear safety. The SSC Module identifies the performance requirements necessary to satisfy the related SFRs, and provides links to the engineering substantiation.
- **Consequence Module**: This module tabulates the various radiological and non-radiological consequences and is used to assign Design Basis Analysis (*DBA*) parameters, and sentence initiating events to the fault schedule, environmental risk assessment, conventional risk assessment etc.
- **Reference Module**: This module contains a definitive list of reference documentation (evidence) including all HAZID documents. Entries in the Hazards Module are manually linked to the source reference in the Reference Module; this ensures traceability back to the source document and consistency of referencing throughout the database. Links to qualification evidence supporting the SFRs and SSCs is managed in the same way.

In addition to the above modules, a number of pre-defined views can be developed to manipulate the data and automatically generate a number of safety case sections including fault schedules, engineering schedules, and SFR and SSC listings.

If managed correctly DOORS can be used to enable the audit trail to be easily followed, from initial requirements capture and hazard identification through the fault schedules to the SFRs and SSCs and the supporting evidence. DOORS enables good access to information and configuration control to be exercised over the data. DOORS can also include self-checking functionality to identify broken, incorrect or missing links.

Challenges include identifying the dataset and links correctly in the first instance and generating the DXL code to make the automated parts of the database function. The appropriate access permissions to provide sufficient checking and approval functionality must be set up correctly to allow for the day-to-day development of the case.

DOORS OPEX

DOORS has recently been used in the production of modern standards safety cases for major new build projects. For two such projects the decision was made to use the DOORS database software to structure and manage the safety case.

The main difficulty encountered was the structuring the database correctly in the first instance, which required some trial and error, and generating the DXL code to make the automated parts of the database function. There were also problems defining the appropriate access permissions to provide sufficient checking and approval functionality while still allowing the day-to-day development of the case.

Adelard ASCE

Adelard ASCE software has been specifically designed for the development and management of safety cases in a CAE or Goal Structuring Notation (*GSN*) format. The intention of the software is to clarify the links between the claims or goals and the supporting arguments or evidence, making the safety cases more accessible and easier to review and manage.

Some of the claimed benefits include:

- Reduction in acceptance risks.
- Better communication of safety controls.
- Improved navigation of the safety case.
- Clear links to safety management system documentation.
- Simpler identification of the impact of changes in evidence.
- Clear management of claims and arguments.

Adelard ASCE is not currently used extensively in the nuclear sector although it is understood that other industries, such as the aviation industry, have applied it successfully.

Adelard ASCE OPEX

There is recent experience in the use of Adelard from the Generic Design Assessment (*GDA*) process, where two prospective licensees initially attempted to use it to structure their Office for Nuclear Regulation (*ONR*) Safety Assessment Principles (*SAP*) compliance with limited success.

While Adelard ASCE is clearly a useful tool for managing and accessing safety cases it does not in itself improve the content, and skill is required to identify the complete set of claims, arguments and evidence. Successful implementation appears very reliant on the user’s ability to use the software. It also relies on others, such as the designers, reviewers, verifiers and regulators, all having access to and being sufficiently familiar with the software to interrogate it and adequately interpret the output.

Microsoft Access

Microsoft Access is part of the Microsoft Office Suite, and is a relational database that is made up of 7 major components.

- Tables.
- Relationships.
- Queries.

- Forms.
- Reports.
- Macros.
- Modules.

Access can be used as the main database or as a front-end program for other back-end databases / tables. Users can create tables, queries, forms and reports and link them together with macros. Advanced users can use Visual Basic for Applications (*VBA*) to determine data manipulation and user controls.

Microsoft Access OPEX

Microsoft Access was used to develop a new licensee's application for a Radioactive Substances Regulation (*RSR*) environmental permit. The RSR permissioning effectively required the licensee to demonstrate that they applied Best Available Technique (*BAT*) to the generation, treatment, storage, discharge and disposal of radiological waste throughout the project lifecycle from cradle to grave. A decision was made early in the development process to adopt a CAE type structure to the demonstration of compliance with the RSR permit conditions. The Microsoft Access database package was selected to manage and control the environmental case.

The RSR permit conditions were used as the basis for the claims within the environmental case, with minor modifications to the wording made where necessary.

The Access-based CAE approach has allowed a clear link to be made between the permit requirements, the claims, and the arguments and evidence that demonstrate compliance. It has also helped to make the CAE case more accessible.

While the claims and arguments are controlled within the Access database, almost all evidence is stored externally in reference documents that are managed by the normal documentation control process. The potential for changes to be made to the reference documents so undermining the claims and arguments in the dataset has been identified, however, this issue is not specific to the CAE / database application and should be adequately mitigated by the existing document and modification control processes.

The database is considered to be a tool rather than a record, and can be used to easily generate a variety of user-specified reports. User access rights are used to control who is able to modify the data, and the intention is to perform regular back-ups so that changes can be rolled back if necessary or the database can be recovered should there be a problem.

Model-Based Systems Engineering (MBSE)

MBSE is defined by the International Council on Systems Engineering (*INCOSE*) as: '*The formalised application of modelling to support system requirements, design, analysis, verification, and validation activities from concept to decommissioning*'. An MBSE approach models, or uses models, to facilitate the system engineering activities which are traditionally performed using a document-based approach. The primary aims of taking an MBSE approach are generally to increase engineering design quality and design process efficiency. MBSE can achieve these in a number of ways, but primarily they are achieved by the following:

- **Providing Context**: Providing a clear narrative (from top to bottom) of where the system of interest sits within the whole system and its purpose.
- **Providing Clarity**: Use of unambiguous language to describe system design and behaviours (at different and appropriate levels for the given party through the development of specific views and viewpoints) supports clarity of design and early detection of defects.
- **Facilitating Efficient Information Exchange**: Providing a central source of information with up to date and fully traceable design / requirement / management information.

In the context of safety case development, the model would tightly link together a system's requirements, its physical system design and the functions the system is performing with the hazards they are designed to control and mitigate. This can be applied at a whole power plant level or to individual subsystems. Modelling in this way supports the scalability of safety cases as their size and complexity grows.

The output of an MBSE-based safety case would be a coherent 'systems model' which ties together whole system information. Systems Modelling Language (*SysML*) is commonly used to develop these models. This is a general purpose graphical modelling language for Systems Engineering applications. The language can be extended to support structured argument notation such as CAE and GSN, enabling close integration between design and functional models with the safety case.

MBSE OPEX

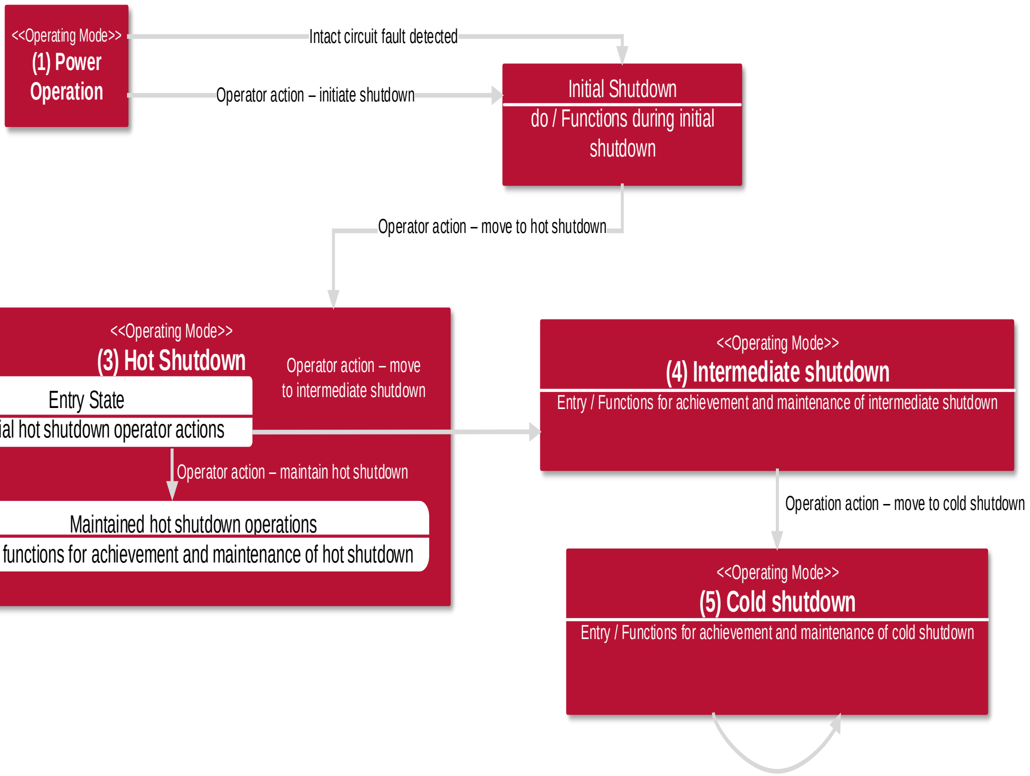
The use of MBSE tools and methods is becoming increasingly common across a range of industries, notably the aerospace and defence sectors. However, to date its application is relatively untested in practice within the nuclear sector, particularly in relation to safety case development.

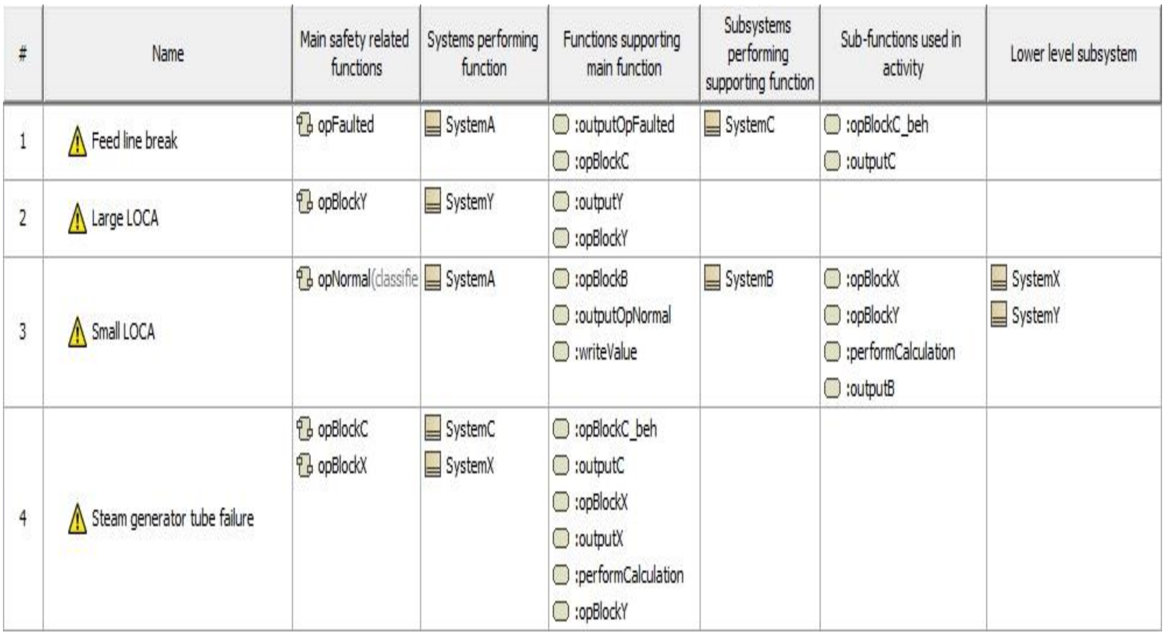
Certain tools and techniques have been successfully used for civil nuclear software design and implementation. For example, many nuclear programs have used model-based development environments such as ANSYS SCADE within modernisation projects, including those in France, Belgium, the Czech Republic and Armenia, and applications include: Reactor Protection Systems, Nuclear Instrumentation & Control Systems, Human System Interface, Other Safety Systems (e.g. safety valve control system, backup diesel auxiliary power engines system).

The application of MBSE is also being explored for the design of Fusion Power Plant by the UK Atomic Energy Authority (*UKAEA*) and Culham Centre for Fusion Energy. Examples of this are provided from the Euratom research and training programme, where MBSE and SysML modelling has been applied to the design of the DEMOnstration power plant (*DEMO*) which will be the successor to the International Thermonuclear Experimental Reactor (*ITER*). This research project has focussed on the role MBSE can play in the development of safe nuclear systems and has demonstrated how:

- The adoption of a formal ontology can support consistent representation of a safety case across different technical engineering areas.
- Safety functional hierarchy can be represented within an MBSE format.
- Plant states and operating modes can be modelled and tied back to system functions and the physical architecture.

- The developed nuclear power plant model can support the automatic generation of ‘systems-based’ views, ‘fault-based’ views and fault schedules.


<<Operating Mode>>
(1) Power Operation
Intact circuit fault detected
Operator action – initiate shutdown
Initial Shutdown
do / Functions during initial shutdown
Operator action – move to hot shutdown
<<Operating Mode>>
(3) Hot Shutdown
Entry State
do / Initial hot shutdown operator actions
Operator action – maintain hot shutdown
Maintained hot shutdown operations
do / functions for achievement and maintenance of hot shutdown
Operator action – move to intermediate shutdown
<<Operating Mode>>
(4) Intermediate shutdown
Entry / Functions for achievement and maintenance of intermediate shutdown
Operation action – move to cold shutdown
<<Operating Mode>>
(5) Cold shutdown
Entry / Functions for achievement and maintenance of cold shutdown



#	Name	Main safety related functions	Systems performing function	Functions supporting main function	Subsystems performing supporting function	Sub-functions used in activity	Lower level subsystem
1	⚠ Feed line break	opFaulted	SystemA	:outputOpFaulted :opBlockC	SystemC	:opBlockC_beh :outputC	
2	⚠ Large LOCA	opBlockY	SystemY	:outputY :opBlockY			
3	⚠ Small LOCA	opNormal(classifie	SystemA	:opBlockB :outputOpNormal :writeValue	SystemB	:opBlockX :opBlockY :performCalculation :outputB	SystemX SystemY
4	⚠ Steam generator tube failure	opBlockC opBlockX	SystemC SystemX	:opBlockC_beh :outputC :opBlockX :outputX :performCalculation :opBlockY			

Additional Information & Guidance

- http://www.onr.org.uk/resources.htm