 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0013	Rev.: 0	Page: 1 / 7
		GDA-REC-GNSL-005780	

REGULATORY OBSERVATION Resolution Plan

RO Unique No.:	RO-UKHPR1000-0013
RO Title:	Modelling of computer based system reliability in the PSA
Technical Area(s)	15.Probabilistic Safety Analysis
Revision:	Rev 0
Overall RO Closure Date (Planned):	2020-10-31
Linked RQ(s)	RQ-UKHPR1000-0226
Linked RO(s)	
Related Technical Area(s)	3.Control & Instrumentation
Other Related Documentation	Refer to Appendix A

Scope of Work


Background

Computer-based I&C systems are to be used for the control and monitoring of safety systems of UK HRP1000, which could contribute to the overall risk profile of the plants. Therefore, in order to properly assess the risks introduced by the computer-based I&C systems, it is important to develop a suitable and sufficient methodology for the modelling of computer-based I&C systems reliability in the Probabilistic Safety Analysis (PSA), to ensure more realistic models are constructed and relevant data are suitably underpinned.

ONR's guidance (Safety Assessment Principles (SAPs) and Technical Assessment Guides (TAG)) require that *"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."* [1, 2] and *"The methodology used for the estimation of probabilities of failure of computer-based systems should meet industry accepted practices. The analysis of the software reliability should identify and take into account the influencing factors that affect the quality of the software."* [2], where the software reliability and common cause failures (CCFs) of computer-based systems are emphasized.

Regarding the modelling of computer-based I&C systems reliability in the Internal Events Level 1 PSA model submitted in October 2018, some aspects have been identified which do not fully align with UK Relevant Good Practice (RGP). RO-UKHPR1000-0013 has therefore been raised by ONR to highlight the following potential gaps:

- Software reliability is not identified and modelled;

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0013	Rev.: 0	Page: 2 / 7
		GDA-REC-GNSL-005780	

- Complex models are developed;
- Data sources are not clarified.

Based on the relevant ONR SAPs [1] and NS-TAST-GD-030 [2], standards such as IAEA-SSG-39 [3], IEC61508 [4] and ASME/ANS RA-S 2008 [5], and other RGP, a methodology for the modelling of computer-based I&C system reliability in the PSA will be developed, and a pilot study to demonstrate the adequacy of the proposed methodology will be conducted where a typical I&C function is selected.


Scope of work

The scope of work is described as follows:

- 1) A methodology for the modelling of computer based I&C system reliability in the PSA will be developed, including the following key points:
 - Determination of I&C functions contributing to the plant safety analysis and identification of the scope and extent of the relevant I&C systems;
 - Identification of standards and Operating Experience (OPEX) relevant to the modelling of computer-based I&C systems reliability in the PSA;
 - Modelling consideration relevant to the I&C system design features;
 - Simplification of models;
 - Analysis of the dependencies between systems / subsystems / components, including hardware and software;
 - Modelling of CCFs ;
 - Collection and analysis of data, including assessments of software reliability data.
- 2) A pilot study to demonstrate the adequacy of the proposed methodology will be conducted, including the following key points:
 - Selection of a typical I&C function with the typical I&C system architecture and design features;
 - Analysis of software error, CCFs and model simplification;
 - Development of the fault tree models;
 - Selection of the reliability data;
 - Quantitative analysis.

For the closure of this RO, the following deliverables will be provided:

- The report titled "*Methodology for the modelling of computer-based I&C system reliability in the PSA*" will be developed as the response to RO Action 1;
- The report titled "*Modelling of a typical I&C function reliability in the PSA*" will be developed as the response to RO Action 2.

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0013	Rev.: 0	Page: 3 / 7
		GDA-REC-GNSL-005780	

Deliverable Description

RO-UKHPR1000-0013.A1 – Provide a methodology and approach for the modelling of computer based system reliability in the PSA and demonstrate that it meets regulatory expectations

The RO action 1 states that:

In response to this Regulatory Observation Action, General Nuclear System Limited(GNS) should:

- *Provide a methodology and approach to modelling computer based systems within the generic UK HPR1000 PSA so that the level of risk arising from computer based systems is adequately understood and demonstrated that it meets regulatory expectations. ONR considers that the response to this Action should:*
 - *Identify the computer based systems and components that will be modelled in the PSA;*
 - *Explain how these will be modelled in the PSA;*
 - *Justify the source of data that will be used to estimate computer based system reliability and demonstrate that it is suitably underpinned;*
 - *Justify relevant standards applied and how the methodology follows industry-accepted practices.*
 - *Explain how dependencies (between systems and between components and subsystems within the same system) will be addressed by the analysis;*
 - *Describe and justify how the analysis gives due consideration to the factors that could lead to common cause failures of computer based systems.*


Resolution Plan

IAEA-SSG-39, Reference [3], states that *Software errors may lead to common cause failure in redundant digital systems if the same software is used in multiple redundancies. Thus, to estimate digital system reliability, it is necessary to estimate the probability of system failure due to hardware failure and software error.* According to this requirement, software error should be identified and taken into account during the modelling of I&C system reliability in the PSA, which is considered as UK RGP.

Addenda to ASME/ANS RA-S 2008, Reference [5], states that *Each parameter shall be clearly defined in terms of the logic model, basic event boundary, and the model used to evaluate event probability.* It is understood that the sources of data used for I&C system reliability shall be clarified.

Compared with UK RGP and regulatory expectations, some potential gaps have been identified, including complex models used, software reliability not considered and data sources not clarified.

In response to Action 1, the report entitled *“Methodology for the modelling of computer based I&C system reliability in the PSA”* will be provided by the end of April 2020. This report will present the methodology which will be developed according to the workflow as shown in Fig. 1 and the following key points will be

	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0013	Rev.: 0	Page: 4 / 7
		GDA-REC-GNSL-005780	

considered:

- The required I&C functions contributing to the plant safety analysis will be determined according to the Internal Event Level 1 / level 2 PSA, by which scope and extent of the computer-based systems and components (including software) to be modelled in the PSA will be identified;
- Standards and OPEX relevant to the modelling of computer-based I&C systems reliability in the PSA will be identified and justified;
- The failure on demand of each I&C function is defined as an unexpected event (i.e. the top event). In order to analyse the failure mechanism. The design features of I&C systems will also be considered in the PSA models, including redundancy, self-supervision, etc. Also, the simplification of modelling will be studied, where the approach for model abstraction and model granularity are considered;
- The dependencies between systems and components and subsystems within the same system of I&C systems will be identified, justified and modelled appropriately;
- CCFs between the redundant parts of I&C systems and the redundant sensors will be modelled properly for the dependencies between them;
- The data used to estimate the reliability of I&C systems and components will be collected and justified. The method for assessing software reliability data will also be studied.

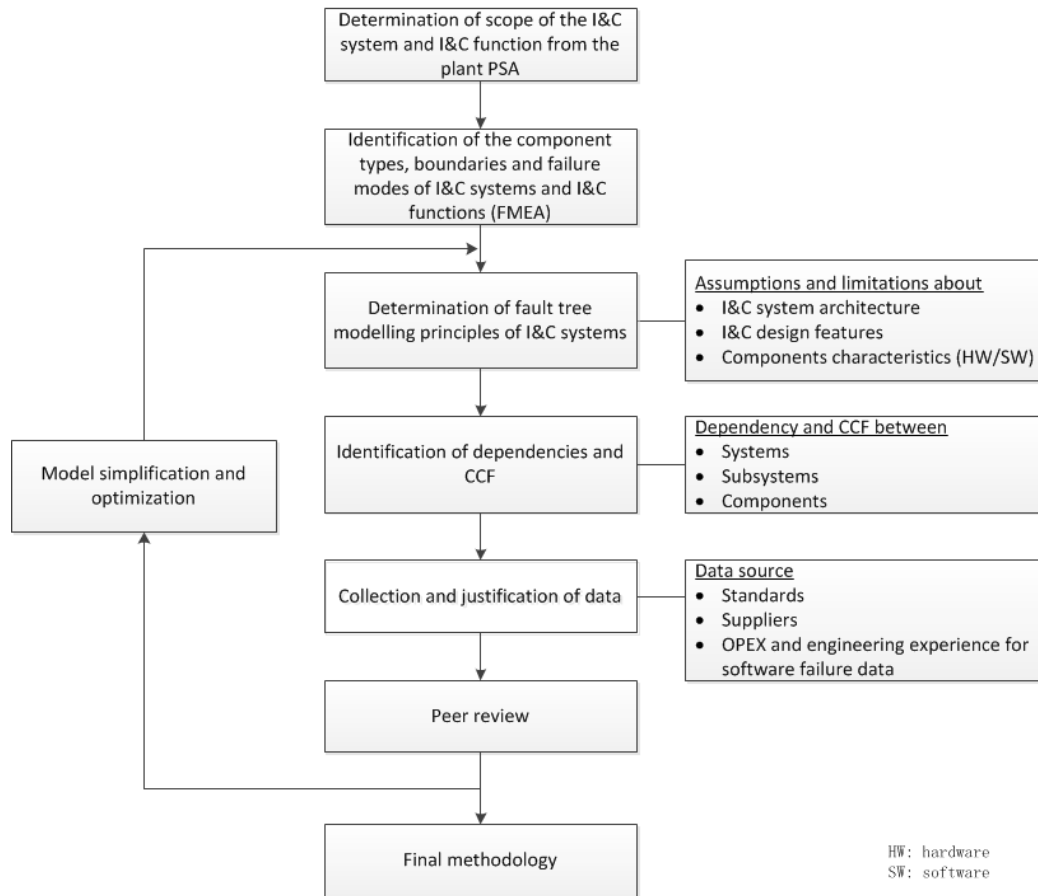



Fig. 1 Workflow for Methodology Development

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0013	Rev.: 0	Page: 5 / 7
		GDA-REC-GNSL-005780	

RO-UKHPR1000-0013.A2 – Perform adequate PSA modelling of computer based system reliability

The Regulatory Observation Action 2 states that:

In response to this regulatory observation action, the requesting party should:

- *Implement the methodology and approach for the PSA based modelling of computer based systems as detailed in the response to Action 1. In responding to the Action the RP should consider staging the response such that ONR is provided with sufficient information to demonstrate the adequacy of the methodology, alongside a forward plan for completion of the full scope of activities necessary.*

Resolution Plan

In response to Action 2, *Modelling of a typical I&C function reliability in the PSA* will be provided by the end of July 2020, in which a typical I&C function will be selected and modelled in order for all of the aspects of the methodology to be put into practice. The typical modelling will include:

- Description of the selected typical I&C function, its system architecture and design features;
- Analysis of dependencies between components and subsystems within this I&C system, and between other systems;
- Analysis of software error;
- Development of the fault tree models for the selected typical I&C function with consideration of CCFs;
- Selection of the reliability data for the selected typical I&C function;
- Quantitative analysis.

Note: The full scope of I&C modelling will be performed, in accordance with the proposed methodology, when validated, in the final version of PSA submission which is out of this RO.

A detailed work plan developed for the modelling activities of computer based I&C system reliability in the PSA is shown in the Gantt chart in APPENDIX A.

Impact on the GDA Submissions

Relevant information will be incorporated into the final version of PSA submission during Step 4. The submissions that are impacted by this resolution plan include:

- Methodology for the modelling of computer based I&C system reliability in the PSA
- Modelling of a typical I&C function reliability in the PSA

Timetable and Milestone Programme Leading to the Deliverables

See attached Gantt Chart in APPENDIX A.

 General Nuclear System	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0013	Rev.: 0	Page: 6 / 7
		GDA-REC-GNSL-005780	

Reference

- [1] ONR, Safety Assessment Principles for Nuclear Facilities, Revision 0, 2014
- [2] ONR, Probabilistic Safety Analysis, NS-TAST-GD-030, Revision 5,2016
- [3] IAEA, Design of Instrumentation and Control Systems for Nuclear Power Plants, SSG-39, 2016
- [4] IEC, Functional Safety of Electrical, Electronic, Programmable Electronic Safety-related Systems, IEC 61508, 2010
- [5] ASME, Addenda to ASME/ANS RA-S 2008: Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS RA-Sb-2013

	REGULATORY OBSERVATION RESOLUTION PLAN RO-UKHPR1000-0013	Rev.: 0	Page: 7 / 7
		GDA-REC-GNSL-005780	

APPENDIX A RO-UKHPR1000-0013 Gantt Chart

Tasks	Steps	2019						2020												
		Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	
RO Action 1																				
Methodology for the modelling of computer based I&C system reliability in the PSA, Rev. A	Development	█	█	█	█	█	█	█	█	█	█									
	Submission											▲								
RO Action 2																				
Modelling of a typical I&C function in the PSA, Rev. A	Development									█	█	█	█	█	█					
	Submission															▲				
Assessment																				
Regulators assessment						█	█	█	█	█	█	█	█	█	█	█	█	█	█	█
Target RO closure Date																			▲	