



Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

Provision of Technical
Support to the Consideration
of Realistic Software
Modelling in PSA

ONR T774

Revision 1.3

Date: 3 March 2023



Executive Summary

ONR has contracted the ATLAS Consortium for providing technical support to the consideration of realistic software modelling in PSA. For this purpose, a document review, a survey and two workshops (one with industry, one with ONR inspectors) were conducted as part of this project to develop suggestions for possible improvements to the relevant TAG and SAPs.

Document Review

In consultation with ONR, a total of 52 documents were selected for review. The selection of documents was aimed at enabling a basis for comparison of modelling of digital C&I in nuclear reactor plants, other nuclear facilities as well as in other high-risk industries (e.g., space, aviation, medicine, defence) to illustrate similarities but also differences in approaches and the crediting of software reliability in safety justifications.

For the review, a matrix/table was created documenting the results of a first round of analysis (this table is included in the appendix of this document). The documents identified as relevant for the project were then further reviewed and the findings documented in presentations that fed into the first workshop with industry experts (see below).

The document review revealed that typically in non-nuclear high-risk industries no more advanced methods are used than in the nuclear industry. The only other industry that takes a comparably advanced probabilistic approach to assessing digital C&I (and software in particular) is space. For example, the NASA has guidelines for conducting probabilistic risk assessments (PRAs) and a NASA guidebook explicitly states that safety assessments are integral parts of the software life-cycle, from the specification of safety-related requirements, through inspection of the software-based control equipment, and into verification testing for hazards.

Within the nuclear industry a number of particularly relevant documents were identified, particularly ones summarising methods developed by EPRI and the US NRC (NUREGs). However, it was concluded that no single method alone is considered sufficient to

accurately estimate software reliability. Combinations of two more methods are/might be necessary

Industry Workshop

The first workshop of this project was held on 4-5 May 2022 in Warrington with experts from the UK nuclear and non-nuclear industries on the topic of realistic modelling of software in PSA.

Prior to the workshop, an additional survey was conducted with potential participants. This was to help the participants to target their presentations/contributions to the topic of the workshop. All contributions as well as the detailed results of the survey can be found in the appendix of this report.

The contributions and the discussions during the workshop confirmed the findings of the document review but also identified a range of current issues, as well as relevant good practice to help overcome these. It has also been confirmed that the nuclear industry has one of the highest levels of software evaluation (compared to other industries). But here, too, there is still a need for further development (especially with regard to guidance and regulations). Both methodologically and in terms of reliability data, no conclusive answers are yet available. All nuclear licensees and requesting parties feel additional guidance would be of benefit to all.

ONR Workshop

The second workshop of this project was held on 6 September 2022 in London. In addition to ONR PSA inspectors, C&I inspectors were also involved here.

First, the results of the document review and the first workshop were presented to new stakeholders (particularly ONR C&I inspectors) who had not yet been involved in the project. C&I inspectors were then given the opportunity to provide their views and present some examples of C&I assessments they have produced in relation to software reliability. Finally, the PSA inspectors also provided their views and presented some examples of PSA assessments they have produced in relation to software modelling in PSA. The different perspectives and examples presented were discussed in detail during the workshop. Furthermore, the ATLAS Consortium additionally presented a number of initial recommendations for improvements to ONR documentation (particularly TAG-030),

which were also discussed in the group. The materials presented during the workshop are available in the appendix of this report.

It was clear from the valuable workshop that greater interaction between PSA and C&I disciplines would be of mutual benefit, both within the ONR and in wider industry.

Suggestions for Updates to Existing Guidance

From work performed throughout this project it is clear that there are two main issues that lead to inconsistency and confusion in the PSA community regarding the inclusion of software in models:

- 1) A lack of guidance on how to generate best estimate software reliability data for use in PSA models so that the software failure events do not artificially dominate results (noting that the majority of other data in the PSA is best estimate).
- 2) A lack of guidance on how systematic software failures should be considered in PSA models to improve where possible on the conservative assumption that all software failures are systematic failures that would simultaneously fail all redundant components / trains using that software.

In addition to current issues and challenges, the work throughout this project resulted in the identification of relevant good practice (RGP) arising from the cross industry literature review and discussions at workshops with industry experts and the ONR. Recommendations have been made for identified RGP to be fed into future updates of TAG-30 in form of additional supplementary guidance on the modelling of software in PSA. In particular, the following items are likely to be of particular significance for inclusion:

- Guidance on the numerical and functional breakdown of DCI systems in PSA models to reduce conservatism and facilitate a wider range of sensitivity analyses
- Guidance on the treatment of systematic software failure
- Use of sensitivity studies in PSA to inform software reliability requirements
- Overview of Independent Confidence Building measures (ICBMs) and how they can support generation of best estimate data for software
- Replication / incorporation of some relevant guidance currently included in TAG-46 into TAG-30

Table of Contents

1	Introduction and Objectives.....	8
2	Task 1: Review of Documents	11
2.1	Basis for the Review	11
2.2	Methodology	11
2.3	Results	12
2.3.1	Non-nuclear Industries.....	12
2.3.2	Nuclear Industry.....	15
2.4	Conclusions	18
3	Task 2: Industry Workshop (WS1).....	19
3.1	Questionnaire	19
3.1.1	Methodology	19
3.1.2	Results	19
3.2	Workshop 1	23
3.2.1	Contributions – Summary	23
3.3	Summary and (Preliminary) Conclusions	28
4	Task 3: ONR Workshop (WS2).....	29
4.1	Contributions – Summary	29
4.1.1	Examples from C&I of assessments ONR have produced related to software reliability	29
4.1.2	Examples from PSA of assessments they’ve produced related to software reliability	31
4.1.3	Suggestions from Atlas for improvements to ONR Documents	32
5	Task 4: Suggestions for Updates to Existing Guidance	33
5.1	Relevant Good Practice Identified During the Task 1 – Literature Review.....	33
5.2	Relevant Good Practice (RGP) identified during Tasks 2 and 3 – Workshops with Industry and the ONR	34
5.3	Guidance on the Breakdown of C&I Systems in PSA Models	35

5.4	Guidance on Best Estimate Reliability Data to be Assigned to Software Failure Events.....	36
5.5	Guidance on Systematic Software Failure	37
5.6	Use of PSA to Perform Sensitivity Studies related to Software Reliability Requirements	39
5.7	Discussion of Statistical Testing to Achieve 50% Confidence	40
5.8	ICBMs and How they can Support Arguments around Software Reliability	41
5.9	Review and Replication of Key Guidance from TAG-046 to Improve Guidance on use of Best Estimate Reliability Values	42
6	References	45
7	Annex	46
7.1	Annex Task 1: Review of Documents	46
7.1.1	Documents Considered for the Review.....	47
7.1.2	Results of Literature Survey – Evaluation Matrix.....	53
7.2	Annex Task 2: Industry Workshop (WS1)	93
7.2.1	Questionnaire	93
7.2.2	Results of Survey – Redacted.....	100
7.2.3	List of participants and agenda - Redacted.....	123
7.2.4	Presentations (proceedings) - Redacted.....	125
7.3	Annex Task 3: ONR Workshop (WS2) - Redacted.....	126
7.3.1	List of participants and agenda - Redacted.....	126
7.3.2	Presentations (proceedings) - Redacted.....	127

Glossary

AGR	Advanced Gas-cooled Reactor
ALARP	As Low As Reasonably Practicable
C&I	Control and Instrumentation
CBSIS	Computer Based Systems Important to Safety
CCF	Common Cause Failures
CINIF	Control and Instrumentation Nuclear Industries Forum, UK
COTS	Commercial-off-the-Shelf
CSNI	Committee on the Safety of Nuclear Installations of NEA/OECD
DCI	Digital Control and Instrumentation
DiD	Defence-in-Depth
EPRI	Electric Power Research Institute, USA
FAA	Federal Aviation Administration, USA
FMEA	Failure Mode and Effects Analysis
ICBM	Independent Confidence Building Measures
NASA	National Aeronautics and Space Administration, USA
NEA	Nuclear Energy Agency of OECD
NKS	Nordic Nuclear Safety Research
OECD	Organisation for Economic Co-operation and Development
OpEx	Operational Experience
PIE	Postulated Initiating Event
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
SEE	Single Event Effect
SFMEA	Software Failure Modes and Effects Analysis
SFTA	Software Fault Tree Analysis
SSC	Structures, Systems and Components
TSC	Technical Support Center
U.S. NRC	Nuclear Regulatory Commission, USA
WGRISK	Working Group on Risk Assessment of NEA/OECD

1 Introduction and Objectives

Safety-related control and instrumentation (C&I) systems in new nuclear facilities often incorporate digital C&I (DCI) technology. In addition, DCI is increasingly being adopted in legacy plants and facilities in the UK as existing analogue equipment becomes obsolete. General experience in conducting PSA for nuclear facilities shows that DCI has a significant potential for critical failures of functions important to safety and often is a significant risk contributor.

PSA models often include representation of DCI in varying levels of detail ranging from simple single 'super component' events to more complex fault trees separating hardware and software elements. Most analyses are carried out based on models and differ, among other things, in their modelling approaches, assumptions, reliability characteristics, and methodological procedures (particularly regarding software). Software reliability is often modelled with a conservative approach, adopting high confidence values. As most other reliability data is a PSA is best estimate, this approach can skew results and risk insights.

For this reason, additional guidance is required for licensees and regulators. ONR has contracted the ATLAS Consortium under contract ONR T774 "Provision of Technical Support to the Consideration of Realistic Software Modelling in PSA". Within this contract, the ATLAS consortium composed by experts from the Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH and Corporate Risk Associates (CRA) Ltd. provided technical support to ONR to update the corresponding TAG and SAPs to have a consistent approach across the industry that helps ensure that PSA models are best estimate so that the risk insights derived from them are as realistic as possible.

The basic approach within the project to achieve these goals is shown in Figure 1-1.

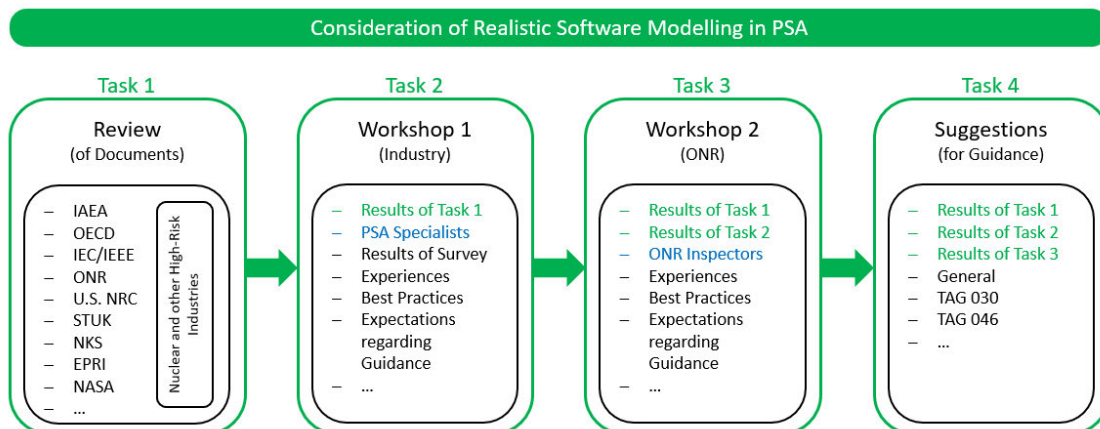


Figure 1-1 Basic approach of this project.

The technical objectives within the project were completed within four Tasks. Further Tasks, which served exclusively the formal handling of the project, are not explained in detail in this report; the relevant information can be taken from the original offer /ATL21/.

In Task 1, a review of selected documents was conducted. The focus here was on the consideration of the reliability of software in PSA in nuclear and other high-risk industries.

The results of Task 1 were directly incorporated into the subsequent Task 2. In this task, a workshop was held with representatives from industry (PSA specialists). Among other things, the participants reported on their experiences with regard to the consideration of software in PSA and, in particular, the application of the guidance to be considered in each case. Additional insights were gained from a survey conducted in advance, which also helped workshop participants prepare for the workshop topics.

The collected results were then discussed in another workshop with ONR inspectors in Task 3. In particular, the different perspectives of ONR PSA and C&I specialists were taken into account. Contrary to the idealized, linear representation of the project flow in Figure 1-1, suggestions for and perspectives on the existing guidance were also introduced by the ATLAS Consortium and discussed within this workshop.

In Task 4, the results of all previous tasks were finally taken into account in order to summarize final suggestions and possibilities for improving the guidance.

With regard to the referencing of sources, there is a special feature in the context of this document. If a reference refers to a document that was also considered in the context of Task 1 (Review of Documents), they are designated in the following text according to the

reference designation in Table 7-1. All other cited documents are listed separately in Chapter 6 (References) and can be recognized by the tildes ("~") around the citation.

2 Task 1: Review of Documents

Originally labelled "Review of Industry Practice for Modelling Software Reliability, particularly within PSA" /ATL21/, a review of documents was conducted in Task 1 to determine the current state of consideration of software in PSA (including regulation) in the nuclear and other high-risk industries.

2.1 Basis for the Review

Based on the experience of the TSCs involved in the project and close and regular coordination with ONR, a total of 52 potential documents were selected for analysis. However, the somewhat limited availability of freely available relevant documents also had an influence on the selection. A complete listing of all documents considered can be found in the appendix (7.1.1).

The selection of documents was aimed at enabling a basis for comparison of modelling of DCI in nuclear reactor plants, other nuclear facilities as well as in other high-risk industries (e.g., aerospace) to illustrate similarities but also differences in approaches and the crediting of software reliability in safety justifications.

The literature reviewed included documents prepared, for example, by the OECD/NEA CSNI WGRISK, the U.S. NRC (NUREGs), EPRI, the NKS, CINIF, and other internationally available documents on DCI assessments performed to date, modelling approaches applied and relevant operating experience. The exact review areas were discussed and agreed with ONR before and during the analyses.

2.2 Methodology

Task 1 was to perform a review of industry practice for modelling the reliability of software, particularly within PSA. Therefore, this task included a literature survey from nuclear and other high-risk industries. The goal of these surveys was to compare the experiences and methodological approaches in nuclear and non-nuclear industries to consider insights from state-of-the-art PSA modelling for nuclear reactors for determining the overall risk posed by a facility and for decision making related to DCI risk insights as well as to consider potential applications of PSA, particularly in respect of modelling DCI, to other risk significant nuclear operations in the UK, notably Sellafield.

Methodologically, a matrix was created for the analysis, in which the results of a first analysis run were documented. The documents identified as relevant to the project were then further analysed. Afterwards presentations have been prepared, which served as the basis for discussions with experts from the nuclear and non-nuclear industry during the first workshop (WS1, see also Task 2, Chapter 3). The complete analysis (evaluation) matrix with an overview of the respective analysis results can be found in section 7.1.2 of the appendix.

The findings obtained by the industry review must be placed in the context of the overall project. Alone, these findings cannot be understood as an already complete statement on best practices regarding software in PSA, but rather as a building block in the exchange with the nuclear and non-nuclear industry in the context of a workshop (see Figure 1-1) to gather possibilities to improve the regulatory guidance concerning the representation of software reliability in PSA.

2.3 Results

According to the objectives and selected industries for the review, some general conclusions can be drawn. These are briefly summarized below in separate sections for the non-nuclear and nuclear industries.

2.3.1 Non-nuclear Industries

2.3.1.1 Aviation

With regard to the aviation industry, exclusively documents related to the Federal Aviation Administration (FAA, USA) were examined on the basis of the available documents. The review showed that this agency follows its own procedures and certification system. The primary concern of the FAA (see DO-178C) is the traceability of development artifacts (requirements, design, code, testing, etc.).

In particular, what can be concluded here is what is also described in a U.S. NRC document (NUREG-CR-6901) as follows: “The authors note the FAA’s approach focuses on development processes and artifacts created during software development as opposed to evaluating risk based on the delivered software itself.”

2.3.1.2 Space

The space industry, essentially the National Aeronautics and Space Administration (NASA, USA), also follows its own procedures and certification system, as does the aviation industry.

For example, the NASA has guidelines for conducting PRAs /NAS11/ and, more specifically, NASA-GB-8719.13 explicitly states that safety assessments are integral parts of the software life-cycle, from the specification of safety-related requirements, through inspection of the software-based control equipment, and into verification testing for hazards. It also provides analyses, methods and guidance which can be applied during each phase of the software life cycle:

- Software Fault Tree Analysis (SFTA),
- Software Failure Modes and Effects Analysis (SFMEA),
- Requirements State Machine,
- Preliminary Hazard Analysis and
- Reliability Modelling.

NASA, based on extensive experience with spacecraft flight operations, has established in this guidebook levels of failure tolerance based on the hazard severity level necessary to achieve acceptable levels of risk (see also IEEE Std 1633-2016 in Table 7-3).

More details on NASA's procedures can be found in section 3.1.2.1, and the corresponding individual documents considered (or the results of the review) can be found in Table 7-3 in section 7.1.2 of the appendix.

2.3.1.3 Medicine (Medical Devices)

The documents considered for the industry review did not themselves contain any examples from medicine or medical devices. However, corresponding investigations were carried out by the NRC and documented in NUREG-CR-6901. Since this document was taken into account in the industry review, at least the corresponding conclusions can be quoted here:

No formal risk assessment is conducted for medical devices (in the USA). The U.S. Food and Drug Administration (FDA) has published guidelines covering principles of software

validation, but the guidelines do not endorse any specific engineering, quality assurance, or quality control techniques. No specific development methodology is sanctioned either. The corresponding guidelines suggest that the 'least burdensome approach' is the best approach.

2.3.1.4 Defence

The used approaches in the USA (at least in available documents) do not address PRA/PSA for digital systems or software components, but it is acknowledged that software risks must be assessed differently. The determination if the systems are truly battlefield-ready is done by essentially system level tests under harsh conditions. While such tests often reveal deficiencies, all too often they fail to find problems that are exposed only under real battlefield conditions (see, e.g., NUREG-CR-6901).

The UK defence industry follows Def Stan 00-56 which requires full lifecycle system safety assessments to be produced when new systems are introduced. Since the document is only available for a fee and was therefore not readily available during the project, the review relies on freely available information from the UK Ministry of Defence. According to this, however, software and software reliability assessment are not explicitly a topic of this standard.

2.3.1.5 Railway

The limited number of documents reviewed for this industry referred to the use of qualitative methods only, such as IEC 61508. Conclusions on probabilistic methods, especially on the consideration of software in PSAs, are therefore not possible.

2.3.1.6 Petrochemistry

The limited number of documents reviewed for this industry referred to the use of qualitative methods only, such as IEC 61508. Conclusions on probabilistic methods, especially on the consideration of software in PSAs, are therefore not possible.

2.3.1.7 Preliminary Conclusions – Non-nuclear Industries

Based on the documents considered in the review, the following conclusions can be drawn for the non-nuclear industry:

In principle, no considerably better methods can be found in other industries for the evaluation of software in PSA (especially e.g. consideration in FTA) than in the nuclear industry. A level comparable to that in the nuclear industry is almost achieved exclusively in the aerospace industry (mainly NASA). Otherwise, the (available) documents on the non-nuclear industry do not provide any significant, new insights. More information can be found in Table 7-3 in section 7.1.2 of the appendix.

2.3.2 Nuclear Industry

2.3.2.1 Potential Methods / Methodologies

There is no consensus in the nuclear community about how the reliability of software systems should be modelled, measured, and predicted, and even whether such a concept makes sense for software. Potential methodologies for the reliability modelling of digital C&I include (without claiming completeness):

- ET/FT methodology (including dynamic FT techniques)
- Markov models
- Dynamic flowgraph methodology
- Bayesian methodologies
- Petri net methodologies
- Test based methodologies
- Software metric-based methodologies
- Black-box methodologies (Schneidewind Model)
- Monte-Carlo simulations

According to the current state of knowledge, no method alone might be sufficient. Combinations of two more methods are/might be necessary.

The Electric Power Research Institute (EPRI, USA) has published an important approach to estimating the reliability of DCI systems in PSA models in two documents

(EPRI 1021077, EPRI 1025278). The first step of the methodology described in EPRI 1021077 is to identify the critical digital failure modes in a PSA model. For the non-critical digital failure modes, a failure probability based on IEC 61508 or OpEx can be used. For the critical digital failure modes, a C&I suitably qualified and experienced personnel (SQEP) review is required to assess the failure probability based on a number of steps documented in the method. The steps are as follows:

1. Identification and classification of the failure mechanisms that can lead to the failure modes and digital common-cause failures determined in the PSA.
2. Development of a reliability model of the digital system (this model is separate to the PSA).
3. Identification and assessment of the defensive measures taken to avoid, eliminate or tolerate certain types of errors, failure modes or failure mechanisms (including common-cause failure) that could affect elements of the digital systems reliability models.
4. Quantification of the rates of occurrence of the failure modes that could affect elements of the digital systems reliability models and have not been rendered negligible by the defensive measures.
5. Use of the digital systems reliability models to compute the critical PSA parameters associated with the failure modes identified using the PSA.

The method focusses effort on the most risk significant digital failure modes (as identified by the PSA), which minimises the effort involved. In addition, the proposed method is logical and relatively straightforward to understand and follow. However, the quantification is dependent, to some extent, on expert judgement and the availability of sufficient information to make a judgement. This may cause problems when being applied.

EPRI 1025278 is an evolution of the method introduced in EPRI 1021077. It includes some further detailed guidance on the modelling of digital C&I compared to EPRI 1021077, but the method itself is largely the same.

2.3.2.2 General Issues

The documents considered in the review identify some general issues for realistic modelling of software in PSA without resolving them yet:

- Failure mechanisms (and thus also failure modes) of software are not well defined, for example:
 - (Potential) new failure modes in digital C&I due to internal (and external) network communication, operation in discrete time steps (for example, the sampling rate can be too low for the application¹), ...
- Consideration of life cycle aspects:
 - Software and hardware of digital C&I may be changed by updates and/or upgrades over its lifetime
 - Probable negative impacts of configuration management of the C&I (maintenance aspects)²
 - Interactions between aged hardware (bathtub curve, /WIK22/) and software
- Software can introduce corrective actions or mitigate failed hardware through fault tolerance or fault recovery
 - But: Software may be able to mask intermittent failures in hardware by this, too
- Digital C&I systems can trigger common cause failures due to the software, even in supposedly diverse systems (use of standardized components (and software, e.g., operating system) for building the systems)

2.3.2.3 Methodology Requirements

The following requirements for potential methodologies can be formulated (see especially NUREG-CR-6901):

- The methodology should account for possible dynamic interactions between:
 - the digital system and controlled/supervised plant physical processes
 - the components of the digital system itself
- The model must be able to predict future failures well and cannot be purely based on previous experience

¹ In contrast to purely analogue systems, in digital C&I systems all values (and for example also actuation signals derived from them) are calculated cyclically (e.g. calculation of the new state every 50 ms). Thus, a digital C&I system cannot react faster than the set cycle time. An unfavourably selected cycle time can thus lead to a reaction time that is too slow for the application.

² Digital systems are changed much more frequently through updates and upgrades. This configuration management can itself be the cause of problems or failures.

- The model must make valid and plausible assumptions and the consequences of violating these assumptions need to be identified
- The data used in the quantification process must be credible to a significant portion of the technical community
- The model must be able to differentiate between a state that fails one safety check and those that fail multiple ones
- The model must be able to differentiate between faults that cause function failures and intermittent failures
- The model must have the ability to provide uncertainties associated with the results

No previously mentioned single methodology (see Section 2.3.2.1) has been identified that satisfies all the requirements. And even more important, none of the previous mentioned methodologies have been shown to satisfy the requirement that the data used in the quantification process must be credible to a significant portion of the technical community.

2.3.2.4 Preliminary Conclusions – Nuclear Industries

The reviewed documents related to the nuclear industry do not yet provide final answers on how to consider software in PSA. Even though the nuclear industry has been one of the few proponents of including software failure rates in deriving the overall reliability of the final design of digital C&I systems, there are still many open questions that could not yet be answered.

2.4 Conclusions

Overall, the industry review has not yet been able to provide any final answers. However, this was not the intention of this review. Rather, the industry review was intended to and could only provide inputs for the discussion at the first workshop (WS1) with the British nuclear industry and ONR.

3 Task 2: Industry Workshop (WS1)

The first workshop (WS1) with experts from the British nuclear and non-nuclear industry on the topic of realistic modelling of software within PSA was the essential building block to determine desirable regulatory boundary conditions with regard to the consideration of software in PSA.

As a basis for triggering the discussions necessary for this, the performance and presentation of the industry review (Task 1, see Chapter 2) was necessary. In addition, however, it was at least as important that the corresponding discussions with the British industry were also supported by the contributions of the participants (in the form of presentations).

3.1 Questionnaire

In preparation for the workshop, and in particular to provide presenters with a guide for preparing their presentations, a questionnaire was prepared and sent to potential participants with the invitation to the first workshop. The complete questionnaire is shown in Section 7.2.1 of the appendix.

3.1.1 Methodology

Like the industry review, the survey, in addition to serving as a guideline for presentation, was also intended to serve as a basis for discussion during the first workshop.

Therefore, the results of the survey were prepared for the workshop in a presentation and presented during the workshop. The corresponding presentation can be found together with all presentations of the workshop in Section 7.2.4 of the appendix.

3.1.2 Results

The full results of the survey, as also presented at the first workshop, can be found both in the corresponding presentation (see Section 7.2.4 of the appendix) and again separately in Section 7.2.2 of the appendix.

In principle, the results also confirm the findings of the industry review, but also provide some deeper insights into the different current approaches in the nuclear and non-nuclear industries.

3.1.2.1 Summary of Non-nuclear Industry Approaches

Feedback from practitioners in non-nuclear industries (mainly from two sectors: aviation and railways) was gathered both through the survey questionnaire and face-to-face interviews.

Aviation Industry

The feedback was in-line with the findings from the literature review. This can be summarised for the aviation industry as follows:

- Systematic Errors are mitigated by implementation of a design assurance process (specifically RTCA DO-178C/EUROCAE ED-12C). DO-178C/ED-12C states that development of software to a software level does not imply the assignment of a failure rate for that software.
- Many methods for predicting software reliability based on developmental metrics have been published, for example, software structure, defect detection rate, etc. This document [DO-178C/ED-12C] does not provide guidance for those types of methods, because at the time of writing, the available methods do not provide an adequate level of confidence.

In practice, this means that software reliability is not included in quantitative risk assessments in the aviation industry for the purposes of generation of final risk results for comparison against numerical targets or goals. However, a representation of software reliability (often using 'decade' numbers – 1E-02, 1E-03 etc) is often included in sensitivity studies and additional analyses that are performed in order to understand, amongst other things, software reliability requirements.

In addition, the aviation practitioners spoken to also mentioned other points worthy of discussion:

- The adoption of a software design assurance process (such as the adoption of DO-178C/ED-12C) remains the most credible means of achieving a high degree

of software integrity. Since the publication of DO-178B/ED-12B in 1992, there has not been a single hull loss accident of a type-certified jet airplane in service that has been ascribed to the failure of software to comply with its requirements. There have been a number of accidents where the software complied with its requirements, but those requirements specified unsafe behaviour in some circumstance (e.g., the Boeing 737 Max accidents). It therefore follows that we need to focus on getting the requirements right if we are to improve safety.

- In relation to estimating software reliability based on statistical testing, ‘software reliability models that assume that software execution is a Bernoulli process are flawed, leading to an exaggerated confidence in probabilistic testing.’
- The use of dissimilar software has been proposed as a means of preventing common cause failure. The feedback considered this approach unsuitable for software based failures.
- One of the correspondents has written a technical paper on this subject /DAN22/.

Space Industry

Much more comparable approaches to the nuclear industry can be found for the space industry (mainly NASA):

NASA has a PRA Procedure Guidance Document (Reference /NAS11/). This refers to the use of the Context-based Software Risk Model (CSRM) (Reference /NAS13/) for dealing with software failures in a typical PSA model and provides a high level explanation. CSRM is a five-step process:

1. Identify the mission-critical software functions.
2. Map the critical software functions to corresponding PRA model events.
3. Develop a set of associated logic models.
4. Identify, from the above models, the software-related cut sets for system and mission failure events.
5. Estimate the probability contribution from the software-related cut-sets to the system and mission failure events of interest. [This may include, at the top-level, the contribution to key risk metrics such as Loss of Mission (LOM) or Loss of Crew (LOC).]

Step 3 of the CSRM involves the development of a set of associated logic models, which means development of dynamic fault trees (Figure 3-1).

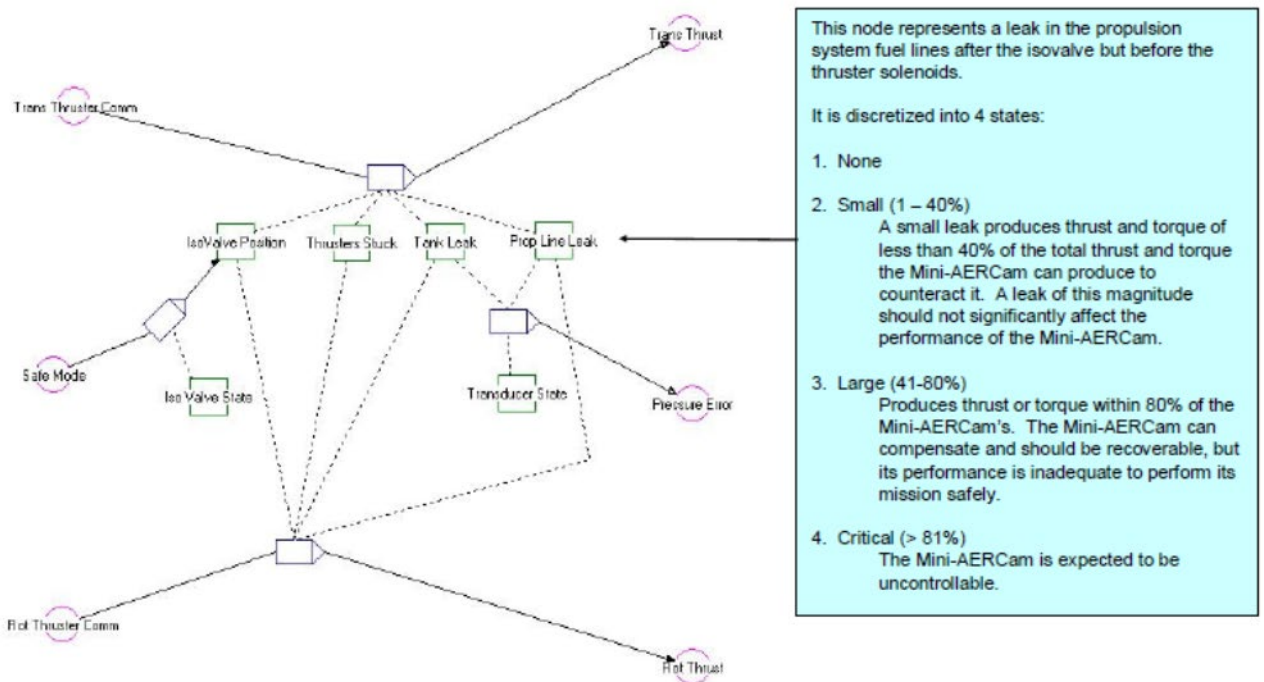


Figure 3-1 Example of an associated logic model, from /NAS11/.

Step 5 involves the estimation of failure probabilities for the critical software failures. This is described as being based on using previous OpEx for similar software combined with specific test data. A Bayesian process is used to combine the two.

Following a high level review during this project, the methods outlined in /NAS11/ and /NAS13/ appear to be complex and are likely to be time consuming. They are also very specific to the application and function of software in the space industry. Whilst further review may be of benefit, it is considered that the methods outlined in these references may not be particularly accessible or applicable for use in the nuclear industry.

Railways

Rail standards covering software reliability are derivatives of international functional safety standards (IEC 61508). Software reliability is therefore quantified in-line with this standard. This means that one of three approaches can be taken:

- High confidence limiting values based on qualitative assessments
- Historical data - this will need to include an argument why the historical data is applicable to the current application

- Test data – this will need to include arguments based on the number of tests and its coverage, to confirm it is applicable to the current application

Preliminary Conclusions – Non-nuclear Industry approaches

- The gathered feedback supports the conclusions of the literature review – no advanced methods for estimating software reliability were identified in use in industries other than space.
- NASA has detailed guidance which could possibly be useful to the nuclear industry but is complex and requires further review.
- The aerospace industry purposefully treats software failures very differently to hardware failures.
- No attempts are made to estimate software failure rates in the aviation industry, therefore software failures cannot be included as part of any quantitative risk assessment for the purposes of generation of final risk results for comparison against numerical targets or goals.

3.2 Workshop 1

The first workshop (WS1) was held May 4-5, 2022 at [REDACTED]
[REDACTED] In this hybrid event (personal participation on site or connection via videoconference), representatives of the industry were able to exchange ideas on the issues of this project. The composition of the participants as well as the agenda of the event can be seen in the appendix, section 7.2.3.

3.2.1 Contributions – Summary

The following summarize some of the key findings of the workshop in bullet form. All presentations can also be found in full in the annex (section 7.2.4).

3.2.1.1 Current Reactors – EDF Energy

- Focus on COTS / smart components

- Not currently quantifying reliability but EDF Energy are occasionally using higher reliability figures than those which components are assessed to by using additional justification
- Some inconsistent approaches in modelling of software in PSA models for each station
- Some other useful points for further consideration (for details see appendix 7.2.4)

3.2.1.2 Planned Reactors – Hinkley Point C Project

- Focus on reactor safety systems
- Modelled in PSA at a fairly detailed level using EDF France ‘compact model’ (sensors, actuators, processors, systems, technology etc)
- Inconsistent approaches to PSA data between technology due to data availability

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

3.2.1.3 Non-nuclear Approaches – Ebeni

- Useful overview of approaches in other industries, particularly Aerospace
- Decision to not try and analyse software reliability and include in risk models quite deliberate
- Focus on use of risk models to understand reliability requirements and inform qualitative substantiation

3.2.1.4 Overview of WGRISK “DIGMAP” project – GRS

- Interesting international benchmarking project with focus on modelling of C&I in PSA as opposed to software reliability directly

- Useful insights drawn particularly for those about to embark upon the development of new PSA models (level of detail, important areas, reliability ‘cliff edges’, etc.)

3.2.1.5 Related Activities

EDF Generation

- Brief overview of the CINIF Prior use Data project
- Smart Devices Simplicity Project (EDF and Adelard)
- Projects focusing on supporting /justifying the reduction of high confidence reliability values

University of Bristol

- Statistical testing and its role in software reliability estimation
- Provided some interesting points of reliability and software in PSA – some overlap with licensee discussions
- Likely significant future challenges the way reactor technology is heading – use of digital twin environment for testing

3.2.1.6 Approach to Specification of Safety Measures (Target Setting) Design Realisation and ALARP Justification –Sellafield Safety Case

The focus is now on decommissioning, this means the following:

- Fault sequences are modelled, but there is not an overall PSA
- There is less rigour than in a reactor PSA
- The tool is focussed on demonstrating that the risk is ALARP
- There has been a general move towards high-level deterministic risk arguments in their safety cases
- The RGP for reactor PSA is not considered to be the same as it is for facility PSA.

The process is as follows:

- The safety case team defines risk targets
- The design team designs to these targets and has to show they have been met (substantiation against the risk targets)

- Older safety cases used to rely on fault trees to show the risk target had been met (developed by the safety case team). This is now done by hand calcs by the design team.
- SL Tech Guide E2.10 presents guidance for safety measures

3.2.1.7 AWE Approach – AWE – C&I Compliance

- QRA is carried out by safety specialists, software failure is generally not included
- QRA is used to produce Safety Functional Requirements (SFRs) for engineers in the design teams
 - AWE Design Authority (DA) helps the design teams to interpret/understand the SFRs
- Other stakeholders:
 - C&I Tech Authority
 - ARM Tech Authority
 - Maintenance Tech Authority
- Unsubstantiated software is limited to 0.3 per year (as per TAG-46).
- Smart components are qualified using Emphasis with some exceptions – legacy systems have used proven-in-use, coupled with 61508 compliance and exhaustive ALARP arguments.

3.2.1.8 DRDL Approach – Babcock Safety Case – PSA

- PSA considers high-consequence risks only
- Deterministic Safety Analysis is the primary tool for setting reliability targets
 - PSA reflects the substantiation against these targets carried out by the design team
 - PSA then provides risk reduction analysis.
- PSA includes Class 1 and Class 2 safety measures
 - PSA can also include Class 3 measures, but there aren't many of these
- Historically, software-based equipment has been avoided
 - Therefore, there is very little software in the PSA, and it doesn't currently have a large impact on risk

- The modelling of systems is quite high-level with systems represented as supercomponents (using the outputs of separate reliability assessments). Dependencies are added where necessary.
- The site is starting to use smart devices and following TAG-46 for their qualification. It is difficult to get manufacturer's data on these devices due to the small numbers being purchased.

3.2.1.9 ONR Guidance on Best Estimate Software Assessment – ONR

- The TAGs don't include any mention of mean values
 - Gives the analyst the choice of what to use
 - Allows conservatism where there is uncertainty
- The TAG states that diagnostics should be taken into account.
 - This is done in the HPC model (as an example) using detected/undetected branches
- The use of 95-99% confidence level intervals was discussed
 - Should best estimate values be used when substantiating reliability targets?
 - 95-99% has to be used for deterministic analysis
 - Lower confidence intervals can be used for PSA, as per para 5.13 of TAG-46.
- TAG-46 also states that statistical testing can be used to derive reliability estimates for PSA models (noting the limitations on where statistical testing can be used, as per the presentation [REDACTED] on the previous day)

ONR Guidance on Best Estimate Software Assessment – group discussion:

- The options for change available were summarised as follows:
 - Exclude software reliability completely (as per the aerospace industry)
 - Include as part of an initial sensitivity study then remove as part of the final calculation.
 - Include software dependencies only (based on a simple justification similar to the UPM beta factor method).
 - Think about an innovative approach, e.g., BBNs.
- Examples would be useful as an output of this project (in addition to the existing TAGs). This might be included as part of a practice guide

- Consider guidance on CCF factors for software based equipment based on software assurance levels.
- CINIF might be a better route for producing practice guides (outside the scope of this project).

3.3 Summary and (Preliminary) Conclusions

- So far, the following steps have been performed:
 - Cross industry relevant good practice review (of available documents)
 - Cross industry practice survey and obtaining further feedback from non-nuclear industries
 - Cross industry practice workshop (with nuclear and non-nuclear industry attendees)
- Preliminary conclusions:
 - One of the highest level of software evaluation is achieved by the nuclear industry
 - But: Here, too, there is still a need for development (especially with regard to guidance and regulations)
 - A level comparable to that in the nuclear industry is almost achieved exclusively in the space industry (mainly NASA)
- A single methodology might not satisfy all the requirements
- Reliability data (for software) is an important issue
- All nuclear licensees and RPs feel additional guidance would be of benefit to all.

4 Task 3: ONR Workshop (WS2)

The second workshop (WS2) was held September 6, 2022, at The ONR Offices in Windsor House, London. The composition of the participants as well as the agenda of the event can be seen in 7.3.1 respectively.

4.1 Contributions – Summary

Sessions 1-3 of WS2 summarised material that is already presented in earlier sections of this report to new stakeholders (particularly ONR C&I inspectors) who had not been involved to date. As such this content is not discussed further in this section. Session 5 provided an opportunity for C&I inspectors to provide their views, as well as provide some examples from C&I of assessments they've produced related to software reliability. Session 7 provided an opportunity for PSA inspectors to provide their views, as well as provide some examples from PSA assessments they've produced related to software. In Session 8, Atlas presented a number of initial recommendations for improvements to ONR documentation (particularly TAG-030) which were then discussed as a group.

It was clear from the valuable workshop that greater interaction between PSA and C&I disciplines would be of mutual benefit, both within the ONR and in wider industry.

The following sections provide a high level summary of some of discussions and key findings of the workshop in bullet form. Presentations for Sessions 5, 7 and 8 can also be found in full in the annex.

4.1.1 Examples from C&I of assessments ONR have produced related to software reliability

For Session 5, presentations were provided by ONR C&I Inspectors [REDACTED] [REDACTED]. The high level presentations covered a variety of topics including the following points of note:

- The high levels of uncertainty in software reliability such that anything more precise than decade values (1E-02/1E-03 etc.) are likely to receive scrutiny as there is currently no agreed way to accurately assess the reliability. The uncertainty is also such that if hardware has a reliability of 1E-03 and the software

has a reliability claim of 1E-03, the overall result is still 1E-03 from a C&I perspective.

- It was agreed that there is general consensus that software failures should be included in the PSA but ideally with more best-estimate reliabilities.
- The idea of using similar software in similar applications was discussed. C&I explained that even in similar circumstances there can be non-continuous behaviour where software will fail upon receiving a certain set of inputs. This makes it difficult to take high confidence from use of similar software in similar (but not exactly equivalent) circumstances. To understand the effects of different inputs on the software you need to really understand what is happening inside the software, and this information often isn't available.
- There was agreement with the PSA area's goal to have better estimate reliabilities, but C&I inspectors expressed concern that this could become a back door to allowing lower integrity claims into the deterministic case.
- C&I inspectors explained that duty holders will often use the PSA model to set requirements on the reliability of a system, e.g. 'this line of protection needs to achieve a 1E-03 reliability to meet the claim'. It was explained that this would most likely be based on a best-estimate PSA model and that the changes being proposed to reduce the conservative values assigned to software would not prevent the PSA models from being used in this way.
- A C&I inspector stated that from long term and broad experience they believe that reliability claims derived from SIL values are typically achieved by systems designed to meet those targets because of the development rigour and techniques applied, but for any given system the actual reliability cannot be known until it is operating.
- C&I provided some examples of where they've accepted proven in use arguments following years of OpEx on the actual plant by the system in question. This is more common at older facilities such as the AGRs/Sellafield where balance of risk and ALARP arguments support outcomes not meeting modern RGP.
- There was a consensus that use of both best estimate and high confidence reliability values in the PSA would be beneficial. The typical approach at the moment is for duty holders to use high confidence, conservative values in their models and then reduce them by exception where they are causing problems. It may be preferable to encourage industry to use 50% values as the default 'base case' and run the 95% reliabilities as sensitivity studies to see what the risk would

be if the software was only as reliable as the lower (poorer) end of its SIL reliability bracket. However the framework for deriving 50% confidence values does not currently exist.

- C&I inspectors suggested that duty holders should consider switching off software failures in their PSA models as a sensitivity so that an assessment of the hardware architecture is easier to carry out.

4.1.2 Examples from PSA of assessments they've produced related to software reliability

For session 7, a presentation was provided by ONR. The presentation focussed on the modelling approaches to digital C&I in the Hinkley Point C (HPC) and HPR1000 PSA models. The approaches used in these PSA models represent some of the most advanced approaches used currently in the UK Nuclear industry. Some further details are provided in the presentation slides [REDACTED] in appendix Section 7.3.2.

The approach used in the Hinkley Point C PSA provides perhaps the most advanced method in terms of breaking digital C&I systems down into their respective components and assigning data from a variety of different sources to each component. The presentation outlined current approaches and their benefits in terms of better representing reality regarding dependent failures.

There was a discussion in the earlier meeting session (5 – Section 4.3.1 above) regarding uncertainty and the fact that if C&I hardware has a reliability of $1E-03$ and the software has a reliability claim of $1E-03$, the overall result is still $1E-03$ from a C&I perspective. This is obviously in contrast to the outcome if reliability values are included in a PSA model under Boolean logic gates in a fault tree. Due to the way PSA software works, reliability values need to be sub-divided amongst different aspects of the C&I systems, otherwise the PSA model will sum the different failure modes to a worse reliability than the (often high confidence) reliability value assigned to each aspect. This is an area that would also benefit from additional guidance supported by an example.

4.1.3 Suggestions from Atlas for improvements to ONR Documents

For Session 8, a presentation was provided by ATLAS Alliance outlining some proposed updates to current guidance for discussion. These included:

- Replication and updates of key advice from TAG-046 to improve guidance on use of best estimate reliability values
 - Guidance on numerical and functional breakdown of C&I systems in PSA models
 - Guidance on systematic software failure
 - Use of sensitivity studies in PSA for software reliability
 - Discussion of statistical testing to achieve 50% confidence
- Overview of ICBMs and how they can support arguments around software reliability

Following the presentation there were discussions surrounding the suggested updates. The outcome of discussions fed into the set of recommended updates to TAG-030 presented in Section 5 of this report.

5 Task 4: Suggestions for Updates to Existing Guidance

The purpose of this report section is to provide recommendations for modifications and additions to current regulatory guidance documents to improve clarity, consistency and alignment with relevant good practice identified during the industry review (Task 1) and workshops (Tasks 2 and 3).

From work performed throughout this project it is clear that there are two main issues that lead to inconsistency and confusion in the PSA community regarding the inclusion of software in models:

- 1) A lack of guidance on how to generate best estimate software reliability data for use in PSA models so that the software failure events do not artificially dominate results (noting that the majority of other data in the PSA is best estimate).
- 2) A lack of guidance on how systematic software failures should be considered in PSA models to improve where possible on the conservative assumption that all software failures are systematic failures that would simultaneously fail all redundant components / trains using that software.

The issues are relevant in all areas where software is represented in PSA, from large and complex digital C&I systems supporting reactor protection/safety functions to smaller and simpler smart components with embedded software (firmware) used in safety related systems.

The subsections below cover the items above plus a number of areas that were discussed at Workshop 2 and provide high level suggestions on potential updates to current guidance.

5.1 Relevant Good Practice Identified During the Task 1 – Literature Review

From the cross industry literature review summarised in Section 2 and Table 7-2 in Section 7.1.2, there are a number of key references where guidance is provided that may be useful to inspectors for comparison when assessing methods that duty holders may have adopted.

- EPRI have published an important approach to estimating the reliability of DCI systems in PSA models in two documents (EPRI 1021077, EPRI 1025278). Further details are provided in Section 2.3.2.1.
- The US NRC have performed a large number of studies investigating different quantitative software reliability methods (QSRMs). NUREG/CR-7044 investigates various QSRMs and whilst no single QRSM meets the complete set of desirable characteristics for software reliability estimation, candidates for further consideration are identified (Software Reliability Growth Methods, Bayesian Belief Network (BBN) Methods and Statistical testing methods). Further details are available in Section 7.1.2
- NASA has a PRA Procedure Guidance Document (Reference /NAS11/). This refers to the use of the Context-based Software Risk Model (CSRSM) (Reference /NAS13/) for dealing with software failures in a typical PSA model. Further details are provided in Section 3.1.2.1

Consideration could be given to inclusion of a table of references to relevant documents that are considered RGP in an update to TAG-30.

5.2 Relevant Good Practice (RGP) identified during Tasks 2 and 3 – Workshops with Industry and the ONR

From the workshops with industry experts and ONR, several areas that can be considered RGP were identified.

- EDF Technical Client Organisation presented the ‘compact model’ developed originally by EDF in France and now applied extensively in the Hinkley Point C PSA. This is currently the most advanced representation of C&I in PSA in the UK. Further discussion is provided in Section 5.3 below.
- ONR presented some more recent developments of how evolution of the compact model has further reduced conservatism in the HPC PSA, as well as the approach adopted in the HPR1000 GDA PSA and how this facilitated sensitivity analysis. The latter is discussed in Section 5.6 below.
- EDF Energy Generation outlined numerous examples where proven in use or other arguments following years of collected OpEx have been used to support a reduction in high confidence reliability values, leading to adoption of reliability values in PSA that are more ‘best estimate’. Whilst these are judgement based

reductions of decade numbers assigned to 'supercomponents' they do help to reduce conservatism in models and prevent skew of results and insights. Further discussion is provided in Sections 5.4 and 5.8 below.

Consideration could be given to inclusion of details of this RGP identified by current duty holders as well as ONR themselves, as suggested in sections referenced above.

5.3 Guidance on the Breakdown of C&I Systems in PSA Models

During the course of the project a wide range of examples have been observed regarding how C&I systems are modelled in PSA. These range from simple 'supercomponent' basic events representing entire functions to more developed detailed fault tree models that separate the various aspects of the system (sensors, processing equipment, C&I platforms and actuators). Examples of the latter have clearly shown benefits in terms of the PSA model more closely reflecting reality, removing conservatisms and allowing the model to be better used to obtain risk insights and risk inform the design. It would therefore seem appropriate to update TAG-030 to include some limited and non-prescriptive guidance to ONR inspectors on suitable modelling approaches, highlighting the benefits of developing more detailed FT models for C&I functions where it is practical to do so, in place of the widespread 'supercomponent' approach.

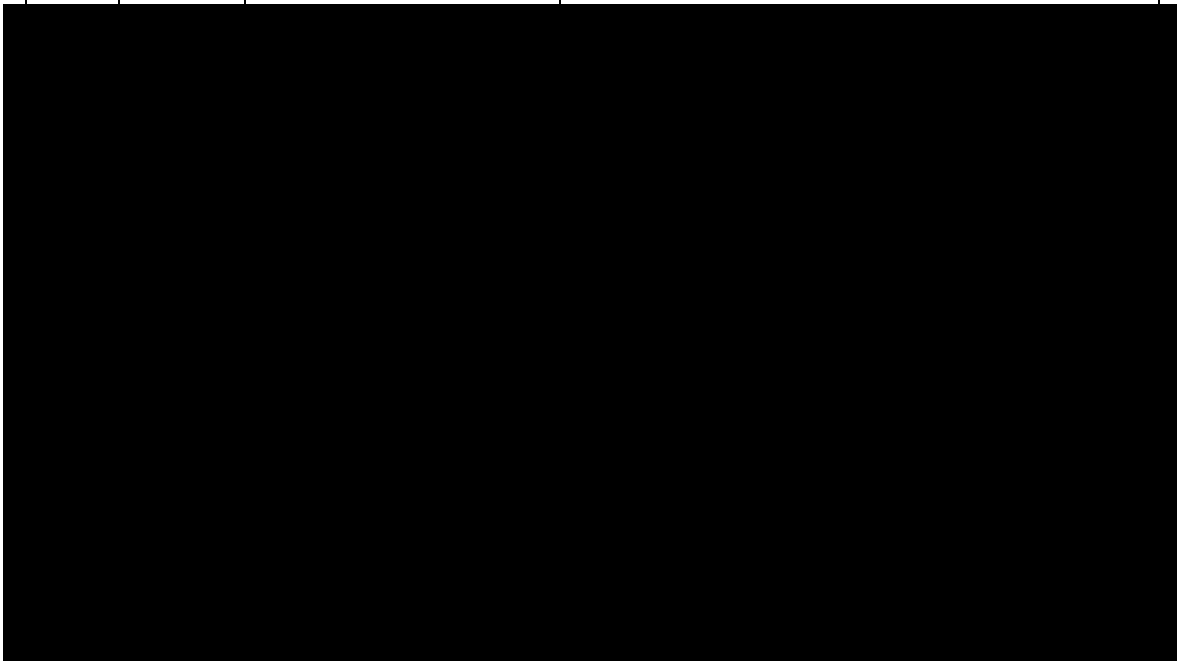
The more detailed FT approach often also allows the hardware and software aspects to be represented separately and explicitly. As there are well understood techniques for estimating best estimate C&I hardware reliability values for both independent failure and CCF this can be useful for reducing conservatisms when compared to a supercomponent approach. The 'compact model' developed originally by EDF in France and now applied extensively in the Hinkley Point C PSA is currently the most advanced representation of C&I in PSA in the UK. This is explained in more detail in the EDF Technical Client Organisation presentation entitled [REDACTED] in appendix Section 7.2.4 and the ONR presentation slides titled [REDACTED] [REDACTED] in appendix Section 7.3.2.

Some of the key principles of the 'compact model' could be distilled, summarised and included in the TAG as an example of RGP.

5.4 Guidance on Best Estimate Reliability Data to be Assigned to Software Failure Events

Whilst the project has confirmed that there are currently no accepted methods for deriving best estimate software reliability values, organisations both within and outside of the nuclear industry are developing and applying methods and techniques to work around this issue and reduce conservatism, and this is to be encouraged. Examples of these are presented in Sections 5.1 and 5.2 above. However, there are also likely to be occasions where it may still be necessary for duty holders to use best estimate values in PSA models that are derived based on judgement.

Where possible, the PSA makes best use of operational experience (OpEx) to support reliability data estimation for the majority of modelled structures, systems and components (SSC). During the course of this project there have been numerous examples where proven in use or other arguments following years of collected OpEx have been used to support a reduction in high confidence reliability values. However, this is more common at older facilities where balance of risk and ALARP arguments support outcomes not meeting modern RGP in the area of qualitative reliability substantiation. Examples include a range of assessments performed by EDF Energy Generation such as those presented in the table below:



Additional examples may be found in the EDF Generation presentation entitled [REDACTED] in appendix Section 7.2.4.

In addition, the reliability data assigned to the Class 2 Safety Automation System (SAS) in the HPC PSA model is broken down via the compact model with individual failure events (for specific logic, signal and platform failures) that are assigned reliability values that are lower than the overall safety integrity level value typically associated with a Class 2 I&C system. This is explained further in the EDF Technical Client Organisation presentation entitled [REDACTED] in appendix Section 7.2.4.

At Workshop 1 there was a discussion concluding that it may be possible to develop a framework to attempt to translate high confidence values to best estimate ones using statistical distributions, noting that the width of the distribution would need to be estimated by use of OpEx or other available inputs to aid judgement. However this activity and any associated guidance would likely sit outside of any update to the TAG, perhaps in a separate working group.

5.5 Guidance on Systematic Software Failure

The inclusion of dependent failures (EC&I, operator actions, other dependencies) in the PSA that have the potential to affect multiple otherwise diverse and redundant safety functions make PSA such a powerful tool for risk informed decision making.

TAG-046 Paragraph 10.19 currently states the following:

*A normal duty function continuous mode (i.e. with a failure frequency defined per year rather than per demand) control system may provide a safety function for a number of fault sequences (as is the case for a data processing and control system, for example). If so, the duty-holder should justify its PSA approach and demonstrate how the analysis is used to inform the CBSIS deterministic requirements. For example, a duty-holder should separately model the probability of each function being delivered only if it is reasonable to claim that the system delivering each function is independent. **If, however, a common cause (i.e. systematic) failure of the control system impacts on the delivery of a number of functions, as is likely if they are implemented in the same control system, then the licensee should model the loss of all control functions as a credible simultaneous event within the PSA.***

TAG-046 Paragraphs 10.31 to 10.33 go on to state that:

When assessing the reliability of a CBSIS, it is appropriate to consider the hardware and software aspects separately since their failure behaviour can be quite different.

Simple hardware failures are considered to be predominantly random; hence coincident failures have a low probability of occurrence unless occasioned by a common cause. Hardware reliability can, therefore, be improved by the use of simple redundancy, although a limitation is imposed due to the incidence of common cause failures.

*In contrast, **software failures are due to systematic faults; their occurrence depends upon the values of input and stored parameters causing paths containing faults to be executed. Here simple redundancy gives a limited reliability improvement that is challenging to prove since each program may see the same input values.** The software equivalent of hardware redundancy is achieved by software diversity, since only by such means can coincident failures be rendered less likely. Where a claim is made that very high reliability has been achieved through software diversity then the assessor should consider the guidance provided in appendix 5 and Ref. 2.*

It is suggested that text is included in TAG-030 recognising the requirement to treat software failures in the PSA as systematic events where it is necessary to do so. There was much discussion throughout the course of the project at both workshops as to

whether a factor of 1 should be assumed in cases of highly redundant software based components or systems. I.e. is the assumption that all software failures are systematic and would fail all identical redundant components/trains in itself a ‘best estimate’ assumption? There are numerous real world examples where this is not the case and there are independent failures of single software based channels/components in redundant systems.

It was suggested that for PSA in some cases it may be appropriate to further reduce the best estimate failure probability of a single simple software based smart component when modelling failure of all redundant components due to a systematic failure. However, in most cases the most straightforward approach is to assume that the software failure events will be systematic in nature. As long as these events are modelled appropriately (see Section 5.3) and assigned best estimate (as opposed to high confidence) data (see Section 5.4) then distortion of results and risk insights should be minimised.

5.6 Use of PSA to Perform Sensitivity Studies related to Software Reliability Requirements

The use of the PSA to perform sensitivity studies and understand how sensitive the overall risk picture is to changes in software reliability values is extremely powerful and was discussed throughout the project.

The adoption of a C&I fault tree model where hardware and software failure events are broken down as far as practical (such as the ‘compact model’ – see Section 5.3) facilitates a greater range of useful sensitivity studies than a model where a C&I system or function is represented by a single supercomponent or a small number of failure events. Updates to guidance should make this point clear. The presentation [REDACTED] in appendix Section 7.3.2 outlined how breaking software failures down to a finer level of detail facilitates a wider range of sensitivity analysis.

TAG-046 Paragraph 10.18 currently states:

*CBSIS reliability claims can also be used for the purposes of PSA. Evaluation of systems important to safety for PSA purposes is usually undertaken on a best estimate (50% statistical confidence level) basis. In addition, **PSA can be used to inform the design process, support the process of safety function categorisation and system***

classification, and assist in the specification of reliability targets for safety systems and safety related systems. The substantiation of computer based systems important to safety should be on a conservative, high statistical confidence, basis (i.e. 95-99%). Paragraph 10.28 provides more information.

There would be benefit in inclusion of this paragraph in TAG30. The wording could be updated to reflect that this is, in fact, an expectation (aligned with FA.14 in the SAPs). It should be noted that the adoption of 'best estimate' data for software failure in the PSA does not make the PSA any less suitable to perform sensitivity studies or inform the appropriate level of reliability or classification required in the wider deterministic case. I.e. whether a SIL 2 software failure event is included in the PSA with a failure probability of 1E-02 or 1E-03 per demand does not affect the ability to understand what impact using a range of values, including these and others, has on overall consequence frequency predictions (core damage, large release etc). In addition, sensitivity studies can be performed switching the software failure events off (i.e. a failure probability of 0) in order to obtain useful additional insights such as hardware or other failures that may have otherwise been masked by the software failures.

It would also be helpful to include high level guidance on the expectations and approaches used for feeding of such information back into the design/modification process. I.e. in cases where the PSA demonstrates that station risk is insensitive to the reliability of classified CBSIS and risk remains As Low as Reasonably Practicable (ALARP) with much lower (worse) reliability values, the deterministic requirements may be relaxed and the CBSIS reclassified as appropriate. This is particularly significant for smart components.

5.7 Discussion of Statistical Testing to Achieve 50% Confidence

The current wording in TAG-046 recognises that duty-holder's claims may be supported by probabilistic numerical claims and that these numerical claims are strengthened by the application of techniques such as statistical testing.

TAG-46 Paragraph 10.28 goes on to state that:

Where statistical testing is required as part of the equipment substantiation, this should be to a high statistical confidence level (e.g., 99%). This requires, for example, of the order of 46,000 tests with no failure for a 1E-4 pfd [Ref. 12]. Where statistical testing is

being used to determine a reliability estimate for modelling purposes (e.g., PSA), best estimate confidence may be appropriate (e.g., 50%). This requires, for example, of the order of 7,000 tests with no failure for the same pfd of 1E-4.

It will often be the case that statistical testing has been performed to support the high confidence reliability requirements of the deterministic safety case. E.g. the deterministic case requires a claim of 1E-04/demand at a high confidence, so of the order of 46,000 tests may have been performed. For the purposes of the PSA and best estimate data if the large number of tests have already been performed to support the deterministic case, more useful guidance would be by how much can the reliability be improved on a best estimate (50% confidence) basis? I.e.

$$N = -\ln(0.01)/1E-04 = 46,052 \text{ tests (1E-04/dem @ 99\% - high confidence)}$$

$$N = -\ln(0.5)/1E-04 = 6,931 \text{ tests (1E-04/dem @ 50\% confidence - "best estimate")}$$

$$-\ln(0.5)/46,052 = \mathbf{1.5E-05/dem @ 50\% confidence - "best estimate"}$$

However, it is recognised that statistical testing is just one type of independent confidence building measures (ICBM) that can provide evidence on top of production excellence assessment to support a reliability claim. The use of such ICBMs is discussed in the section below.

5.8 ICBMs and How they can Support Arguments around Software Reliability

The ONR SAPs outline, under ESS. 27, the expectation of a two-legged approach to substantiate CBSIS, i.e., production excellence (PE) assessment supported by independent confidence building measures (ICBM). The philosophy of this multi-legged approach is that substantiation of the system centres on both a demonstration of high quality production and an independent searching examination of the system's fitness for purpose that reveals no significant faults or errors that compromise the system's required safety performance.

A wide range of ICBM activity is often completed and recorded to complement the production excellence assessment and overall qualitative substantiation of CBSIS. These activities include but are not limited to:

- Device type tests
- Commissioning tests
- Examination, inspection, maintenance and testing (EIMT) records
- Data on prior use from reputable sources
- Evidence of manufacturer pedigree
- Device hardware failure modes and effects analysis
- Dynamic analysis of source code
- Static analysis of source code
- Independent desk top review of source code
- Statistical testing
- Certification by an independent body (supported by evidence)
- Independent Functional Safety Assessment (FSA)
- Independent tool review

Discussions with C&I Inspectors during the course of the project have confirmed that some ICBMs provide a more significant contribution than others in helping to build confidence in a particular reliability value being achieved, although in general a demonstration will always require ICBMs in combination. The PSA community does not generally have a feel for the relative weight each ICBM may provide to best estimate reliability estimation. Further information on this would be beneficial to aid understanding in the PSA community and to potentially include in a future update to TAG-030.

5.9 Review and Replication of Key Guidance from TAG-046 to Improve Guidance on use of Best Estimate Reliability Values

During the review of the ONR Technical Assessment Guide (TAG) for PSA (TAG-030) it was identified that TAG-030 contains very little guidance related to the keyword “software”. There are 19 instances but only one group of instances really relate to the context of software reliability data. TAG-030 is one of the key documents inspectors - and by extension PSA engineers in duty holder organisations - turn to for understanding of regulatory expectations and is currently very light on guidance on the topic of software reliability.

The totality of the current guidance on the topic of software reliability in TAG-030 is reproduced below:

*iv. Any methodologies used by licensees to estimate computer or software-based system reliability for use in PSA are expected to use **best-estimate methods** and to consider uncertainty and sensitivity. These methodologies **should meet industry accepted practices and consider the contributions of both hardware and software failures**. Estimation of software reliability should take into account influencing factors (primarily systematic) that affect the quality of the software and are informed by the specification and design of the system (e.g. considering the reliability targets for system design based on safety integrity levels in IEC 61508 or equivalent). Any dependencies introduced by the systematic nature of software failure(s) should be accounted for accordingly in the PSA. If software elements of a computer based system (e.g. operating systems, application software supporting different functions) have been individually modelled in the PSA, the dependencies between the various parts should be addressed explicitly. Any self-checking or diagnostic functions built in the computer based system should be taken into account in an adequate manner (e.g. considering the dependencies between these functions and the primary safety functions delivered by the system). The dependencies between two (or more) computer based systems should be dealt with explicitly. NSTAST-GD-046 (Ref 7.8) and IAEA report NP-T-3.27 (Ref 8.4) provide additional guidance on the assessment of reliability for a computer based system.*

While there are well established industry accepted practices for C&I hardware reliability assessment (and these are often employed in NPP PSA), the work performed during this project has not found equivalent practices for determining best estimate reliability data for software failures. This makes interpretation of this current guidance difficult. IEC 61508 provides a recognised method of deriving a high confidence upper limit estimate of software reliability, based on meeting a number of qualitative requirements, that can be successfully justified in a safety case. However, this existing IEC 61508 safety integrity level framework does not intend to provide a more precise software reliability best estimate.

TAG-030 refers the reader out to TAG-046 (Computer Based Safety Systems) for further information in a number of places. TAG-046 contains a surprising amount of guidance related to the keyword “PSA” considering its target audience of C&I (as opposed to PSA) inspectors. It is recommended that some of the PSA related content in TAG-046 is duplicated in TAG-30, in particular to recognise/re-enforce that:

- For the PSA it is appropriate to use ‘best estimate’ data as opposed to 95-99% ‘high confidence’ data for events representing software failure (TAG-046 Paragraph 5.13);
- That the above use of ‘best estimate’ data also includes that assigned to Postulated Initiating Events (PIEs) related to spurious failures of computer based systems important to safety (CBSIS) (TAG-046 Paragraph 10.20);
- In particular circumstances, it may be acceptable for duty-holders to claim a best estimate reliability of lower than 1E-4/demand for the purposes of a probabilistic safety analysis only (TAG-046 Paragraph 10.6);
- That PSA can be used to inform the design process, support the process of safety function categorisation and system classification, and assist in the specification of reliability targets for safety systems and safety related systems (TAG-046 Paragraph 10.18);
- That a duty-holder should separately model the probability of each function being delivered only if it is reasonable to claim that the system delivering each function is independent. If, however, a common cause (i.e. systematic) failure of the control system impacts on the delivery of a number of functions, as is likely if they are implemented in the same control system, then the duty holder should model the loss of all control functions as a credible simultaneous event within the PSA (TAG-046 Paragraph 10.19);
- That the number of statistical tests required to support a best estimate reliability value varies from the number required to meet a high confidence one (TAG-046 Paragraph 10.28).

During review of TAG-046 it was also noted that Paragraphs 10.14 to 10.19 appear under the heading “NUMERICAL CLAIMS (PROBABILISTIC ANALYSIS)”. It is not the intention of this PSA project to suggest updates to TAG-046. However, these paragraphs largely relate to guidance when high confidence numerical claims are made on CBSIS in the deterministic safety case. It is therefore recommended that consideration could be given to clarifying this and removing reference to the phrase “(PROBABILISTIC ANALYSIS)” to avoid any potential confusion to readers in a future update to TAG-046.

6 **References**

- /DAN22/ D. Daniels, N. Tudor: *Software Reliability and the Misuse of Statistics*, Safety-Critical Systems eJournal by the Safety-Critical Systems Club C.I.C., 2022
- /ATL21/ ATLAS Consortium: ONR Technical Support Framework, Disciple – PSA, *Provision of Technical Support to the Consideration of Realistic Software Modelling in PSA*, ONR/T774, TUV SUD NT Ref: T6837, 1st September 2021
- /NAS11/ NASA/SP-2011-3421: *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, Second Edition, December 2011
- /NAS13/ NASA/CR-2013-218111: *Context-Based Software Risk Model (CSRM) Application Guide*, Version 1.0, October 2013
- /WIK22/ Wikipedia, *Bathtub curve*, https://en.wikipedia.org/wiki/Bathtub_curve

7 Annex

7.1 Annex Task 1: Review of Documents

7.1.1 Documents Considered for the Review

Table 7-1 below provides an overview of all documents considered for the industry review in Task 1 (chapter 0). After the initial analysis of these documents (in the form of an evaluation matrix, see section 7.1.2), it was possible to identify the documents that must be considered particularly relevant for this project (Table 7-2).

Table 7-1 Complete list

Reference	Title	Industry	Country	Organisation	Year
ARP4754A	Guidelines for Development of Civil Aircraft and Systems	aerospace	international	SAE	2010
BS EN 50126-1	Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). Generic RAMS Process	railway	international	EN	2017
BS EN 50126-2	Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). Systems Approach to Safety	railway	international	EN	2017
CM9 2021/65745	A High-Level Overview of the Approaches Adopted to Assess Software Reliability	nuclear	UK	ONR	2021
Def Stan 00-55	Requirements for Safety Related Software in Defence Equipment	defence	UK	UK Ministry of Defence	2016
Def Stan 00-56	Safety Management Requirements for Defence Systems	defence	UK	UK Ministry of Defence	2018
DO-178C/ED-12C	Software Considerations in Airborne Systems and Equipment Certification	aerospace	international	RTCA EUROCAE	2012
EPRI 1016731	OPEX Insights on Common-Cause Failures in Digital C&I Systems	nuclear	USA	EPRI	2008
EPRI 1021077	Estimating Failure Rates in Highly Reliable Digital Systems	nuclear	USA	EPRI	2010
EPRI 1022986	Digital Operating Experience in the Republic of Korea	nuclear	USA	EPRI	2011

Reference	Title	Industry	Country	Organisation	Year
EPRI 1025278	Modelling of Digital Instrumentation and Control in Nuclear Power PSA	nuclear	USA	EPRI	2012
EPRI 3002002943	OPEX Review: C&I Component-Related Event Data Analysis Methodology	nuclear	USA	EPRI	2015
GUIDE YVL A.7	Probabilistic Risk Assessment and Risk Management of a Nuclear Power Plant	nuclear	Finland	STUK	2019
GUIDE YVL B.1	Safety Design of a Nuclear Power Plant	nuclear	Finland	STUK	2019
GUIDE YVL E.7	Electrical and I&C Equipment of a Nuclear Facility	nuclear	Finland	STUK	2019
IEC 61508-3	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems – Part 3: Software Requirements	general	international	IEC	2010
IEC 61513	Nuclear power plants – Instrumentation and control important to safety – General requirements for systems	nuclear	international	IEC	2011
IEEE Std 1633-2016	IEEE Recommended Practice on Software Reliability, 2016DO-178B: Software Considerations in Airborne Systems and Equipment Certification	aerospace	international	IEEE	2016
ISO 20815:2018	Petroleum, petrochemical and natural gas industries — Production assurance and reliability management	petro	international	ISO	2018
NASA-GB-8719.13	NASA Software Safety Guidebook	aerospace	USA	NASA	2004
NEA/CSNI/R(2014)16	Failure Modes Taxonomy for Reliability Assessment of Digital Instrumentation and Control Systems for Probabilistic Risk Analysis (DIGREL)	nuclear	international	OECD NEA/CSNI WGRISK	2021
NEA/CSNI/R(2021)x	Digital I&C PSA - Comparative Application of Digital I&C Modelling Approaches for PSA (DIGMAP) - in publication	nuclear	international	OECD NEA/CSNI WGRISK	2022
NKS-330	Guidelines for reliability analysis of digital systems in PSA context, Nordic nuclear safety research	nuclear	Sweden	NKS	2015
NKS-341	Software reliability analysis for PSA: failure mode and data analysis, Nordic nuclear safety research	nuclear	Sweden	NKS	2015
NKS-361	Modelling of Digital I&C, MODIG, Nordic nuclear safety research	nuclear	Sweden	NKS	2015

Reference	Title	Industry	Country	Organisation	Year
NRC BTP 7-19	Guidance for Evaluation of Defense in Depth and Diversity to Address Common-Cause Failure Due to Latent Design Defects in Digital Safety Systems	nuclear	USA	U.S. NRC	2021
NR-T-3.27	Dependability Assessment of Software for Safety Instrumentation and Control Systems at Nuclear Power Plants, IAEA Nuclear Energy Series	nuclear	international	IAEA	2018
NR-T-3.30	Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants, IAEA Nuclear Energy Series	nuclear	international	IAEA	2020
NR-T-3.31	Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial Digital Instrumentation and Control Equipment for Use in Nuclear Power Plant Applications, IAEA Nuclear Energy Series	nuclear	international	IAEA	2020
NS-TAST-GD-005	Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable), Nuclear Safety Technical Assessment Guide, Rev. 11	nuclear	UK	ONR	2020
NS-TAST-GD-030	Probabilistic Safety Analysis, Nuclear Safety Technical Assessment Guide, Rev. 7	nuclear	UK	ONR	2019
NS-TAST-GD-031	Safety Related Systems & Instrumentation, Nuclear Safety Technical Assessment Guide, Rev. 6	nuclear	UK	ONR	2018
NS-TAST-GD-046	Computer Based Safety Systems, Nuclear Safety Technical Assessment Guide, Rev. 6	nuclear	UK	ONR	2019
NUREG/CR-6901	Current State of Reliability Modelling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments	nuclear	USA	U.S. NRC	2006
NUREG/CR-6928	Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants	nuclear	USA	U.S. NRC	2007
NUREG/CR-6942	Dynamic Reliability Modelling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments	nuclear	USA	U.S. NRC	2006
NUREG/CR-6962	Traditional Probabilistic Risk Assessment Methods for Digital Systems	nuclear	USA	U.S. NRC	2008
NUREG/CR-6985	A Benchmarking Implementation of Two Dynamic Methodologies for the Reliability Modeling of Digital Instrumentation and Control Systems	nuclear	USA	U.S. NRC	2009

Reference	Title	Industry	Country	Organisation	Year
NUREG/CR-6997	Modelling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods	nuclear	USA	U.S. NRC	2009
NUREG/CR-7006	Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems	nuclear	USA	U.S. NRC	2010
NUREG/CR-7042	A Large Scale Validation of a Methodology for Assessing Software Reliability	nuclear	USA	U.S. NRC	2011
NUREG/CR-7044	Development of Quantitative Software Reliability Models for Digital Protection Systems of Nuclear Power Plants	nuclear	USA	U.S. NRC	2011
NUREG/CR-7233	Developing a Bayesian Belief Network Model for Quantifying the Probability of Software Failure of a Protection System	nuclear	USA	U.S. NRC	2018
NUREG/CR-7234	Development of A Statistical Testing Approach for Quantifying Safety-Related Digital System on Demand Failure Probability	nuclear	USA	U.S. NRC	2017
NUREG/CR-7273	Developing a Technical Basis for Embedded Digital Devices and Emerging Technologies	nuclear	USA	U.S. NRC	2021
SAPs	Safety Assessment Principles for Nuclear Facilities, 2014 Edition, Revision 1 (January 2020)	nuclear	UK	ONR	2020
SSG-39	Design of Instrumentation and Control Systems for Nuclear Power Plants	nuclear	international	IAEA	2016
TECDOC-1848	Criteria for Diverse Actuation Systems for Nuclear Power Plants, IAEA TECDOC Series	nuclear	international	IAEA	2018
TECDOC-1922	Reliability Data for Research Reactor Probabilistic Safety Assessment, IAEA TECDOC Series	nuclear	international	IAEA	2020
TF SCS	Licensing of safety critical software for nuclear reactors, Common position of international nuclear regulators and authorised technical support organisations, Revision 2021	nuclear	international	TF SCS	2021
NUREG/GR-0020	Embedded Digital System Reliability and Safety Analyses	nuclear	USA	U.S. NRC	2001
NUREG/GR-0019	Software Engineering Measures for Predicting Software Reliability in Safety Critical Digital Systems	nuclear	USA	U.S. NRC	2000

Reference	Title	Industry	Country	Organisation	Year
NUREG/CR-6848	Preliminary Validation of a Methodology for Assessing Software Quality	nuclear	USA	U.S. NRC	2004

Table 7-2 Documents with high relevance

Reference	Title	Industry	Country	Organisation	Year
EPRI 1021077	Estimating Failure Rates in Highly Reliable Digital Systems	nuclear	USA	EPRI	2010
EPRI 1025278	Modelling of Digital Instrumentation and Control in Nuclear Power PSA	nuclear	USA	EPRI	2012
IEEE Std 1633-2016	IEEE Recommended Practice on Software Reliability, 2016DO-178B: Software Considerations in Airborne Systems and Equipment Certification	aerospace	international	IEEE	2016
NASA-GB-8719.13	NASA Software Safety Guidebook	aerospace	USA	NASA	2004
NEA/CSNI/R(2014)16	Failure Modes Taxonomy for Reliability Assessment of Digital Instrumentation and Control Systems for Probabilistic Risk Analysis (DIGREL)	nuclear	international	OECD NEA/CSNI WGRISK	2021
NEA/CSNI/R(2021)x	Digital I&C PSA - Comparative Application of Digital I&C Modelling Approaches for PSA (DIGMAP) - in publication	nuclear	international	OECD NEA/CSNI WGRISK	2022
NKS-330	Guidelines for reliability analysis of digital systems in PSA context, Nordic nuclear safety research	nuclear	Sweden	NKS	2015
NKS-341	Software reliability analysis for PSA: failure mode and data analysis, Nordic nuclear safety research	nuclear	Sweden	NKS	2015
NKS-361	Modelling of Digital I&C, MODIG, Nordic nuclear safety research	nuclear	Sweden	NKS	2015
NR-T-3.27	Dependability Assessment of Software for Safety Instrumentation and Control Systems at Nuclear Power Plants, IAEA Nuclear Energy Series	nuclear	international	IAEA	2018
NR-T-3.30	Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants, IAEA Nuclear Energy Series	nuclear	international	IAEA	2020

Reference	Title	Industry	Country	Organisation	Year
NS-TAST-GD-030	Probabilistic Safety Analysis, Nuclear Safety Technical Assessment Guide, Rev. 7	nuclear	UK	ONR	2019
NUREG/CR-6962	Traditional Probabilistic Risk Assessment Methods for Digital Systems	nuclear	USA	U.S. NRC	2008
NUREG/CR-7042	A Large Scale Validation of a Methodology for Assessing Software Reliability	nuclear	USA	U.S. NRC	2011
NUREG/CR-7044	Development of Quantitative Software Reliability Models for Digital Protection Systems of Nuclear Power Plants	nuclear	USA	U.S. NRC	2011
NUREG/CR-7233	Developing a Bayesian Belief Network Model for Quantifying the Probability of Software Failure of a Protection System	nuclear	USA	U.S. NRC	2018
NUREG/CR-7234	Development of A Statistical Testing Approach for Quantifying Safety-Related Digital System on Demand Failure Probability	nuclear	USA	U.S. NRC	2017
SAPs	Safety Assessment Principles for Nuclear Facilities, 2014 Edition, Revision 1 (January 2020)	nuclear	UK	ONR	2020

7.1.2 Results of Literature Survey – Evaluation Matrix

Table 7-3 Evaluation Matrix

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
ARP4754A	Guidelines for Development of Civil Aircraft and Systems	aerospace	This document discusses the development of aircraft systems taking into account the overall aircraft operating environment and functions. This includes validation of requirements and verification of the design implementation for certification and product assurance. It provides practices for showing compliance with the regulations and serves to assist a company in developing and meeting its own internal standards by considering the guidelines herein.	This document addresses the development cycle for aircraft and systems that implement aircraft functions. It does not include specific coverage of detailed software or electronic hardware development, safety assessment processes, in-service safety activities, aircraft structural development nor does it address the development of the Master Minimum Equipment List (MMEL) or Configuration Deviation List (CDL). More detailed coverage of the software aspects of development are found in RTCA document DO-178B , "Software Considerations in Airborne Systems and Equipment Certification" and its EUROCAE counterpart, ED-12B . Coverage of electronic hardware aspects of development are found in RTCA document DO-254/EUROCAE ED-80, "Design Assurance Guidance for Airborne Electronic Hardware". Design guidance and certification considerations for integrated modular avionics are found in appropriate RTCA/EUROCAE document DO-297/ED-124. Methodologies for safety assessment processes are outlined in SAE document ARP4761, "Guidelines and

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
				Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment". Details for in-service safety assessment are found in ARP5150, "Safety Assessment of Transport Airplanes In Commercial Service" and ARP5151 Safety Assessment of General Aviation Airplanes and Rotorcraft In Commercial Service." Post-certification activities (modification to a certificated product) are covered in section 6 of this document. The regulations and processes used to develop and approve the MMEL vary throughout the world. Guidance for the development of the MMEL should be sought from the local airworthiness authority
CM9 2021/65745	A High-Level Overview of the Approaches Adopted to Assess Software Reliability	nuclear	This report provides a high-level overview of the approaches adopted by ONR to assess software reliability in regulation of the nuclear industry in the United Kingdom. This activity was prompted by a request from KAERI, in the context of a NEA/WGRISK task (DIGMAP) - see also ref. NEA/CSNI/R(2021)x.	This report provides a high level overview of the approaches adopted by ONR to assess software reliability in regulation of the nuclear industry in the United Kingdom. This activity was prompted by a request from KAERI, in the context of a NEA/WGRISK task (DIGMAP) - see also ref. NEA/CSNI/R(2021)x.
Def Stan 00-55	Requirements for Safety Related Software in Defence Equipment	defence	The first part of the Standard describes the requirements for procedures and technical practices for the development of Safety Related Software (SRS). These procedures and practices are applicable to all MOD Authorities involved in procurement through specification, design, development and certification phases of	Since the document is largely only available for a fee and was therefore not available, it is not possible to review any other parts.

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
			SRS generation, and maintenance and modification.	
Def Stan 00-56	Safety Management Requirements for Defence Systems	defence	The Standard considers a system to be a combination of elements that are used together in a defined operating environment to perform a given task or achieve a specific purpose. The elements would include personnel, procedures, materials, tools, products, facilities, services and/or data as appropriate. Whilst a contract life may be limited, application of this Standard should require consideration of the full life of the system, and for clarity, be and defined in the contract. Application of the Standard should relate to all situations and scenarios, including but not limited to trials, operations and training for operations as defined in the user requirement.	Since the document is largely only available for a fee and was therefore not available, the review is based on freely available presentation of the UK Ministry of Defence. Software and software reliability are not explicit topics of this document.
DO-178C/ED-12C	Software Considerations in Airborne Systems and Equipment Certification	aerospace	The entire DO-248C/ED-94C document (Supporting Information for DO-178C and DO-278A) falls into the "supporting information" category, not guidance.	DO-178C, the actual version of DO-178 (Software Considerations in Airborne Systems and Equipment Certification) is the primary document by which the certification authorities (e.g., FAA, EASA and Transport Canada) approve all commercial software-based aerospace systems. The Software Level, also known as the Design Assurance Level (DAL) or Item Development Assurance Level (IDAL) as defined in ARP4754 (DO-178C only mentions IDAL as synonymous with Software Level), is determined from the

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
				<p>safety assessment process and hazard analysis by examining the effects of a failure condition in the system. The failure conditions are categorized by their effects on the aircraft, crew, and passengers.</p> <p>DO-178C alone is not intended to guarantee software safety aspects. Safety attributes in the design and as implemented as functionality must receive additional mandatory system safety tasks to drive and show objective evidence of meeting explicit safety requirements. The certification authorities require and DO-178C specifies the correct DAL be established using these comprehensive analyses methods to establish the software level A-E. "The software level establishes the rigor necessary to demonstrate compliance" with DO-178C.[10] Any software that commands, controls, and monitors safety-critical functions should receive the highest DAL - Level A</p>
EN 50126-1	Railway applications — The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). Generic RAMS Process	Railway standard for RAMS	EN 50126 references EN 50128 - this is the software safety standard for railways. This reference defines the qualitative methods used to analyse software to assure a SIL (derived from IEC 61508).	EN 51028 has not been reviewed yet. It is based on the qualitative approach of IEC 61508 so there is limited benefit in carrying out a review of this reference.
EN 50126-2	Railway applications — The specification and demonstration of	Railway standard for RAMS	See above	See above

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
	Reliability, Availability, Maintainability and Safety (RAMS). Systems Approach to Safety			
EPRI 1016731	OPEX Insights on Common-Cause Failures in Digital C&I Systems	OPEX Review	EPRI 1016731 presents a detailed OPEX review of individual failures and CCFs that were potentially related to software failures. It was based on data from various databases, including INPO's OPEX data and search engine and the NRC's ADAMS database. In total 322 nuclear plant operating experience reports describing digital system events between 1987 and 2007 were evaluated.	The report does not attempt to provide an estimate of the likelihood of individual failures or CCFs due to software failures. It is intended to draw qualitative insights from the OPEX that can be used to improve measures to protect against CCFs of digital systems.
EPRI 1021077	Estimating Failure Rates in Highly Reliable Digital Systems	Methodology for estimating the reliability of Digital C&I Systems in PSA models.	<p>The first step of this methodology is to identify the critical digital failure modes in a PSA model. The non-critical digital failure modes can use a failure probability based on IEC 61508 or opex.</p> <p>For the critical digital failure modes, C&I SQEPS are required to assess the failure probability based on a number of steps documented in the method. The steps are as follows:</p> <ol style="list-style-type: none"> 1. Identification and classification of the failure mechanisms that can lead to the failure modes and digital common-cause failures determined in the PSA. 2. Development of a reliability model of the digital system (this model is separate to the PSA). 3. Identification and assessment of the 	<p>This method is highly relevant to this study.</p> <p>The method focusses effort on the most risk significant digital failure modes (as identified by the PSA), which minimises the effort involved. In addition, the proposed method is logical and relatively straightforward to understand and follow. However, the quantification is dependent, to some extent, on expert judgement and the availability of sufficient information to make a judgement. This may cause problems when being applied.</p>

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
			<p>defensive measures taken to avoid, eliminate or tolerate certain types of errors, failure modes or failure mechanisms (including common-cause failure) that could affect elements of the digital systems reliability models.</p> <p>4. Quantification of the rates of occurrence of the failure modes that could affect elements of the digital systems reliability models, and have not been rendered negligible by the defensive measures.</p> <p>5. Use of the digital systems reliability models built in Step 6 to compute the critical PSA parameters associated with the failure modes identified using the PSA</p>	
EPRI 1025278	Modelling of Digital Instrumentation and Control in Nuclear Power PSA	Methodology for estimating the reliability of Digital C&I Systems in PSA models.	<p>EPRI 1025278 is an evolution of the method introduced in EPRI 1021077.</p> <p>As per EPRI 1021077, the technique involves the identification of the digital failure modes of low importance. For the digital failure modes identified as significant, detailed analysis is required to estimate a failure probability (as described in EPRI 1021077).</p>	This method is an evolution of the method described in EPRI 1021077 (see above). It includes some further detailed guidance on the modelling of digital C&I compared to EPRI 1021077, but the method itself is largely the same.
EPRI 3002002943	OPEX Review: C&I Component-Related Event Data Analysis Methodology	OPEX review	The intent of EPRI 3002002943 was to provide information on ways to sort, filter, and combine I&C component failure data from the Institute of Nuclear Power Operations (INPO) Consolidated Events System (ICES) database. This was done to identify any trends for the data and	The report does not include any methods to estimate software reliability.

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
			determine actions to improve equipment reliability and performance based on these trends.	
GUIDE YVL A.7	Probabilistic Risk Assessment and Risk Management of a Nuclear Power Plant	nuclear	This document deals with the requirements of the development and use of the PRA: --General requirements -PRA during the design and construction licence phases of a nuclear power plant -PRA during the construction and operating licence phases of a nuclear power plant -PRA during the operation of a nuclear power plant --Contents and documentation of PRA --Risk assessments for a nuclear power plant due for decommissioning	This Guide deals with the Levels 1 and 2 of the PRA and presents requirements and guidelines for the drawing up, contents, scope and application of the PRA to light-water reactor nuclear power plants. This Guide applies to the design, construction and operating phases of a nuclear power plant. This Guide also applies to spent nuclear fuel storage in pools adjacent to the reactor and spent nuclear fuel storage in separate storages and to nuclear power plants at which power operation has ended but still contain spent nuclear fuel. Software and software reliability are not explicit topics of this document.
GUIDE YVL B.1	Safety Design of a Nuclear Power Plant	nuclear	The document describes requirements for the safety design of NPP. With regard to C&I, a few explicit requirements are also named, but specific information on software is not included.	This Guide applies to the design of a nuclear power plant and its systems important to safety. The Guide shall apply equally to the original design of the plant and any system modifications. This Guide may also be applied to the design of other nuclear facilities. 323. The facility, entities of systems, systems, components, software, auxiliary devices, parameters (settings), interfaces and their related documentation shall be defined as hierarchical configuration units. 330a. To allow efficient version management of software-based systems

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
				<p>and to manage human factors, software and hardware versions shall be provided with unique identifiers.</p> <p>5205. The safety significance of the information technology tools and testing methods (such as computational software, software compilers and testing tools) used in the design of I&C systems shall be assessed in terms of the end product being designed. The tools used in the design and implementation of safety-classified systems shall be identified. If the quality of a tool or testing method is of direct significance to the proper functioning or failure rate of the end product, it shall be validated. Detailed requirements for the validation of tools are specified in Guide YVL E.7. Each tool version shall be specifically validated.</p> <p>5236. In the design of the I&C systems, due consideration shall be given to random failures (e.g. component failures), systematic errors and failures (e.g. software errors) and any passive and active failures resulting from these.</p> <p>5414. Electrical systems and equipment utilizing software-based technology shall fulfil the requirements of Section 5.2.</p> <p>3. For I&C systems: the overall I&C system architecture, including system interfaces, connections and interaction between systems and connections to the outside environment; prioritisation of the</p>

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
				commands given by the I&C systems; equipment platforms of software-based systems complete with qualification details.
GUIDE YVL E.7	Electrical and I&C Equipment of a Nuclear Facility	nuclear	<p>This guide sets forth detailed safety requirements concerning the electrical and I&C equipment and cables of nuclear facilities, and it describes STUK's supervision and inspection related procedures.</p> <p>With regard to the qualification of safety-classified software, the following topics are described:</p> <ul style="list-style-type: none"> -General software requirements -Qualification of the system platform software and the application software -Software design procedures and processes -Software tools -Existing software -Software testing <p>No usable information is available with regard to concrete methods or reliability characteristics (concerning software).</p>	<p>This Guide sets forth detailed safety requirements concerning the electrical and I&C equipment and cables of nuclear facilities, and it describes STUK's supervision and inspection related procedures.</p> <p>This Guide applies to the electrical and I&C equipment and cables of a nuclear facility throughout its life cycle.</p> <p>338. A suitability analysis performed on an electrical or I&C equipment implemented by means of software-based technology shall cover the assessment of software and hardware.</p> <p>339. The equipment description presented in connection with the suitability analyses shall include the descriptions of any software tools used.</p>
IEC 61508-3	Functional safety of electrical/ electronic/programmable electronic safety-related systems Part 3: Software requirements	International standard on functional safety.	IEC 61508 is the international standard for functional safety. Part 3 of the standard covers safety related software. It establishes requirements for safety lifecycle phases and activities to be applied during the design and development of the safety related software. These requirements need to be met in order to justify that the overall Safety Integrity Level (SIL) of the safety related system can be	IEC 61508-3 (and IEC 61508 in general) does not present any methods for estimating software reliability. The Safety Integrity Levels (SILs) are limiting values that can be claimed provided that the requirements of the standard are met. The standard includes quantitative methods for estimating random errors, but states that for systematic errors (including software failures) 'qualitative techniques and

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
			<p>met.</p> <p>It also includes a detailed list of techniques to be used during the development of the safety related software. These techniques are classified depending on their suitability for the different safety integrity levels.</p>	<p>judgements have to be made to achieve the required safety integrity'.</p> <p>SIL values are often used to represent software failure probabilities in PSA models. Therefore, even though this standard does not present any suitable methods for estimating software reliability, it is important to understand it and what the SIL values represent.</p>
IEC 61513	Nuclear power plants – Instrumentation and control important to safety – General requirements for systems	Nuclear industry specific standard on functional safety.	<p>IEC 61513 provides the interpretation of the general requirements of IEC 61508-1, 61508-2 and 61508-4 for the nuclear industry. IEC 60880 and 62138, which sit beneath IEC 61513, provide the interpretation of IEC 61508-3 (which covers software safety requirements) for the nuclear industry.</p> <p>IEC 61513 uses the categorisation of safety functions and classification of safety systems whereas IEC 61508 uses SIL values to determine the level of assurance required and the level of reliability achievable. The categorisation of safety functions (and corresponding classification of a safety system) is based on a deterministic assessment in the nuclear industry (as per IAEA Safety Guides and IEC 61226) while the SIL requirements are based on a quantitative measure of the risk reduction required, e.g. the output of a LOPA.</p>	IEC 61513 states that the reliability of the functions performed by the safety system shall be assessed. It goes on to state that the contribution of hardware failures to the reliability of a function shall be determined by a quantitative assessment, whereas the contribution of software failures to the reliability of a function shall be determined by a qualitative assessment.

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
IEEE Std 1633-2016	IEEE Recommended Practice on Software Reliability, 2016DO-178B: Software Considerations in Airborne Systems and Equipment Certification	aerospace	<p>This publication provides guidance for employing software reliability analyses. It provides information necessary for the application of software reliability and establishes the basic principle for collecting the data needed to assess and predict the reliability of software:</p> <ul style="list-style-type: none"> - models for predicting software reliability - methods to analyse software failure modes and failures effects - ability to assess the reliability of COTS - procedures with checklists and examples. <p>Although there are some distinctive characteristics of aerospace software, the principles of reliability are generic, and the results can be beneficial to software reliability engineering (SRE) in any industry. The American Institute of Aeronautics and Astronautics defines SRE as “the application of statistical techniques to data collected during system development and operation to specify, predict, estimate, and assess the reliability of software-based systems.”</p>	<p>The methods for assessing and predicting the reliability of software, based on a life-cycle approach to software reliability engineering (SRE), are prescribed in this recommended practice:</p> <ul style="list-style-type: none"> - Software Failure Mode and Effect Analysis (SFMEA); examples of SFM: faulty sequencing, faulty timing, faulty data, faulty functionality, - Software Defect Root Cause Analysis (e.g. faulty requirements, faulty implementation, faulty source and version control, faulty usability), - Software reliability prediction models, - Software reliability growth models - Software Fault Tree Analysis (FTA): software fault tree should be part of an overall system FTA, - Sensitivity analysis, - Usage of reliability metrics, - Development of reliability tests and measure test coverage, - Increase test coverage via fault injection, - Failure Reporting and Corrective Action Systems (Fracas). <p>This document provides also a table of actual software reliability values based on the size of the software and the number of installed sites.</p>
ISO20815	Petroleum, petrochemical and natural gas industries — Production assurance and reliability management	Generic standard on production assurance and reliability	Provides very limited description of dealing with software reliability	Describes the use of FMECA or FTA to identify critical software elements then refers to the use of 61508 to assess the software reliability.

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
		management for the petrochemical industry		The standard does not include any detailed information/methods.
NASA-GB-8719.13	NASA Software Safety Guidebook	C&I of generic spacecraft	<p>The document discusses pro and cons of different methodologies for the software assessment during whole life cycle of the digital C&I and provides also benefit rating of the analysis methods. The presented analysis techniques can be divided into two categories:</p> <ol style="list-style-type: none"> 1. Top down system hazards and failure analyses, which look at possible hazards or faults and trace down into the design to find out what can cause them. 2. Bottom up review of design products to identify failure modes not predicted by top down analysis. This analysis ensures the validity of assumptions of top down analysis, and verifies conformance to requirements. <p>NASA provides also guidance on tailoring the number of analyses required to match the risk of the software hazards.</p>	<p>Safety assessment are integral parts of the software life-cycle, from the specification of safety-related requirements, through inspection of the software-based control equipment, and into verification testing for hazards.</p> <p>Verification & Validation (V&V) is a system engineering process employing a variety of software engineering methods, techniques, and tools for evaluating the correctness and quality of a software product throughout its life cycle. This document provides analyses, methods and guidance which can be applied during each phase of the software life cycle:</p> <ul style="list-style-type: none"> - Software Fault Tree Analysis, - Software Failure Modes and Effects Analysis, - Requirements State Machine, - Preliminary Hazard Analysis and - Reliability modelling. <p>NASA, based on extensive experience with spacecraft flight operations, has established in this guidebook levels of failure tolerance based on the hazard severity level necessary to achieve acceptable levels of risk.</p>
NEA/CSNI/R(2014)16	Failure Modes Taxonomy for Reliability Assessment of Digital Instrumentation	Generic digital C&I of a NPP	DIGREL Task Group has develop a taxonomy failure modes of digital components of digital C&I systems for the	The taxonomy approach represents a framework for definition and classifying failure modes associated with a system.

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
	and Control Systems for Probabilistic Risk Analysis (DIGREL)		<p>purposes of probabilistic risk analysis (PRA) for NPPs. This report provides basic principles for comprehensive evaluation of probable failure modes of digital C&I systems:</p> <ul style="list-style-type: none"> - definition of hierarchical abstraction levels for model-based FMEA, - survey results of failure modes applied for digital C&I systems. 	<p>Important requirements of a FMEA in supporting PRA modelling include completeness of failure modes, failure effects are clearly defined, and possibility for quantification of the associated failure rates and probabilities.</p> <p>In addition, the report provides an approach to consider the software of digital C&I systems in reliability analysis:</p> <ul style="list-style-type: none"> - decomposition of the entire software into functional modules, - modelling of the failures of individual modules - development of specific CCF model. <p>The report provides also an example for modelling of safety relevant C&I system including software for the PRA. Furthermore, there is explained an approach for the analysis of the fault activation and propagation (Failure model for hardware and software).</p>
NEA/CSNI/R(2014)16	Failure Modes Taxonomy for Reliability Assessment of Digital Instrumentation and Control Systems for Probabilistic Risk Analysis (DIGREL)	nuclear	<p>Each participant developed its own PSA model based on the reference case. Through the modelling effort and comparison, various approaches and valuable insights for future modelling method development were identified. The main goals of this task identified in the proposal were:</p> <ul style="list-style-type: none"> - To compare the developed PSA models concerning methods used, level of details, quantification issues, and consideration of specific features of digital technology; 	<p>In June 2017, the Committee on the Safety of Nuclear Installations (CSNI) approved the Working Group on Risk Assessment (WGRISK) activity on Digital I&C PSA – Comparative Application of Digital I&C Modelling Approaches for PSA (DIGMAP), as a step towards establishing internationally well-agreed methods for DI&C modelling in PSA. The objective of this study was to compare modelling approaches for DI&C systems important to safety in an exemplary NPP (reference case) for the purpose of PSA. Each</p>

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
			<p>- To identify possible modelling methods and issues for further development. The task group translated these goals into four objectives:</p> <ul style="list-style-type: none"> - Comparison of different approaches for PSA modelling of DI&C systems; - Identification of main contributors to the core damage frequency (CDF) and to safety signal failure; - Evaluation of the effect of important parameters and assumptions on the risk through sensitivity analysis; - Identification of key areas for future research. 	<p>participant developed its own PSA model based on the reference case.</p>
NKS-330	Guidelines for reliability analysis of digital systems in PSA context, Nordic nuclear safety research	nuclear	<p>This report provides similar to DIGREL project of OECD/NEA an example based guidance for considering digital C&I in the PSA:</p> <ul style="list-style-type: none"> - Taxonomy results of DIGREL project, - Guidelines for failure modes analysis and fault tree modelling of digital I&C, - Approach for modelling and quantification of software. 	<p>This report provides guidelines regarding level of abstraction in system analysis and screening of components, failure modes and dependencies. It presents also an approach for modelling and quantification of software and of common cause failures (CCF) between components of the safety C&I.</p> <p>The annexes of the report provide description of an example PSA model (simplified boiling water reactor, safety digital C&I system, some support systems), results of the FMEA of C&I components, assumed software failures, CCF groups.</p> <p>Quantification was made based on</p> <ul style="list-style-type: none"> - Safety system equipment: Generic data (T-book) - IE frequencies : Assumed based on Nordic operating experience

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
				<ul style="list-style-type: none"> - Digital I&C hardware: Fictive data, engineering judgement - Digital I&C hardware CCF: Generic data (NUREG/CR-5497) - Digital I&C software: Assumed based on engineering judgement
NKS-341	Software reliability analysis for PSA: failure mode and data analysis, Nordic nuclear safety research	nuclear	<p>This report proposes a method for quantification of software reliability for the purpose PSA for nuclear power plants, developed in the Nordic DIGREL project (see also NKS-330 report).</p> <p>The engineering judgement approaches used in PSA can be divided into the following categories depending on the argumentation and evidence they use:</p> <ul style="list-style-type: none"> - screening out approach - screening value approach - expert judgement approach - operating experience approach. <p>The reliability model used for software failures is practically always the simple “probability of failure per demand”</p>	<p>The outlined approach to quantify software reliability is an attempt to demonstrate how evidence can be provided for PSA. The research report suggests a numerical scheme to correlate between the metrics and failure probability, in terms of a “shaping factor” for quantification of software failures. The resulting value is assumed to include all failure modes (fatal failure, no actuation, spurious actuation). Expert judgement is considered to estimate the fractions of different failure modes.</p> <p>The quantification values obtained with the proposed quantification method have not been validated, and there are a number of technical issues which require further justification.</p> <p>The appendixes of the report provide some interesting information concerning quantification of software failures:</p> <ul style="list-style-type: none"> - Software complexity analysis, - Justification of failure fractions of application software failures, - Estimation of number of demands to the TXS-based I&C systems, - Description of an example PSA model.

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
NKS-361	Modelling of Digital I&C, MODIG, Nordic nuclear safety research	Reliability analysis of software in nuclear facilities	NKS-361 presents an evolution of the approach proposed in NKS-341.	<p>The proposed approach breaks down software failures into operating system or application specific levels.</p> <p>Operating system failure probabilities are estimated based on OPEX.</p> <p>Application specific failure modes are further divided into fatal and non-fatal failure modes. A fatal failure will affect all ongoing processes and therefore will affect all applications running on the same processor. A non-fatal failure only affects the output of the current application software.</p> <p>Unlike NKS-341, the updated approach in NKS-361 proposes that fatal failure probabilities are estimated based on OPEX for the processors being used. Non-fatal failures are estimated based on engineering judgement. The engineering judgement uses the same process as NKS-341, i.e. a Bayesian Belief Network using V&V class, software complexity and OPEX (where available) as evidence. The judgement of complexity is based on a modified version of the SICA flow diagram, also used in NKS-341.</p>
NRC BTP 7-19	Guidance for Evaluation of Defense in Depth and Diversity to Address Common-Cause Failure Due to Latent Design	nuclear	The guidance in this Branch Technical Position is intended for staff reviews of I&C safety systems proposed (1) in requests for license amendments as modifications to	The report does not include any methods to estimate software reliability.

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
	Defects in Digital Safety Systems		licensed NPPs, or (2) in applications for CPs, OLs, COLs, DCs, SDAs, and MLs.	
NR-T-3.27	Dependability Assessment of Software for Safety Instrumentation and Control Systems at Nuclear Power Plants, IAEA Nuclear Energy Series	nuclear	<p>The objective of this IAEA report is to provide an overview of the current knowledge, best practices, experience, benefits and challenges regarding the evaluation and assessment of software used in NPP safety I&C systems. In this report, software dependability is defined as the extent to which reliance can justifiably be placed on software, in the framework of the system architecture or, more specifically, in the context of the system function.</p> <p>This report presents an assessment framework based on the following:</p> <ul style="list-style-type: none"> - principles and overall strategy to guide the assessment that considers the behaviour of the system as well as its interactions, vulnerabilities and compliance with standards; - an approach to developing and communicating the assessment based on claims, arguments and evidence (CAE); - Guidance on a high level process for deploying the framework with guidance on specific issues. 	<p>This report provides a framework for the dependability assessment of software in safety systems. Report provides examples of techniques of generating evidence and compliance with standards, validation, software analysis techniques, and also includes insights from operational experience. The main approach is usage of CAE concept in each phase of dependability of the software. This report describes briefly techniques of generating evidence for the various dependability claims:</p> <ul style="list-style-type: none"> - Operational experience: the trustworthiness could be established by an analysis of the procedures used for collecting the operational experience (report refers to IEC 60880 and other guidance documents); - Compliance and quality assurance (report refers to IEC, IEEE standards and other guidance documents); - Functional validation: modelling and simulation techniques, Functional FMEA, FTA, HAZOP, System-theoretic process analysis (STPA) - Software analysis techniques: formal verification (e.g. model checking), static analysis - Testing: functional testing, negative testing, statistical testing, fault injection; - Inspection and reviews.

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
				This report provides description of some approaches for quantification of software reliability based on statistical testing, analysis of prior operational experience, worst case bound theory, estimation approaches. Furthermore the report examples of vulnerabilities and challenges based on nuclear industry experience.
NR-T-3.30	Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants, IAEA Nuclear Energy Series	nuclear	The objective of this report to support the application of computer security concepts and measures to provide protection from cyberattacks for C&I systems at NPPS. It discusses the benefits and challenges of the various methods.	The report provides some useful information concerning security aspects of the software-based application of the functions of the C&I systems: - software modifications (e.g. via removable data, via external interface); - data communication: network topology design, access control, configuration management using hardware and software; - recommendations for essential data collection. Further the report provides some information regarding methods for security assessment of digital C&I, e.g. - attack surface modelling (e.g. EPRI approach); - threat modelling. Important issue is to establish adequate V&V process for hardware and software of digital C&I for security reason.
NR-T-3.31	Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial	nuclear	Main objective of this publication to provide guidance on the requirements for justification usage of digital Commercial Off The Shelf (COTS) equipment in nuclear	This report provides detailed explanation of justification process for COTS including software. In the appendices are presented some

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
	Digital Instrumentation and Control Equipment for Use in Nuclear Power Plant Applications, IAEA Nuclear Energy Series		safety applications. The report presents also challenges in the use of the COTS: - specific hardware and software vulnerabilities; - complexity of the components, multifunctions; - generic and limited justification/qualification; - change and obsolescence management (e.g. software update, version control, undeclared changes). Report makes an important statement, that the acceptability of a digital COTS device for a nuclear application needs to address both nuclear safety and security.	examples of licensing practices in different countries (Canada, USA, Switzerland etc.) for the of the COTS equipment. One appendix serves as a reference to available failure analysis tools and techniques (e.g. FMEA, FTA, HAZOP) that can be used during the design process to define design requirements associated with defensive measures and diagnostics, to identify hazards and failure mechanisms that could lead to failure of the performance of a safety function and to prevent unintended functions.
NS-TAST-GD-005	Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable), Nuclear Safety Technical Assessment Guide, Rev. 11	ALARP guidance	This is a guidance document for ONR inspectors to help them judge whether a licensee has met the requirements to reduce risk to ALARP.	This TAG does not include any specific guidance related directly to the estimate of software reliability for use in a PSA model.
NS-TAST-GD-030	Probabilistic Safety Analysis, Nuclear Safety Technical Assessment Guide, Rev. 7	PSA guidance	This TAG provides an interpretation of the SAPs related to PSA and specific guidance to inspectors when assessing a PSA or PSA related submission. It states the following: iv. Any methodologies used by licensees to estimate computer or software-based system reliability for use in PSA are expected to use best-estimate methods and to consider uncertainty and sensitivity. These methodologies should meet industry	The TAG refers to NSTAST-GD-046 and IAEA report NP-T-3.27 for additional guidance on the assessment of reliability for a computer based system.

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
			<p>accepted practices and consider the contributions of both hardware and software failures. Estimation of software reliability should take into account influencing factors (primarily systematic) that affect the quality of the software and are informed by the specification and design of the system (e.g. considering the reliability targets for system design based on safety integrity levels in IEC 61508 or equivalent). Any dependencies introduced by the systematic nature of software failure(s) should be accounted for accordingly in the PSA. If software elements of a computer based system (e.g. operating systems, application software supporting different functions) have been individually modelled in the PSA, the dependencies between the various parts should be addressed explicitly. Any self-checking or diagnostic functions built in the computer based system should be taken into account in an adequate manner (e.g. considering the dependencies between these functions and the primary safety functions delivered by the system). The dependencies between two (or more) computer based systems should be dealt with explicitly. NSTAST-GD-046 (Ref 7.8) and IAEA report NP-T-3.27 (Ref 8.4) provide additional guidance on the assessment of reliability for a computer based system.</p>	

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
NS-TAST-GD-031	Safety Related Systems & Instrumentation, Nuclear Safety Technical Assessment Guide, Rev. 6	Safety Related Systems and Safety Instrumentation guidance for ONR inspectors	This TAG provides guidance to aid Inspectors in the interpretation and application of SAPs related to, the assessment of nuclear licensees' safety submissions in the area of Safety Related Systems (SRS) and Safety Related Instrumentation (SRI).	This TAG does not include any specific guidance related directly to the estimate of software reliability for use in a PSA model.
NS-TAST-GD-046	Computer Based Safety Systems, Nuclear Safety Technical Assessment Guide, Rev. 6	Computer Based Safety Systems guidance	This TAG provides additional guidance for applying SAP ESS.27. ESS.27 presents the elements of a multi-legged procedure that should be used to demonstrate the adequacy of a computer-based safety system.	Appendix 4 provides detailed guidance on the software substantiation of Computer Based Systems Important to Safety (CBSIS). This includes guidance on the substantiation of numerical claims, which covers both deterministic assessments (90-95% confidence levels (i.e. high confidence values)) and PSA (50% statistical confidence level (i.e. best estimate values)). It does not mandate any particular technique to substantiate these values, but does present statistical testing as a technique that can be used, stating the following, 'Where statistical testing is being used to determine a reliability estimate for modelling purposes (e.g. PSA), best estimate confidence may be appropriate (e.g. 50%). This requires, for example, of the order of 7,000 tests with no failure for the same pfd of 1E-4.'
NUREG/CR-6848	Preliminary Validation of a Methodology for Assessing Software Quality	nuclear	This report summarizes the results of research conducted by the University of Maryland to validate a method for predicting software quality. The method is termed the Reliability Prediction System	The application under validation, Personnel entry/exit ACcess System (PACS), is a simplified version of an automated personnel entry access system that controls physical access to

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
			<p>(RePS). The RePS methodology was initially presented in NUREG/GR-0019. The current effort is a preliminary validation of the RePS methodology with respect to its ability to predict software quality (measured in this report and in NUREG/GR-0019 in terms of software reliability) and, to a lesser extent, its usability when applied to relatively simple applications.</p>	<p>rooms/buildings, etc. This system shares some attributes of a reactor protection system, such as functioning in real-time to produce a binary output based upon inputs from a relatively simple human-machine interface with an end user/operator. PACS's reliability (ps) was assessed by testing the software code with an expected operational profile. The testing process involves: developing a test oracle using Test Master, a tool that generates test scripts in accordance with the operational profile; executing the test scripts using WinRunner, the test harness that also records the test results; and calculating the reliability of PACS using the recorded results.</p> <p>This research gives preliminary evidence that the rankings of software engineering measures in the form of RePSs can be used for assessing the quality of software in safety critical applications. The rankings are based on expert opinion, as described in NUREG/GR-0019.</p> <p>Further validation effort is planned and will include data from the entire software development life cycle of a larger scale software product, preferably a highly reliable application of requisite complexity. This larger-scale validation effort will demonstrate the efficacy of the RePS</p>

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
				methodology to predict software quality of nuclear safety-related systems.
NUREG/CR-6901	Current State of Reliability Modelling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments	nuclear	<p>NUREG 6901 describes issues that need to be addressed both in the reliability modelling of digital instrumentation and control systems and in the incorporation of the digital C&I system reliability models into existing PRA models. The report also outlines the acceptance criteria to be used for digital C&I system models prior to the implementation in regulatory applications.</p> <p>Interactions are categorised into two groups: Type I and Type II. Type I are dynamic interactions between the reactor protection and control systems and controlled plant physical processes (e.g. heat up, pressurization). Type II interactions are between components of the reactor protection and control systems themselves (e.g. communication between different components, multi-tasking, multiplexing).</p> <p>The NUREG states that numerous concerns have been raised about the capability of the ET/FT approach to treat the coupling between the plant physical processes and triggered or stochastic logical events (e.g. valve openings, pump start-ups) that may arise due to Type I and Type II interactions</p>	<p>NUREG 6901 concludes that reliability modelling of digital C&I systems cannot be addressed purely in terms of hardware and software. The reliability model needs to account for the possible dynamic interactions among the digital C&I system components, as well as between the controlling (supervising) system and controlled (supervised) process.</p> <p>None of the identified methods satisfy all of the requirements described above. However, the dynamic flowgraph methodology (DFM) and Markov/ Cell-to-Cell mapping technique (CCMT) methodologies rank as the top two with most positive features and least negative or uncertain features when evaluated against the stated requirements for the reliability modelling of digital C&I systems. The CCMT is a type of continuous time Markov model which operates by considering transition between defined states.</p> <p>Regarding the applicability of the conventional Event Tree (ET)/Fault Tree (FT) approach to digital C&I systems, no actual comparisons to dynamic methodologies have been encountered in the literature. The extrapolation of existing computational evidence based on a few</p>

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
				<p>comparative studies on dynamic systems seems to indicate that the ET/FT approach may yield satisfactory results when a digital C&I system does not involve certain features listed in the document.</p> <p>In cases where certain features are involved, the ET/FT approach has been found to overestimate the predicted Top Event frequencies and this can be large - up to an order of magnitude. The ET/FT approach may also not be able to identify possible dependencies between failure events due to the omission of some failure mechanisms.</p>
NUREG/CR-6928	Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants	nuclear	There is no specific reference to DCI reliability estimation in NUREG 6928. The report characterises current industry-average performance for components and initiating events at U.S. commercial nuclear power plants. Studies have indicated that industry performance has improved since the 1980s and early 1990s. Typically data for 1998-2002 were used to characterize current industry-average performance. Four types of events are covered: component unreliability (e.g. pump fail to start or fail to run), component or train unavailability resulting from test or maintenance outages, special event probabilities covering operational issues (e.g. pump restarts and injection valve re-openings during unplanned demands) and initiating event frequencies.	The report does not include any methods to estimate software reliability.

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
NUREG/CR-6942	Dynamic Reliability Modelling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments	nuclear	<p>NUREG 6942 follows on from NUREG 6901. The main objective of the report is to illustrate the implementation of the dynamic flowgraph methodology (DFM) and Markov/Cell-to-Cell mapping technique (CCMT) methodology on a system representative of the digital C&I systems used in nuclear power plants.</p> <p>Dynamic modelling is used to address concerns raised in NUREG 6901 involving the conventional ET/FT methodology which may not yield satisfactory results when a digital C&I system:</p> <ul style="list-style-type: none"> - Interacts with a process that has multiple Top Events, logic loops and/or substantial time delay between the initiation of the fault and Top Event occurrence; - Relies on sequential circuits which have memory; - Has tasks which compete for the C&I system resources; - Anticipates the future states of controlled/monitored process. <p>An example of a feed water system is described and FMEA findings are summarised. The two methods (DFM and Markov/CCMT) are then used to model the system and the results are discussed along with models into the Example Plant PRA model.</p>	<p>The document identifies a number of challenges with the DFM and CCMT methods. One of these is that there is no consensus in the technical community on how software reliability should be quantified and in fact whether such a concept is appropriate at all. However, the proposed methodologies can be used to obtain qualitative information on the failure characteristics of digital I&C systems (i.e. prime implicants) as well as quantitative, and, in that respect, can be helpful in the identification of risk important event sequences even if the data issue is not resolved.</p> <p>The report does not include any methods to estimate software reliability</p>

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
NUREG/CR-6962	Traditional Probabilistic Risk Assessment Methods for Digital Systems	nuclear	<p>NUREG 6962 is a sister document to NUREG 6942 and considers the use of traditional (non-dynamic) methods. It covers capabilities and limitations of using traditional reliability modelling methods to develop and quantify digital system reliability models. In particular it covers the following four areas:</p> <ol style="list-style-type: none"> 1. Develop a set of desirable characteristics for reliability models of digital systems that could provide input to the technical basis for risk evaluations related to current and new reactors; 2. Comparison of two traditional reliability methods and apply them to two example digital systems to determine the capabilities and limitations of these methods; 3. Compare the resulting digital system reliability models to the set of desirable characteristics to identify areas where additional research might improve the capabilities of the methods; 4. Develop a method, if necessary, for integrating the digital system reliability models into a NPP Probabilistic Risk Assessment (PRA). 	<p>Section 8.2 outlines Issues in Digital System Data Analyses and states the following for the topic Software Failures:</p> <p><i>A unique feature of digital systems is the use of software. It is known that software can fail resulting in failure of the digital component it supports. Software failure may be separately modelled in the system reliability model and quantified based on available data. For example, Teleperm XS modules have reported 5260 module years of operating experience [Niedzballa 2004], which is useful in estimating the failure rate of the platform software. The estimation of the software reliability parameters should be consistent with the model being used. It is possible that in some databases, some software-induced hardware failures may not be attributed to failure of the software. Without knowing how software failure is treated in the data, digital system reliability modelling may be difficult.</i></p> <p>Section 8.3.3 covers the PRISM database. PRISM is a software tool developed by the Reliability Analysis Center (RAC) for assessing system reliability. PRISM provides a method (known as the RACRates model) for determining software failure rates at the system level using the capability maturity model (CMM) of the Software Engineering Institute of Carnegie Mellon University. Basically, the CMM level</p>

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
				<p>or other measures (e.g., RTCA safety level [RTCA 1992] and ISO 9000 [ISO 2000] certification) is converted into the number of faults per thousand lines of code, which in turn is converted into mean time to failure using a reliability growth model. The PRISM method is described in more detail in the PRISM User's Manual [RAC PRISM].</p> <p>Section 10.7 presents some recommendations for further research and includes the following:</p> <ul style="list-style-type: none"> - Methods for estimating the risk from software faults in both application and support software. - Methods for modelling software CCF across system boundaries (e.g., due to common support software).
NUREG/CR-6985	A Benchmarking Implementation of Two Dynamic Methodologies for the Reliability Modeling of Digital Instrumentation and Control Systems	nuclear	NUREG 6985 builds on NUREG 6942 and discusses two dynamic methodologies, DFM and the Markov/CCMT, implemented on the benchmark Digital Feedwater Control System (DFWCS). The results obtained from the DFM and Markov/CCMT models of the DFWCS failure modes are compared. The study shows that a DFWCS similar to that of an operating plant can be modelled using dynamic methodologies and that the results can be incorporated into an existing PRA to quantify the impact of a digital upgrade on the plant CDF. NUREG 6985 defines dynamic methods as	<p>Shortcomings raised in NUREG 6942 and addressed in this report include:</p> <p>Concern 3 - Impact of the hardware/software/firmware and process interactions on the risk significant events under consideration (in view of the fact that no comparison of dynamic versus traditional PRA approach results were available for the system and scenario considered).</p> <p>The question at the core of Concern 3 (Impact of hardware/ software/ firmware interactions on risk-significant events) has</p>

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
			<p>those that attempt to explicitly model the interactions between a digital instrumentation and control system and the plant physical processes.</p> <p>Possible shortcomings with the FT/ET method, first raised in NUREG 6901, are covered, considering the same issues of a digital C&I system considered in NUREG-6942, discussed above.</p>	<p>been addressed in previous work by several researchers in the field. However, no conclusive results regarding Concern 3 have been reached at the time of this publication.</p> <p>The report does not include any methods to estimate software reliability</p>
NUREG/CR-6997	Modelling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods	nuclear	<p>NUREG 6997 builds on work of NUREG 6962, which documented initial Brookhaven National Laboratory (BNL) work in this area, including developing desirable characteristics for evaluating reliability models of digital systems and establishing the process for performing a reliability study of a DFWCS using two traditional reliability modelling methods.</p> <p>NUREG 6997 documents the application of these methods to the DFWCS. This report also compares the resultant models to the desirable characteristics identified in NUREG 6962 to identify areas where additional research could potentially improve the quality and usefulness of digital system reliability models.</p>	<p>This project generally did not involve advancements in the state of the art, such as detailed analysis and quantification of software reliability.</p> <p>Section 9.3 states "Quantitative software reliability is beyond the scope of this study. Nevertheless, the FMEA and reliability model consider some basic software failures, such as common cause failure (CCF) of the software of the main and backup CPUs. Two types of software failure modes are considered: software continues running but generates erroneous results, and software stops running. In addition, the simulation model accounts for the performance of software given the occurrence of one or more component failures.</p> <p>It should be pointed out that a commonly accepted basis for modelling software failures probabilistically has not been established yet and additional research is</p>

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
				needed, although it seems to be supported by previous work in Chu [2006]."
NUREG/CR-7006	Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems	nuclear	This report is a compilation of safe field-programmable gate array (FPGA) design practices that can be used by NRC staff as guidance for reviewing FPGA-based safety systems in nuclear power plants. It can also serve as a basis for development of specific activities that will support the licensing process such as FPGA-specific review procedures and acceptance criteria. The report follows on the investigation of existing regulatory documents and standards related to design and review of safety-related FPGA systems. Since the existing regulatory documents are not specific about FPGA design practices, this report also serves as the complement to the standards that cover general issues related to digital and software safety systems in nuclear power plants	The report does not include any methods to estimate software reliability.
NUREG/CR-7042	A Large Scale Validation of a Methodology for Assessing Software Reliability	nuclear	<p>This report summarizes the results of a research program initiated by the U.S. Nuclear Regulatory Commission at the University of Maryland to validate a method for predicting software reliability.</p> <p>The method is termed the Reliability Prediction System (RePS). The RePS methodology was initially presented in NUREG/GR-0019, "Software Engineering Measures for Predicting Software Reliability in Safety Critical Digital Systems" and validated on a small control</p>	The objective of this research was to perform a large-scale validation of the methodology proposed in NUREG/GR-0019 and apply it to a nuclear-safety application. This was done by applying the methodology to a set of twelve, pre-determined software engineering measures (including five of the six measures that served in the initial validation study described in NUREG/CR-6848). RePSs are developed for these twelve measures for all life-cycle phases. In this research, the application of the

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
			<p>system application with a set of five RePSs in NUREG/CR-6848, "Validation of a Methodology for Assessing Software Quality." The current effort is a validation of the RePS methodology with respect to its ability to predict software quality (measured in this report and in NUREG/GR-0019 in terms of software reliability) and, to a lesser extent, its usability when applied to safety-critical applications.</p>	<p>RePSs to a nuclear power plant reactor safety-control system (Plant X) was limited to the testing phase because the post-mortem nature of the study did not allow reconstruction of the required state of the application throughout the development life-cycle. Such validation helps determine the predictive ability and practical applicability of the methodology to the nuclear power industry.</p> <p>The research described in this report provides evidence that twelve selected software engineering measures in the form of RePSs can be used (with different degrees of accuracy) to predict the reliability of software in safety-critical applications. These twelve measures are ranked based on their prediction ability. The rankings are then compared with those obtained through an expert opinion elicitation effort, as described in NUREG/GR-0019, and with those obtained through a small-scale validation, as described in NUREG/CR-6848</p>
NUREG/CR-7044	Development of Quantitative Software Reliability Models for Digital Protection Systems of Nuclear Power Plants	nuclear	<p>Subsequent to NRC's Advisory Committee on Reactor Safeguards Subcommittee on Digital C&I Systems, BNL reviewed a spectrum of quantitative software reliability methods (QRSMs) to catalogue potential methods that can serve to quantify software failure rates and per-demand failures. Software failure can be defined as not successfully performing a</p>	<p>Various QSRMs are discussed and compared against a list of ten desirable characteristics.</p> <p>No QRSM met the complete set of desirable characteristics, and no single method clearly stands out as the most appropriate. However based on a review the QRSMs selected as candidates for</p>

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
			<p>specified/intended function or performing unintended actions. A software failure occurs when some inputs to the software occur and interact with the internal state of the digital system to trigger a fault that was introduced into the software at some point during the software lifecycle (including faults that result from incomplete or incorrect requirements and specifications).</p> <p>The study documented in NUREG CR-7044 continued the preceding work on software reliability by selecting candidate QSRMs and further developing them in preparation for a case study of the selected method(s). The actual case study(s) will be documented in a separate report.</p>	<p>further consideration included:</p> <ul style="list-style-type: none"> - Software Reliability Growth Methods; - Bayesian Belief Network (BBN) Method; - Statistical testing methods (Test-based Methods and Metrics-Based Methods). <p>Statistical testing was concluded to be the most practical approach for quantifying the probability of failure on demand of a protection system. However, it involves testing the software over many possible inputs, defined by the software's operational profile. Since the number of inputs can be very large, testing the software in this way entails undertaking an extremely large number of tests, with the consequent costs in time, money, and effort.</p>
NUREG/CR-7233	Developing a Bayesian Belief Network Model for Quantifying the Probability of Software Failure of a Protection System	nuclear	<p>A new approach has been developed to quantify the software failure probabilities in nuclear power plant (NPP) digital instrumentation and control (I&C) systems. Specifically, this approach uses a Bayesian belief network (BBN) to model the causal relationships between the software development life cycle, the number of residual defects within software, and the software failure probability.</p> <p>The software development life cycle (SDLC) characteristics (e.g., development quality and verification and validation (V&V) quality), and software-self</p>	<p>Three rounds of expert elicitation were used to complete the BBN model. The first two rounds used experts with knowledge and experience in the general application of software quality assurance to assist in the identification of BBN nodes, the construction of the BBN model structure (the causal relationship), and the establishment of the Node Probability Tables (NPTs) (the causal relationship quantification). The NPTs were further Bayesian updated using literature data available from the literature and the limited amount of development and V&V data. The</p>

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
			<p>characteristics (e.g., size and complexity) are represented using a hierarchical structure. As part of the BBN model development, the SDLCs were classified into five phases: requirements, design, implementation, testing, and installation/checkout. Information for each phase (or activity) was abstracted from the relevant guidance and standards documents. A BBN sub-model was then developed for each phase to estimate the number of software defects remaining.</p>	<p>insights gained from these elicitations were used to develop a BBN model for NPP digital safety software.</p> <p>The outputs from the third round of elicitations were used as inputs to the BBN model applications to two trial nuclear systems: (1) the Loop Operating Control System (LOCS) of the Advanced Test Reactor (ATR) at Idaho National Laboratory, and (2) the prototype Integrated Digital Protection System-Reactor Protection System (IDiPS-RPS) developed by the Korea Atomic Energy Research Institute (KAERI).</p> <p>Experts who are familiar with the software development, including V&V activities, of the two trial systems provided these inputs. The results obtained from applications of the modified BBN model to two nuclear applications as well as an assessment of the feasibility of using BBNs for quantifying software failure probabilities are discussed in the report.</p>
NUREG/CR-7234	Development of A Statistical Testing Approach for Quantifying Safety-Related Digital System on Demand Failure Probability	nuclear	<p>A statistical testing approach for quantifying on-demand failure probabilities for safety-related digital systems has been developed and applied to the loop-operating control system (LOCS) of an Advanced Test Reactor (ATR) experimental loop at Idaho National Laboratory (INL). This work is the result of</p>	<p>The study used the ATR's PRA to define the testing environment, that is, the conditions under which the safety system would be called upon to initiate a safety function. Based on the PRA accident sequence information, a thermal-hydraulic model (RELAP5) was used to simulate the experimental loop conditions (e.g.,</p>

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
			<p>a collaboration between Brookhaven National Laboratory (BNL), INL, and the Korea Atomic Energy Research Institute (KAERI).</p> <p>The objectives of the study include:</p> <ol style="list-style-type: none"> 1. development of a statistical testing approach for estimating digital system failure probability, the results of which are suitable for including in a probabilistic risk assessment(PRA); and 2. application of this approach to the LOCS, and insights into the feasibility, practicality, and usefulness of the estimation in models of digital systems for inclusion in nuclear powerplants' PRAs. 	<p>pressure, temperature, and flow) during the selected accident sequences in order to provide realistic input signals to the LOCS test platform. To ensure that the test cases provided adequate coverage of operational conditions, thirteen probabilistic failure process models (PFPMs) were developed to represent the varieties associated with timing, component failure modes, and process variable control. An automated test platform was developed to supply input signals for each test case to the LOCS digital system and monitor when a trip signal was generated. The testing results were then used to quantify the on-demand failure probability of the digital LOCS system.</p> <p>The result of no failure in 10,000 tests was used to estimate the probability of failure of the software on demand. Since the tests were done on the actual LOCS system, both its hardware and software were tested. The results can also be used to estimate system failure probability.</p> <p>In addition, the PRA was used to determine the importance of the LOCS in terms of the total core-damage frequency. The PRA results show that the reliability of the LOCS system, based on the results of statistical testing, is consistent with its stated reliability goal of 10-04. The PRA</p>

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
				<p>results also indicate that LOCS failure is a minor contributor to the core damage frequency, and a larger failure probability does not significantly affect the total core damage frequency. This in turn can lead to fewer test scenarios required to demonstrate LOCS reliability. The main reason for the low contribution is that the plant protection system always serves as a backup to the LOCS.</p> <p>A number of issues arising from the use of simplified assumptions that could impact the realism of the study were resolved. The lessons learned with respect to these issues are summarised in the report.</p>
NUREG/CR-7273	Developing a Technical Basis for Embedded Digital Devices and Emerging Technologies	nuclear	<p>An embedded digital device (EDD) is a component consisting of one or more electronic parts that requires the use of software, software-developed firmware, or software-developed programmable logic, that is integrated into hardware equipment to implement one or more system safety functions.</p> <p>This report provides a technical basis for developing guidance for the safe use of EDDs in commercial nuclear power plants (NPPs) in the United States (U.S.), along with relevant observations, based on their classification, functionality, configurability, consequences of failure, and potential for common-cause failures (CCFs), and it reviews how other agencies worldwide,</p>	The report does not include any methods to estimate software reliability.

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
			both nuclear and nonnuclear, regulate, approve the use of, and actually use EDDs.	
NUREG/GR-0019	Software Engineering Measures for Predicting Software Reliability in Safety Critical Digital Systems	nuclear	<p>The objective of this study is to identify a set of software engineering measures from which the potential reliability of a digital I&C system can be predicted. This study commences a long-term research effort for developing a method to obtain a quantitative estimate of the reliability of a digital system.</p> <p>A set of software engineering measures from which the potential reliability of a digital I&C system can be predicted is developed from a set of 30 pre-selected software engineering measures. These measures are derived from a pool of 78 software engineering measures identified by Lawrence Livermore National Laboratory (LLNL). The concepts of structural classification, software development life-cycle classification, and family are presented. These 30 measures are categorized using these concepts. The concept of RPS and an extended structural representation are introduced to bridge the gap between software engineering measures and reliability. Expert opinion is elicited as the input in ranking the pre-selected 30 measures in terms of software reliability prediction</p>	This study is the first step towards a systematic approach predicting the reliability of a real-time I&C software using Reliability Prediction Systems (RPS) established from the top-ranked measures and families. However, current knowledge prevents the quantitative estimation of the accuracy of such prediction. Further experiments are required to investigate the quantitative reliability as a function of the RPS measures.

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
NUREG/GR-0020	Embedded Digital System Reliability and Safety Analyses	nuclear	<p>This report recognises that the migration from analogue to digital systems in the instrumentation and control (I & C) within a nuclear power plant has increased the complexity of the instrumentation. The need to understand the effects of various failure modes, including common cause failures and common mode failures, in these systems is becoming increasingly important because the failure of an I & C system could lead to risk significant events. In order to understand the effects of common cause and common mode failures on a system, a survey of existing definitions and applications of these definitions as they apply to digital embedded systems was performed. From this survey, it was found that the definitions and analysis treated the hardware and the software as independent entities. However, when embedded digital systems are in actual operation, there is tight integration of the hardware and software components; that is, the function realized by a such system cannot be partitioned between hardware and software but must be analysed in a unified manner. In addition to addressing the limitations of the existing common cause and common mode failure definitions, a detailed assessment of existing modelling techniques to assess their effects is also presented.</p>	<p>Whilst the report does cover the inclusion of digital I&C in PRA, including a discussion of various methods (Markov models, static and dynamic FTs etc) the parameter estimation section does not provide any detail on methods to estimate software reliability.</p>

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
SAPs	Safety Assessment Principles for Nuclear Facilities, 2014 Edition, Revision 1 (January 2020)	Safety Assessment Principles	The SAPs are described as follows, 'ONR's inspectors use these Safety Assessment Principles (SAPs), together with supporting Technical Assessment Guides (TAGs), to guide their regulatory judgements and recommendations when undertaking technical assessments of nuclear site licensees' safety submissions.'	<p>In terms of the data input to the PSA it states the following:</p> <p>'Paragraph 655 - Best-estimate methods and data should be used as far as possible within the PSA and in particular for determining initiating event frequencies and in the supporting transient, accident progression, source term and radiological analyses. Where this is not practicable, conservative assumptions should be made and the sensitivity of the results to these assumptions should be established.</p> <p>Para 657 - When models are used for the calculations of input probabilities, for example in human errors or failures of computer-based systems (including software errors), common cause failures, or the failures of structures, then the methodologies used should be justified, and should account for all key influencing factors.'</p> <p>The SAPs do not include any explicit examples/descriptions of the models that might be used.</p>
SSG-39	Design of Instrumentation and Control Systems for Nuclear Power Plants	nuclear	This Safety Guide provides recommendations on the design of C&I systems of nuclear power plants to meet the requirements established in IAEA Safety Standards Series. It is expected that this Safety Guide will be used in conjunction with detailed industrial	This Safety Guide provides general recommendations on software of the digital C&I (e.g. topics software requirements, design, implementation, V&V process). These recommendations apply to all types of software for application in, or to, C&I equipment important to safety, for

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
			standards. This document provides general guidance relating to the development of computer software for use in I&C systems important to safety as well as for digital data communication, including design, verification and validation.	example, operating systems, predeveloped software or firmware, software to be specifically developed for the project, or software to be developed from an existing predeveloped family of hardware or software modules. Detailed discussion concerning analysis methods and reliability data of digital C&I is outside the scope of this document.
TECDOC-1848	Criteria for Diverse Actuation Systems for Nuclear Power Plants, IAEA TECDOC Series	nuclear	This publication identifies, based on current practices, common criteria for the design and implementation of a diverse actuation system (DAS) as a backup system to a reactor protection system. A justification for the DAS system may be based upon deterministic and/or probabilistic analyses of initiating events. The report discusses issues concerning commonality of software and measures against probable CCF in the C&I architectures.	The report provides recommendation for analysis of defence in depth and diversity is one of the means of investigating the vulnerability of C&I safety systems to common cause failure. The annexes of the report provide several examples of design solutions for implementation of a DAS which illustrate the range of various concepts and different scopes.
TECDOC-1922	Reliability Data for Research Reactor Probabilistic Safety Assessment, IAEA TECDOC Series	nuclear	This report presents the results of research projects conducted from 1989 to 2004 by participants from 11 countries. The report provides information on a wider range of issues pertaining to reliability data for research reactor PSA. One chapter provides discussion concerning consideration of digital C&I in the PSA.	Detailed discussion of analysis methods and reliability data of digital C&I is outside the scope of this TECDOC report.
TF SCS	Licensing of safety critical software for nuclear reactors, Common position of international nuclear regulators and	nuclear	There are several approaches offered to a licensee and a regulator for the demonstration of the safety of a computer-based system. The demonstration may be conditioned on the provision of evidence	This consensus document has been revised and improved by the Regulator Task Force on Safety Critical Software (TF SCS) several times since its original publication in 2000, in order to provide up-

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
	authorised technical support organisations, Revision 2021		<p>of compliance with a set of agreed rules, laws, standards, or design and assessment principles (rule-based approach). It also may be conditioned on the provision of evidence that certain specific residual risks are acceptable, or that certain safety properties are achieved (goal based approach). Any combination of these approaches is of course possible. A safety demonstration may be multi-legged, supported by many types of evidence. None of these approaches is without problems. The law-, rule-, design principle- or standard- compliance approach often fails to demonstrate convincingly by itself that a system is safe enough for a given application, thereby entailing licensing delays and costs. A multi-legged approach may suffer from the same shortcomings. By collecting evidence in three different and orthogonal directions, which remain unrelated, one may fail to convincingly establish a system property. The safety goal approach requires ensuring that the initial set of goals, which is selected, is complete and coherent.</p>	<p>to-date practical guidance and consistent standards of quality in the regulatory review of safety critical software. TF SCS member organisations routinely use the document and recommend it to nuclear regulators and licensees throughout the world, for their reference and use. The task force decided at an early stage to focus attention on computer based systems used in nuclear power plants for the implementation of safety functions (i.e. the functions of the highest safety criticality level); namely, those systems classified by the International Atomic Energy Agency as “safety systems”. Therefore, recommendations of this report – except those of chapter 1.11 – address “safety systems” and not “safety related systems”. The Task force has adopted the view that three basic independent types of evidence can and must be produced: evidence related to the quality of the development process; evidence related to the adequacy of the product; and evidence of the competence and qualifications of the staff involved in all of the system life cycle phases. In addition, convincing operating experience may be needed to support the safety demonstration of pre-existing software. As a consequence, the Task force reached early agreement on an important</p>

Reference	Title	Scope, Subject	Methodology, Approach	Reliability Assessment of Software of Digital C&I
				<p>fundamental principle (see 1.1.3.1) that applies at the inception of any project, namely:</p> <p><i>A safety plan¹ shall be agreed upon at the beginning of the project between the licensor and the licensee. This plan shall identify how the safety demonstration will be achieved. More precisely, the plan shall identify the types of evidence that will be used, and how and when this evidence shall be produced.</i></p>

7.2 Annex Task 2: Industry Workshop (WS1)

7.2.1 Questionnaire

Background

Safety-related control and instrumentation (C&I) systems in nuclear facilities are nowadays usually realised using digital C&I (DCI) technologies. In addition, DCI is increasingly being adopted in legacy plants and facilities in the UK as existing analogue versions become obsolete. General experience, also from other application areas of DCI (e.g., aerospace industry), shows that DCI has a significant potential for critical failures of functions important to safety.

An assessment of the reliability of DCI is often performed applying probabilistic methods. Most analyses are carried out based on models and differ, among other things, in their modelling approaches, assumptions, reliability characteristics, and methodological procedures (particularly regarding software). For this reason, additional guidance is required for licensees and regulators. The UK Office for Nuclear Regulation (ONR) have recognised this and initiated a project via the Atlas Alliance (GRS and CRA Ltd) to address the issue. The project has begun with a review of relevant approaches (including those used in non-nuclear industries) due to be completed by the end of April 2022.

The ultimate goal of the project is to update the corresponding relevant TAG/s and SAPs to ensure a consistent approach across the industry and allow representation of software in Probabilistic Safety Assessment (PSA) models that is 'best estimate' (as opposed to unduly conservative) so that the risk insights derived from them are as realistic as possible. Furthermore, additional recommendations should be included in existing guidance on how to make proportionate decisions using DCI-related PSA insights to reduce risk as much as reasonably practicable.

To support the project, a two-day workshop will be held in May to present the findings of the cross-industry literature review to current and prospective UK Nuclear site licensees. In addition, views from participants on current methods and associated problems/issues will be sought to ensure that the proposed changes to the TAG/s and SAPs are practical and useful to both regulators and licensees. The planned workshop for this includes the following:

- Introduction and overview of the purpose and objectives of the workshop.
- Presentation of literature review findings and summary of 'modern best practices' including approaches in other high-risk industries.
- Overview of the experience of experts in performing DCI modelling in PSA.
- Discussion of topics from presentations by specialists from the UK reactor and non-reactor facility licensees, for example:
 - DCI analyses and assessments performed to date and inclusion in the safety case,
 - Current approaches for DCI modelling in PSA – methodology, level of detail, etc.,
 - Current sources of data for DCI components and software,
 - Overlap with qualitative C&I assessments,
 - Consideration of DCI risk insights in decision making,
 - Issues/problems encountered, etc.
- Discussion on the expectations of the UK reactor and non-reactor facility licensees regarding the update of the UK guidelines.
- Concluding discussion on a possible way forward.

Consideration of Realistic Software Modelling in PSA, 4/5 May 2022, Warrington, UK



Purpose of this questionnaire

The workshop in May will be held as a hybrid event (in person and online attendance possible).

Representative/s from your organisation are invited to attend and encouraged to do so in person to maximise the interaction and benefits.

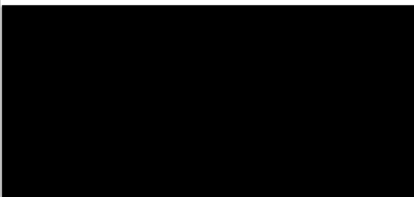
Date: 4th May 2022, 10:30 GMT – 5th May 2022, 16:00 GMT

Microsoft Teams invite for virtual attendance to be sent closer to the workshop date.

Whilst we would like the workshop to be attended by as many UK licensees (and other interested parties) as possible, we recognise that this may be difficult due to busy work schedules.

Engagement and input from UK licensees are however extremely valuable to the project and therefore we request that you please complete the questionnaire below as much as possible regardless of your planned attendance at the workshop. For workshop attendees, if you are also able to structure a short presentation around these questions providing some further detail this would be greatly appreciated. We will be in contact regarding your ability /desire to provide this presentation in due course.

Please send the completed questionnaire, preferably electronically, to the following address no later than **22/04/2022**:



If you are unable to attend the workshop, we would still appreciate your response to the questionnaire.

Participant (Voluntary Information)

Name:

Organisation:

Do you plan to participate at the workshop in May?

Yes, in person

Yes, online

No

**Consideration of Realistic Software Modelling in PSA,
4/5 May 2022, Warrington, UK**



I. Topic: Requirements, Guidance

1. Are quantitative risk assessments for safety evaluation of technical systems required in your activities?

Yes

No

2. If yes, do you take potential failures of Digital C&I (DCI) into account?

Yes

No

a) If no, how is this justified?

b) If yes, does your organisation have specific requirements/guidelines concerning DCI, especially software, which should/must be met when creating quantitative risk assessments?

Yes

No

i. If yes, what form does this guidance take?

ii. If yes, in which way do the requirements for DCI, especially for software, include quantitative safety targets? (e.g., "less than 10^{-x} ")

3. What additional guidance do you feel is needed in the area of software/firmware reliability?



II. Topic: Methodology

4. Which methods are applied in your organisation to analyse the reliability of DCI (especially software) for quantitative risk assessments?

- a) What is the (necessary) level of detail for modelling DCI (especially software)?

- b) Which failure modes of DCI (especially for software) are assumed/considered in your organisation's quantitative risk models?

- c) Which dependencies concerning DCI (e.g., with communication, support systems, shared hardware) are considered?

- d) Can current approaches lead to distortion of results and therefore meaningful risk insights?

Yes

No

**Consideration of Realistic Software Modelling in PSA,
4/5 May 2022, Warrington, UK**



- i. If yes, are you able to provide examples (anonymised if necessary) and how these were overcome?

- 5. Does your organisation perform additional sensitivities studies related to the inclusion of DCI in quantitative risk models?

- a) If so, how are these performed and used?

III. Topic: Data for DCI - in particular Software/Firmware

- 6. Does any available guidance within your organisation cover suggested approaches for obtaining/ deriving values for software/firmware reliability?

- 7. Which databases does your organisation currently use for obtaining failure data (frequencies/rates/probabilities) for failure modes of DCI components (hardware, software)?

**Consideration of Realistic Software Modelling in PSA,
4/5 May 2022, Warrington, UK**



8. Are the uncertainties in the failure data taken into account in your organisation's quantitative risk models? If so, how?

9. Is there sufficient operational experience (OpEx) data within, and outside, your organisation to support use in quantitative risk models?

Yes

No

a) Does your organisation collect and/or process OpEx on the performance of DCI equipment and software?

Yes

No

b) Does your organisation use OpEx in the data assigned to DCI equipment and software in quantitative risk models?

Yes

No

c) Are you aware of alternative approaches that are available for software reliability estimation?

10. The C&I community tends to work with high confidence reliability values/data. The PSA community tends to work with best estimate values/data when these are available. Do you feel the phrase 'best estimate' (in the context of data) is well understood in your organisation and/or with external regulation?

Yes

No

**Consideration of Realistic Software Modelling in PSA,
4/5 May 2022, Warrington, UK**



- a) If no, what issues does this cause? Are you able to provide examples (anonymised if necessary) and how these were overcome?

11. Are there any other topics or issues you feel are relevant and would like to see covered in the workshop or by the wider project?

Many thanks for your participation!

7.2.2 Results of Survey – Redacted

