Writing 'usable' Nuclear Power Plant (NPP) Safety Cases using Bowtie methodology

Fidel Ilizástigui Pérez, Principal Consultant & Ilieva Ilizástigui Arissó, Consultant, Todus Advisors

Historically, the majority of Nuclear Power Plants (NPP) Safety Cases have been produced and implemented under highly prescriptive regulatory regimes, with emphasis placed on demonstrations of the robustness of the facility's design basis against a set of deterministic criteria and technical standards and rules set by the Regulatory Body. This has resulted in Safety Cases that are technically sound, but at the same time too complex and therefore, not easily accessible to and used by persons responsible for ensuring safe operations; i.e. operations and maintenance staff who are in direct control of the plant as well as managers who are accountable for safety – the key end-users.

Shortcomings regarding the 'usability' of the Safety Cases are not new and have been the subject of discussion in recent years. They are deeply rooted in the way these documents are produced and implemented. It means that in order to overcome these difficulties attention should be focused primarily on the Safety Case process, affording it the same importance that is given to the final product – the documented Safety Case. This paper explores the advantages that incorporation of the Bowtie risk management methodology into the Safety Case (production) strategy can bring to the delivery of a fit-for-purpose, accessible and usable Safety Case, supporting current efforts undertaken by the nuclear industry to ensure 'Right First Time Safety Cases'.

The paper also suggests how to conduct Bowtie workshops - in the authors' opinion - the most important part of the Bowtie building process – to secure the necessary input from people who have most knowledge and experience about the facility and its current operational status during the Bowtie building process. This will have a direct effect on the usability of the resultant product during plant operation.

A fault schedule for a generic Advanced Boiling Water Reactor (ABWR) has been taken as an example to highlight the claimed advantages. It reflects how the use of fault schedules to draft Bowtie diagrams within a workshop setting can make the safety case process a true 'aid' to thinking and deliver a final product that is accessible and easy-to-understand by key end-users, while using it during plant operation.

Key words: Nuclear Safety Cases, Safety Case process, Bowtie

Introduction

Historically, the majority of Nuclear Power Plants (NPP) Safety Cases have been produced and implemented under highly prescriptive regulatory regimes, with emphasis placed on demonstrations of the robustness of the facility's design basis against a set of deterministic criteria and technical standards and rules set by the Regulatory Body. This has resulted in Safety Cases that are technically sound but often too complex and complicated documents, not easily accessible to and therefore not used by those charged with ensuring safe operations, including operations and maintenance staff and managers who are accountable for safety – the key end-users.

Nuclear Power Plant Safety Cases are indeed among the more complex of all major hazard industry sectors. The UK Nuclear Safety Case Forum guidance "Right First Time Safety Cases: How to write a usable Safety Case" made the following statement in relation to Nuclear Safety Cases: …*notoriously long, complicated, overly technical and difficult to follow with some licensees feeling that they are producing Safety Cases for the regulator, not for themselves, and yet frequently fail to satisfy the regulator, being accused of producing Safety Cases that do not 'tell the story' and Safety Cases where the 'claims, argument, evidence trail goes cold*…".

Safety Case shortcomings are not new and have persisted over the years in the history of Safety Case production. They have had significant implications in terms of accessibility and understanding of these documents by key end-users, all of which have severely restricted use as an effective tool to support informed decision-making in relation to the management of nuclear safety risks during plant operation leaving them 'gathering dust on a shelf'.

Perhaps, the best definition of what is happening regarding safety case production was given by Haddon Cave QC in the Nimrod Review:

"The Safety case regime has lost its way. It has led to a culture of 'paper safety' at the expense of real safety"

Today, it is widely recognized that the above shortcomings are indicative of underlying problems in the manner in which Safety cases are produced and not the result of an invalid concept. They are therefore deeply rooted in the safety case production process itself. Thus, it becomes clear that in order to eliminate the root causes of these shortcomings and not just treat the symptoms, the safety case process must be accorded equal importance alongside the final product – the documented Safety Case.

The Safety Case (production) process

The importance of having a robust safety case production process in place before undertaking the production of safety case deliverables should not be understated. ONR has developed a 'Right First Time Safety Case (RFTSC)' concept to put more focus on the whole process within Licensees Organizations for producing safety cases, rather than the technical content or methodologies for safety case production. It has been benchmarked against the lessons from the Nimrod Review and encompasses the key types of weaknesses in a Safety Case process highlighted in that review.

The importance of the safety case process has been clearly established by ONR in the Safety Assessment Principles (SAP SC.1, SC.2 and SC.5) and further developed in ONR guide "The purpose, scope and content of safety cases" NS-TAST-GD-051 Revision 4.

.."The process for producing safety cases should take into account the needs of those who will use the safety case to ensure safe operations. It is essential that the safety case documentation is clear and logically structured so that the information is easily accessible to those who need to use it (see paragraph 87). This includes designers, operations and maintenance staff, technical personnel and managers who are accountable for safety…"[2]

.."The safety case is a key element to enable safe management of the facility or activity in question. It is important to those who interact directly with the facility, for example the operators who control the conditions within the facility and those who maintain the facility. It is also important to senior management who are responsible and accountable for safety. They rely upon the safety case for accurate and objective information on risks and control measures to make informed decisions that may affect safety. Therefore, the key users of the safety case should be involved in its development, production/review and implementation..".

Apart from RFTSC, other models have been created and adopted in an attempt to overcome safety case shortcomings by addressing weaknesses of the safety case process itself (for example, OUCH, SCOAP, SHAPED and PSHAPED) just to name the most relevant ones. They all highlight desirable qualities of both the safety case and the safety case production process that are critical to the delivery of a fit-for-purpose and usable safety case.

In relation to Nuclear Safety Cases, the UK Safety Case Forum Guide: How to write a Usable Safety Case establishes the following 6 principles that 'Usable' Safety Cases should be based on (as recommended by Haddon Cave QC in the Nimrod Review) with the incorporation of an additional principle of 'Preparation' to emphasize the importance of having a sound safety case production process in place with clear definition of responsibilities, resources, scope and purpose and strategy for the production of a safety case. PSHAPED is understood as follows: <u>P</u>reparation, <u>S</u>uccinct, <u>H</u>ome-grown, <u>A</u>ccessible, <u>P</u>roportionate, <u>E</u>asy-to-use and <u>D</u>ocument-lite.

Aspects regarding the robustness of the Safety Case production process as well as cultural aspects surrounding the Safety Case process associated with, for example, both compliance and complacency attitudes, confirmation bias, etc. during the production of the safety case are of paramount importance to ensure a good quality Safety Case but are beyond the scope of this paper.

Use of Bowtie to increase safety case usability

The Bowtie methodology is a state-of-the-art, barrier-based, qualitative risk management tool that has gained popularity in the last 10 years or so as an effective tool to manage major hazard risks. Since it is based on the "barrier model" of defense, it is thus fully compatible with the 'defense in depth' approach – the cornerstone of nuclear safety. Bowtie methodology offers unique strengths that may lessen many of the shortcomings associated with the production of 'usable' safety cases. Some of them are summarized in Table 2 against the desirable SHAPED qualities of the Safety Cases:

Table 3.1 Bowtie strengths against desirable SHAPED qualities of the Safety Case

Area	Process Weaknesses	Bowtie strengths
Home-grown	• Routine outsourcing to external consultants • Lack of vital Operator support • Tick-box exercise • Failing to highlight and concentrate on principal hazards • Archeological exercise of design and compliance documentation	• A 'true' aid to thinking • A highly interactive workshop-based tool • A barrier management tool
Usability	• Too long and bureaucratic length with unnecessary detail • Obscure, inaccessible and difficult to understand language (by key end-users) • Not living documents	• Increases visibility and communication: 'A picture paints a thousand words' • A 'living' document

Essentials of the Bowtie methodology

Perhaps the easiest way to fully appreciate the advantages that this methodology can bring to the usability of a Nuclear Power Plant Safety Case is through studying an example of its application to a generic Advanced Boiling Water Reactor (ABWR). Firstly, some explanations are provided regarding the standard terms and Bowtie element definitions used in the Bowtie methodology. Fig 1. shows a Bowtie diagram with Bowtie elements. Table 1 provides definitions of each of them. It is important to note here that the existence of multiple levels of defense in depth (several physical barriers, each with dedicated levels of protection) adds complexity to the Bowtie but can be successfully managed to keep the diagram as simple as possible. In the same fashion, barrier rule definition that is being suggested to ensure consistency of the methodology, comprising detect, decide and act barrier elements some technical measures have been grouped into a single barrier when applied to Nuclear Power Plant design.

From fault schedule to Bowtie diagram

A fault schedule is regarded by ONR as an important document which summarizes key aspects of a nuclear plant's Safety Case by linking of: Initiating Faults, Fault Sequences and Safety Measures resulting from the Design Basis Analysis (DBA), thus showing the adequacy of the system. It 'tells the story' of how hazards are controlled by making links between safety and engineering substantiation. ONR provides the following definition of "Fault schedule" (Safety Assessment Principles):

"A fault schedule (sometimes known as a safety schedule or a fault protection schedule) should be provided to links faults, fault sequences and safety measures (see principle FA.8). For each initiating fault or event, the schedule should identify the relevant initiating fault frequencies, the potential fault consequences, the safety systems and administrative safety measures that provide protection, any beneficial safety-related systems, the mitigated fault sequence frequency and the overall protection claim. The fault schedule should also identify any passive safety measures claimed to prevent faults or mitigate their consequences".

The following demonstrations should be summarized in a fault schedule (SAP, FA.8). Most fault schedules share some common features:

- The faults considered within the safety case are systematically and comprehensively identified
- The initiating event frequencies attributable to identified faults are indicated
- The major safety functions (e.g. control of reactivity, fuel cooling and containment/confinement functions)
- The SSCs claimed in the safety case as being available and effective to deliver the necessary safety functions following a fault , along with their safety classification, are identified

Fig. 2 shows a Bowtie diagram that may well be the outcome of a Bowtie workshop carried out by a Licensee based on the information contained in the fault schedule with input sought from people who have most knowledge and experience about the facility and its current operational status. The Bowtie depicts a medium Loss of Coolant Accident (LOCA) design basis accident scenario, associated with the high pressure core flooder (HPCF) system line break. This accident is regarded as a bounding fault for all LOCA-type scenarios within the primary containment.

In the Bowtie diagram, the *Hazard* has been defined as *ABWR Reactor Normal Operation* or more comprehensively: *Nuclear fuel cladding is cooled during normal operation*. The *Top Event* (i.e. the moment when the control over the hazard is lost – the release of the hazard) may be defined as the *Loss of reactor coolant resulting from a guillotine break in the HPCF system line*. The Top event has the potential to cause damage to the fuel cladding containing the nuclear fuel as explained below.

The right hand side of the Bowtie depicts the fault sequences leading to each of the consequences arising from the HPCF system line break. Consequences can be related to the loss of each of the Fundamental Safety Functions (FSFs), i.e. those that mitigate the fault progression. FSFs are shown in red boxes in the right hand side of the Bowtie and described in Table 2 below:

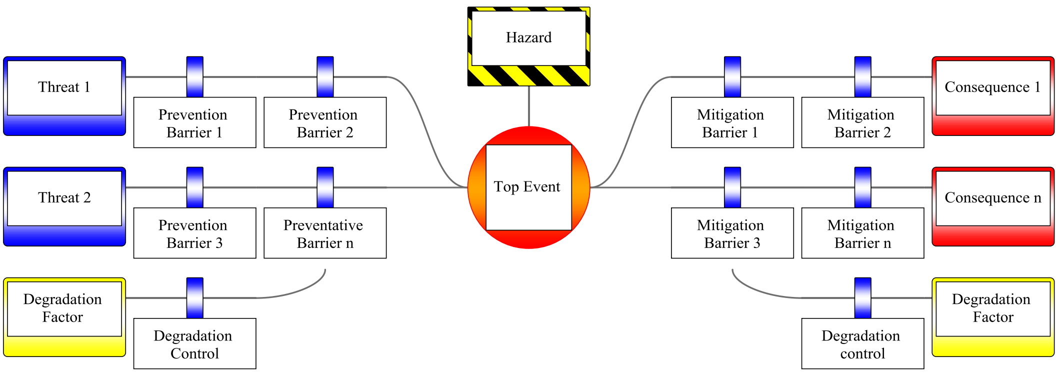


Fig 1. Standards terms for Bowtie diagram

Table 1. Bowtie elements definition

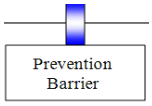
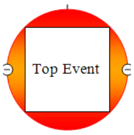
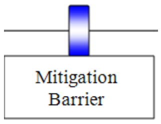
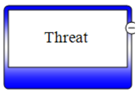
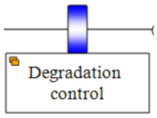
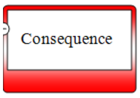
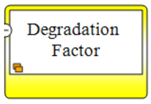
Bowtie element	Symbol	Definition	Bowtie element	Symbol	Definition
Hazard		Something with the potential to cause harm if the control is lost	Prevention Barrier		Barrier that eliminates the Threat or prevents the Top event
Top Event		A deviation from the desired state or activity – the 'release' of the hazard	Mitigation Barrier		Barrier that avoids or mitigates the consequences
Threat		Credible causes for the Top Event	Degradation Factor		Factors that reduce the effectiveness of the barrier – 'failure modes'
Consequence		Hazardous outcomes arising from the Top event	Degradation Control		Control that reduce the effects of degradation

Table 2. Fundamental Safety Functions (FSFs) for ABWR and associated Consequences

FSFs	Consequences
Control of reactivity	▪ Reactor thermal power not reduced (insufficient core cooling capability). ▪ Fuel cladding design (temperature/oxidation) margins exceeded ▪ Potential for core damage (severe accident)
Fuel cooling	▪ Core becomes uncovered (insufficient core cooling capability) ▪ Fuel cladding design (temperature/oxidation) margins exceeded ▪ Potential for core damage (severe accident)
Long-term heat removal	▪ Heat is not removed from the containment ▪ Containment failure with complete loss of coolant ▪ Potential for core damage (severe accident)
Confinement/Containment	▪ Fission products released to the environment ▪ Potential for severe accident

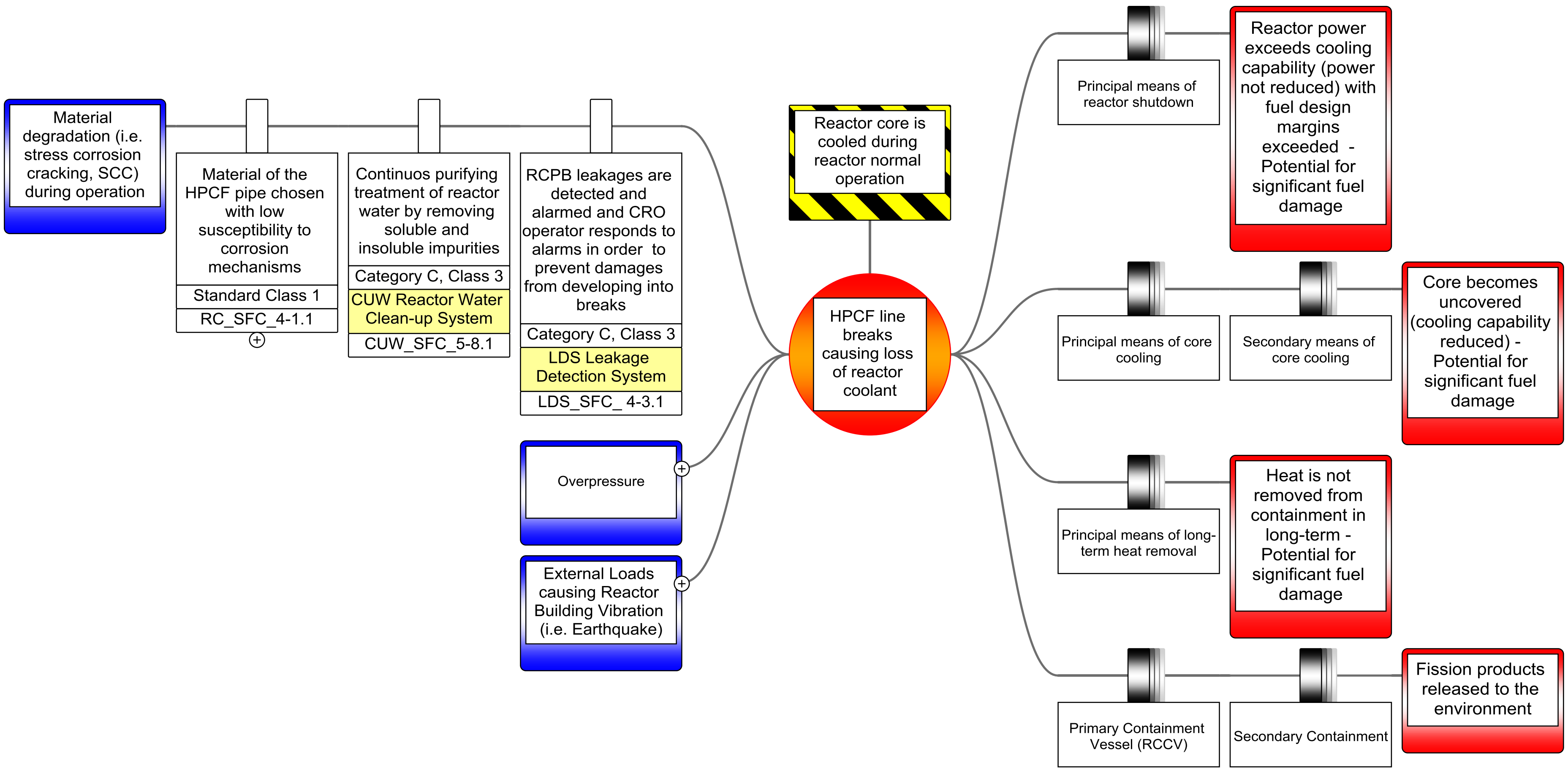


Fig. 2. Bowtie diagram for a Medium LOCA in a generic ABWR reactor, with left-hand side developed to show Prevention Barriers (Not all inclusive)

The left hand side of the Bowtie depicts the *Threats*, which represent a credible cause that can directly cause the Top Event, for instance: *Material degradation (i.e. stress corrosion cracking during operation), Overpressure and external loads causing Reactor Building Vibration (i.e. earthquake)*.

Prevention barriers, both hardware and/or human (placed between the *Threats* and the *Top Event*) which are in place to eliminate the *Threats* entirely or prevent the *Threats* from causing the *Top Event* are systematically identified. For the Threat: *Material degradation during operation*. *Prevention Barriers are:*

- Material of the HPCF pipe chosen with low susceptibility to corrosion mechanisms
- Continuous purifying treatment of reactor water by removing soluble and insoluble impurities
- Control Room Operator (CRO) responds to Reactor Coolant Pressure Boundary (RCPB) leakage alarms to prevent larger leaks
- CRO responds to sampling and monitoring (SAM) alarms as per Reactor Chemistry Limits and Conditions (LCO) by taking corrective actions.

Mitigation barriers, both hardware and human barriers (placed between the *Top Event* and the *Consequences*) which are in place to reduce the likelihood of the *Consequence* or mitigate its severity, are systematically identified. For instance, for the *Consequence Core becomes uncovered with potential for core damage. Mitigation barriers* are*:*

Primary means of core cooling (grouped in the first box and marked yellow):

- Low RPV water reactor level/high dry well pressure signal is detected (by Safety System and Logic Control, SSLC)
- Water injection to RPV starts on RPV low water level signal (by Reactor Core Isolation Cooling System, RCIC)
- RPV is depressurized to allow water injection to RPV in low pressure state with 30 sec. delay (by Automatic Depressurization System, ADS)
- Water is injected to RPV in low pressure state (by Low Pressure Core Flooder System, RHR-LPFL)

In addition, the Bowtie diagram also allows depicting secondary means of core cooling (grouped in the second box and marked yellow) to deal with Beyond Design Basis Accidents (BDBFs) with a complete loss of primary means of core cooling as a result of common Cause Failure (CCF). These are:

- Low RPV water reactor level/high dry well pressure signal is detected (by Hardwired Backup System, HWBS)
- RPV is depressurized to allow water injection to RPV in low pressure state (by Reactor Depressurization Control Facility, RDCF)
- Water is injected to RPV in low pressure state (by Flooder System of Specific Safety Facility, FSLL)

For each *Mitigation barrier* involved in core cooling, additional information is shown on the Bowtie diagram regarding the following:

High Level Safety Functions (HLSFs) and Safety Functional Claims (SFC)

FSFs are broken down into a set of High Level Safety Functions (HLSFs). The HLSFs define lower level safety functions which enable individual safety measures to be identified such that they contribute to the achievement of overarching FSFs. HLSFs are further decomposed into Safety Functional Claims (SFCs) specific to particular safety measure.

SFCs are uniquely identified using the HLSF and the system code. There is a direct relationship between the HLSFs and the SFCs and it is the SFCs that are used to link safety claims to an appropriate Structure, System or Component (SSC). The key point of SFCs is that all systems that either perform the safety function or provide support (power, cooling chain, Control and Instrumentation (C&I) etc.) use the same HLSF within the SFC code. This means that each SFC code is both unique but also self-referencing across engineering disciplines and can be readily traced back to the fault studies from where the requirements for SFCs are derived.

In the Bowtie diagram in Fig. 3, SFCs are shown for each of the frontline safety systems that are claimed in the fault schedule to fulfil specific high level safety functions (for example, SSLC_SFC_3-1.1, or RCIC_SFC_2-1.1).

Safety categorization and safety classification

One of the common problems with Safety cases encountered by ONR is the confusion between safety categorization - the process for determining the safety of significance of safety functions - and safety classification - the process of determining the level of engineering rigor applied to structures, systems and components. Fig. 4 shows the assigned the safety categorization of safety functions to be delivered within the facility, both during normal operation and in the event of medium size LOCA, based on their significance with regard to safety (SAP, ECS.1 – Safety Categorization). Also, the safety classification of the structures, systems and components that deliver safety functions is provided in the Bowtie diagram on the basis of those functions and their significance to safety (SAP, ECS.2 Safety Classification of structures, systems and components).

In addition, it is also possible in the Bowtie diagram to link barriers (safety measures) with any other relevant design information (for example, Safety Property Claims (SPCs), codes and standards, design documentation, etc.).

Linking fault schedule with safety management system

The importance of the safety management system (SMS) for ensuring safe plant operation has been long recognized by the nuclear industry and in this regard, the Safety Case should be considered the most important way to demonstrate that the safety is being properly managed and that management controls are appropriate and sufficient, i.e. it must also "tell the story" of how the Licensee manages the operational risks.

Here, the Bowtie methodology offers a unique strength that is not always exploited to its full potential – the possibility of visualizing the links between barriers (safety measures) and the management system. In practice, the Bowtie can establish strong links between the technical safety measures and the management system to show adequacy of the safety management system.

Each technical safety measure (safety or safety-related system) can be linked through the Bowtie diagram to specific persons/positions in the organization with accountability for ensuring the integrity of the system. A link can be established also between the technical safety measure with those in-service testing, inspection and other maintenance safety critical tasks (Examination, Maintenance, Inspection and Testing, EMIT) carried out by competent persons governed by procedures, which are required to ensure safety measures are working and remain effective at all times (*SAP, EMT.1 Identification of requirements*).

The right-hand side of the Bowtie in Fig. 3 shows the existing links between safety measures with accountable persons and EMIT activities. For example, the RCIC system is linked to the EMIT activity "System Functional Test, carried out by Maintenance Department". This shows that the safety management system supports safety systems by ensuring they remain 100% available when required to function.

This increases the awareness of the staff in relation to the importance of their roles in ensuring plant safety. Frontline operation and maintenance personnel can use Bowties to understand their roles in preventing nuclear accidents whilst managers can use them to understand what they and the organization need to put in place for barriers to function as intended.

Use Bowties to manage operational risk

With Bowties it is possible to visualize the actual conditions of the barriers by providing a colour code against the condition. Bowtie also allows actual performance of the barrier to be assessed by incorporating information provided by a wide range of different data sources on barrier performance, such as incident investigations, audits and maintenance systems.

This makes it possible for responsible persons to periodically review and update the existing Bowtie, thus assuring a near-real time tracking of barrier condition and a timely decision-making regarding the adoption of remedial actions depending on the actual condition of the barrier. All of this will help answer the following questions:

- Is it safe to continue operations?
- Are immediate mitigations required to continue operations?
- Which barrier or safeguards should be prioritised for rectification to regain their design intent?

LCO that guarantee the delivery of safety functions.

Maintenance of the required availability of safety systems in operation usually places constraints on, for example, which systems may undergo planned maintenance or testing during specific operational modes or what action must be taken in what timescale if a system is discovered to be in a failed or degraded state during testing.

In order to ensure that technical measures are operated within safety limits and that design requirements from the safety case are met during the operating regime, appropriate LCOs and surveillance requirements to ensure LCOs are met as well as corrective actions (measures) to follow when an LCO is not met are defined. LCO may be specified to ensure:

- The required availability of the systems that deliver safety functions (for example, 2 trains of system X must be operable in modes X and Y"), and

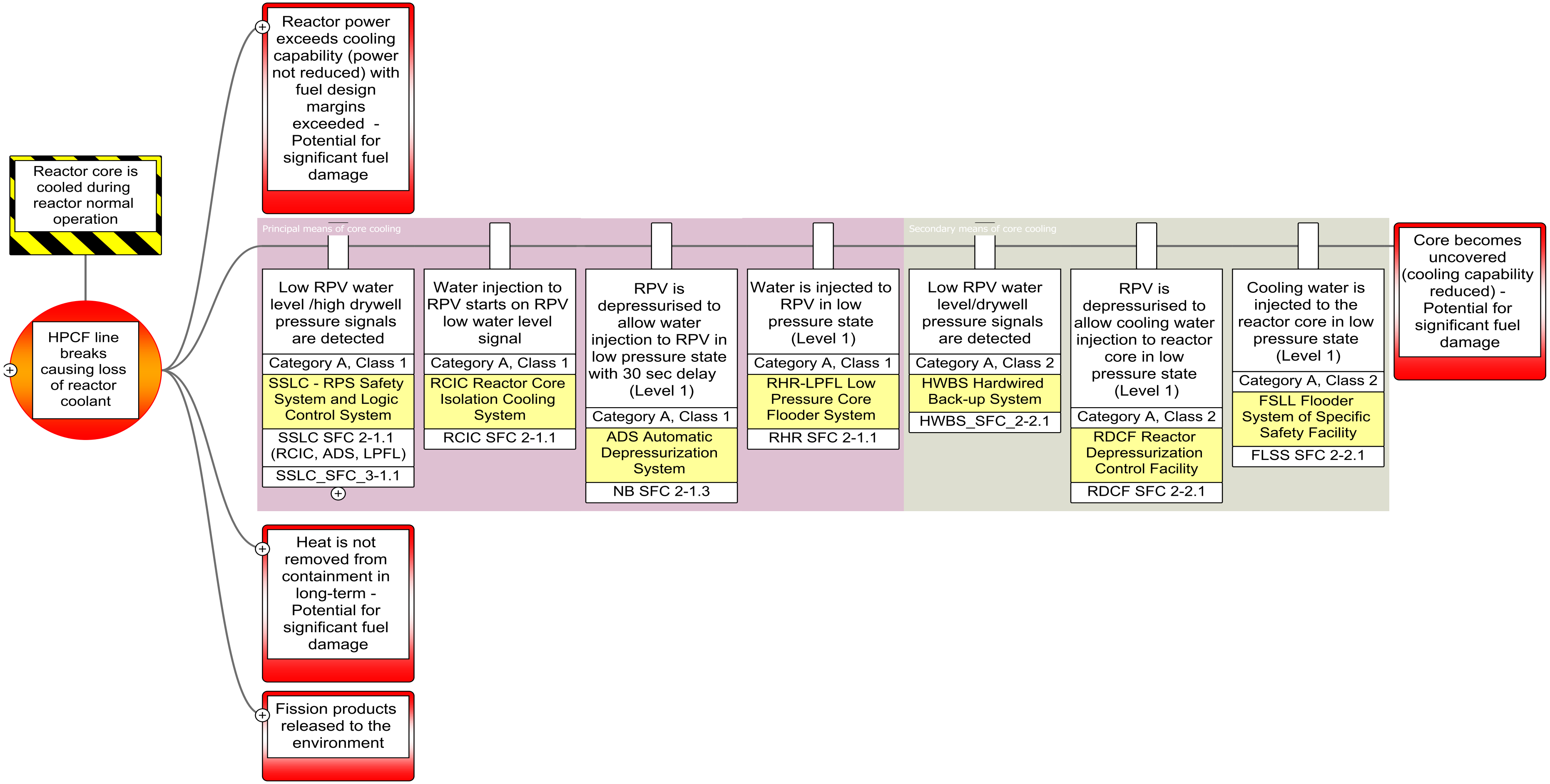


Fig. 3. Bowtie diagram for a Medium LOCA in a generic ABWR reactor with right hand side developed to show mitigation barriers for the Safety Function – Fuel Cooling (with both primary and secondary means) – Not all inclusive. It has been postulated that the RCIC is available and primary means of core cooling have failed even in the event of Infrequent Faults

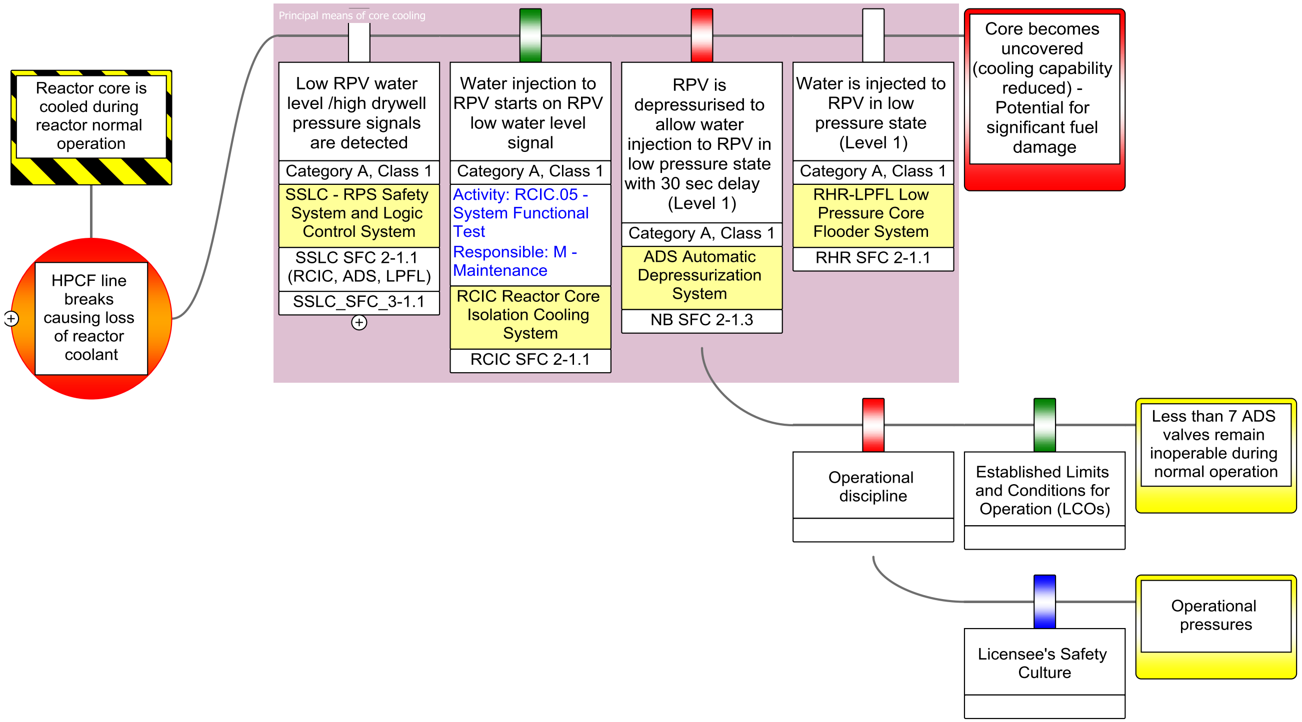


Fig. 4 Bowtie diagram for a Medium LOCA for a generic ABWR. Right hand side show links between technical safety systems with the management system through: Responsible persons (Technical Authorities); Examination, Maintenance, Inspection and Testing (EMIT) activities and Limits and Conditions for Operation (LCO), with assigned actual barrier condition

Table 3. Suggested barrier condition rating

Condition	Condition	Color Code
Effective	In place, available and effective	
Partially Effective	In placed and available, but operating below its intended functionality	
Not effective	Not in place, not available	
No data	No operational information is currently available	
Deactivated	Not in place, turned-off, deactivated	

- Minimum performance requirements for the systems that deliver safety functions, which must be confirmed by specified surveillance requirements to ensure that parameters that control the delivery of the safety function are within prescribed limits (for example, testing of system must ensure that flowrates are greater than X m^3/h)

If the corresponding systems are found to be outside the limits set by the LCO for any reason, the operators must restore the system to the defined operability within a prescribed timescale.

Fig. 4 shows the assessment of actual barrier condition of safety measures against the specified LCOs, as may be assessed during a Bowtie Workshop with responsible and knowledgeable persons using the colour code system shown in Table 3, where each colour represents a specific condition of the barrier. In this hypothetical example, the second mitigation barrier (RCIC) was hypothetically assessed against LCO which prescribes the required availability (functional requirements), whereas the condition of the third mitigation barriers (ADS) was assessed against the LCO which prescribes the minimum performance requirements. In this way, the barrier 'health' can be continuously measured and clearly shown in the Bowtie diagram.

The third ADS technical barrier is linked to a specific *Degradation Factor*, namely: *Less than 7 ADS valves remain inoperable during normal operation,* which can be understood as a specific failure more which reduces the effectiveness of the technical barrier. To prevent the *Degradation Factor* from occur, *Degradation Controls* are identified usually linked to deeper organizational aspects of safety. In this particular case, the existence of *Limits and Conditions for operation (LCO)* for the system in question and the *Operational discipline* that must be in place to ensure compliance with those LCOs. The effectiveness of these latter *Degradation Controls* can be further interrogated and corresponding *Degradation Factors* will arise in turn. For example, for the *Degradation Control* 'Operational Discipline', things like, *Operational pressures* may be a *Degradation Factor and Licensee's Safety Culture'* the corresponding *Degradation Control* (see Fig. 4).

Making the fault schedule, a 'living' document

With the advent of modern IT developments, Bowtie methodology has been incorporated as part of Electronic Safety Cases (ESCs), making it possible to easily review, update and monitor Safety Case information in an easy format (e.g. Electronic Safety Cases).

Conclusions

The bowtie methodology can significantly enhance the quality of Nuclear Power Plant (NPP) Safety Cases by making them 'usable' and 'fit-for-purpose' documents. It is not, of course a panacea or a silver bullet. It will not solve the many shortcomings associated with a lack of a robust safety case process in the first place. But the incorporation of the Bowtie into the safety case production strategy will bring the following advantages to Licensees;

- An increased understanding, visibility and accessibility of complex and highly technical documents to key end-users;
- Increased workforce involvement and ownership of the safety case process;
- Visible links between the barriers (e.g. safety systems) accounted for in the fault assessment with the management system arrangements which support them via safety critical tasks;
- Tracking barrier performance and monitoring barrier health in relation to adopted Limits and Conditions for Operations (LCOs)
- Better incorporation of human and organizational factors (HOFs)

As with other methodologies, it is important that the Bowtie building process is carried out with a 'questioning' attitude in order to challenge established practices and norms.

In comparison with other major hazard industries such as oil and gas and aviation, the nuclear industry has thus far been reluctant to make a widespread use of Bowties in its Nuclear Power Plant (NPP) Safety Cases. It is suggested that so doing will confer an additional value to the Safety Case as an effective tool for managing nuclear safety risks during plant operation.

References

1. IMechE event: 6th June 2017 Fit for purpose safety cases in the nuclear industry What does "fit for purpose" mean when we are talking about nuclear safety cases? Geraint Williams – ONR Principal Inspector. 6th June 2017, Birmingham S Brinsden, NNL
2. IMechE - Fit for Purpose Safety Cases in the Nuclear Industry. S H A P E-ing the Safety Case Summary Report – a case study in 'failure'?. 6th June 2017, Birmingham S Brinsden, NNL
3. Producing Safety Cases Good Practice Based on Lessons Learnt in the UK and Middle East. Mike Bates Risktec Solutions DMCC, Dubai. Safety Case Symposium 2018, Singapore.

4. Thompson, E, Taylor, M. Are Safety Cases past their sell-by date? Can we make them more relevant?. Hazards 28. Edinburgh, UK. 2018.

5. Ilizastigui, P.F "Use of Bowtie methodology in the generic pre-construction safety report (GDA PCSR) for Advanced Water Cooled NPPs. IAEA International Conference on Topical Issues. Vienna, Austria. 2017.

UK ABWR GDA document library page. ABWR Pre-Construction Safety Report (PCSR). 2017.

http://www.hitachi-hgne-uk-abwr.co.uk/gda_library.html