Analyzing Defense-in-Depth Properties of Nuclear Power Plant Instrumentation and Control System Architectures Using Ontologies

Björkman, Kim; Pakonen, Antti

Published in:
13th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2023)

DOI:
10.13182/NPICHMIT23-41042

Published: 01/07/2023

Document Version
Publisher's final version

Link to publication

Please cite the original version:
Björkman, K., & Pakonen, A. (2023). Analyzing Defense-in-Depth Properties of Nuclear Power Plant Instrumentation and Control System Architectures Using Ontologies. In *13th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2023)* (pp. 1590-1599). American Nuclear Society (ANS). https://doi.org/10.13182/NPICHMIT23-41042

Analyzing Defense-in-Depth Properties of Nuclear Power Plant Instrumentation and Control System Architectures Using Ontologies

Kim Björkman, Antti Pakonen[*]

VTT Technical Research Centre of Finland Ltd., Espoo, Finland

doi.org/10.13182/NPICHMIT23-41042

ABSTRACT

The overall instrumentation and control (I&C) architecture of a nuclear power plant (NPP) is comprised of several I&C systems and their dependencies. The architecture needs to fulfil the principle of defense in depth (DiD). Defense-in-depth is the principal method for preventing accidents and mitigating the potential consequences of accidents. The levels of DiD should be independent of each other. The primary means to achieve independence are diversity, physical separation, and functional isolation. Approaches with extensive tool support for ensuring that the design solutions of nuclear overall I&C architectures realize relevant DiD properties are scarce. An ontology of the semantic web is a specification of a representational vocabulary for a shared domain of discourse, containing definitions of classes, individuals, and their relationships. An ontology-based knowledge base, built on named graphs, enables a computer to combine pieces of information into valuable knowledge based on queries. In this paper, we present an ontology-based approach for assessing that an NPP I&C architecture fulfils different DiD properties. In our approach, we aim at checking requirements related to physical separation, electrical isolation, communication independence, diversity, safety classification, and failure tolerance. We also discuss the developed work process and tool chain for ontology-based analysis. We demonstrate the use of the ontology and the work process based on two case studies.

Keywords: Control systems, Ontology, Systems architecture, Semantic Web

1. INTRODUCTION

The overall instrumentation and control (I&C) architecture is the organizational structure of the I&C systems important to the safety of a nuclear power plant (NPP) [1]. The architecture gives a high-level view of the individual I&C systems and how they relate to one another. It establishes the allocation of plant functions to individual I&C systems and the specification of the interface requirements of the individual I&C systems, including the layout of communications between individual I&C systems [2].

The overall I&C architecture should consider several key principles in its design and implementation [2]. Defense in depth (DiD) is the principal means of preventing accidents and mitigating the potential consequences of accidents [3]. The levels of DiD should be independent of each other. The primary means to achieve independence are diversity, physical separation, and functional isolation. Striving for total independence between DiD levels is not practical. However, the DiD levels should be sufficiently independent and the adequacy of the independence should be justified by appropriate means [3]. Approaches with extensive tool support for ensuring that the design solutions of nuclear overall I&C architectures realize relevant DiD properties are scarce.

[*] antti.pakonen@vtt.fi

The Semantic web [4] strives to derive information from the Web through a semantic theory providing an account of "meaning", where the logical connection of terms drives machine reasoning. This enables computers to search and combine heterogeneous pieces of data from different sources, based on an "understanding" of what a human user would find a meaningful association. A knowledge base based on Semantic Web technology runs on directed graphs, and can answer complex queries typically expressed in SPARQL [5]. An ontology is a specification of a representational vocabulary for a shared domain of discourse, containing definitions of classes, individuals, and their relationships [6]. Machine interpretability can be achieved through ontology languages such as OWL [7].

In nuclear organizations, the knowledge management is often focused on organizational and thematic structures [8]. Such structures can contain thousands of files in different formats with limited amount of meta data. Thus, information related to the overall I&C architecture can be scattered in different documents and systems. Information models, when they exist, may have a specific viewpoint (e.g., functional vs. physical). In such cases, utilization of semantic techniques could provide immediate benefits by enabling to search and combine the pieces of information into valuable knowledge. Outside the scope of I&C, Semantic Web techniques have shown to be useful in building rich knowledge models in nuclear applications [8].

In this paper, we present an ontology-based approach for assessing that an NPP I&C architecture fulfils different DiD properties. This paper continues the work presented in [9] by enhancing the exemplary ontology and by defining a work process for performing the ontology-based assessment. The rest of this paper is structured as follows. In section 2, we review the related research. We present the refined ontology in section 3. In section 4, we present a work process for performing the analysis and the tools we used in the case studies. We discuss the case studies in section 5. Section 6 concludes this study.

2. RELATED RESEARCH

We have reviewed related work in [9]. Our aim is not to repeat the review but to extend it with research related to evaluating I&C architecture and the use of ontologies in the nuclear domain.

Traditionally, the evaluation of an I&C architecture seems to have focused on analyzing failure tolerance. In Finland, the scope of the failure tolerance analysis (i.e. a framework to organize individual analyses, such as failure mode and effects analyses, common cause failure (CCF) analyses [10]), required by the Finnish regulatory guides [11], includes also the I&C architecture. Especially spurious actuations are considered in the I&C architecture context. Defense-in-depth and diversity analyses have been used for assessing vulnerabilities to digital CCFs (see e.g., [12], [13], [14]). The scope of these analyses is a bit different from our approach. They go into more detail within the fixed topic.

Both deterministic and probabilistic analysis methods need be utilized in the assessment of DiD requirements [15], [3]. The approaches discussed in, e.g., [15] and [16] represent probabilistic approaches, whereas our approach is a deterministic approach. In [15], the use of probabilistic risk assessment (PRA) in assessing DiD, especially related to I&C architecture is discussed. In [16], the use of PRA to assess level 2 defense-in-depth (DiD), considering especially preventive safety functions and associated systems, is discussed. In [13], also probabilistic approaches for analyzing digital CCFs are discussed.

In the nuclear domain, ontologies have been utilized in different contexts. In [17], a reactor control ontology is developed. In [18], semantic web based technologies are used to develop a knowledge management portal for a fast breeder test reactor. For improving the management of NPP procedures, [19] has developed a methodology that uses natural language processing technologies for extraction of syntactic and semantic information from the procedures. In [20], a preliminary ontology for simulation scenario development to facilitate human-system interface design, evaluation, and deployment during modernization of control room was developed. In [21], the use of ontologies in multi-agent systems in the energy domain is reviewed. To enhance the efficiency and veracity of materials failure analysis, an ontology based method is proposed in [22] for knowledge sharing. An NPP is used as an example system.

3. OVERALL I&C ARCHITECTURE ONTOLOGY

3.1. Requirements for the Ontology and Competency Questions

In the design and implementation of an overall I&C architecture the following issues related to defense-in-depth need to be considered; the degree of independence between the DiD levels, the manner in which non-safety systems are separated from safety systems, the number of independent channels in safety systems, and the degree of separation between the safety channels [1]. Independence between the I&C systems on the different layers can be achieved through separation, i.e. physical separation, electrical isolation, functional independence, independence of communication and independence of support systems, and through diversity [1], [3].

In our approach, we aim at checking requirements related to all of the above-mentioned aspects of the design. The requirements can be specified, e.g., in national regulations or international standards and guides. The knowledge base should be able to answer queries related to:

1. physical separation (separation by distance and/or structural barriers),
2. electrical isolation (electrical fault in one system does not degrade a connected system),
3. communication independence (guaranteed one-way communication, or deterministic data communication protocol),
4. diversity (protection against CCF [23]),
5. safety classification, and
6. failure tolerance

For each of these categories, we have listed competency questions (CQ), i.e. questions stated in natural language defining the scope of knowledge represented by an ontology [24]. The full list of competency questions is available online[1]. Examples of competency questions are:

CQ3.3: Are there interfaces across DiD lines?
CQ5.3: Are the support systems of the same (or higher) safety class as the system?

3.2. Ontology Class Structure and Object Relationships

The ontology should support to query the knowledge base for answers to the specified competency questions. Thus, the structure of the ontology depends on the knowledge we wish to collect from the base.

The developed ontology class structure and the related object relationships extends and refines the ontology discussed in [9]. The main classes of the ontology are: FunctionalEntity, PhysicalEntity, and Classification. The PhysicalEntity class covers I&C systems (and the interfaces between them), I&C devices, support systems, and their locations. The subclasses under the PhysicalEntity have not been updated from [9]. However, we have updated the related object relationships. The placement of physical entities into spaces has been refined. The new object relationship implementedWithProduct was created to specify with what product (subclass of Classification) I&C systems, I&C devices, and interfaces have been implemented with. In addition, signals are received by I&C systems (see Fig. 1) or by I&C devices.

[1] https://doi.org/10.5281/zenodo.7690661

The FunctionalEntity class covers initiating events, DiD levels, and I&C functions (and their parts and connections). As new features (see Fig. 1), FunctionalEntity includes also signals (e.g., alarms, control actions, measurements) and variables (control and measured variables). Some new key object relationships are shown in Fig. 1. Classification has subclasses such as SafetyClass, SeismicCategory, which can be applied to either the functional or the physical entities. As a refinement, Classification includes also the subclass DiversityAttribute [23] that covers, e.g., logic, manufacturer, product, and technology.

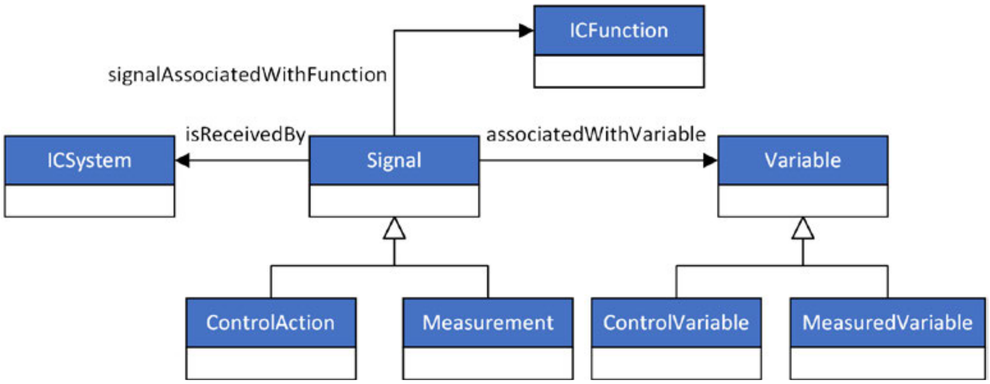


Figure 1. Main new classes and properties from our ontology.

3.3. Queries

Based on the ontology, we can flexibly specify SPARQL queries to address the different dependencies between I&C systems in the architecture. SPARQL [5] is a set of specifications providing languages and protocols to query and manipulate Resource Description Framework (RDF) graph data (a standard model for data interchange on the Web [25]). SPARQL queries can be considered as formalizations of competency questions [24]. The full list of SPARQL queries is available online[2]. Here we present an example query.

CQ3.5: Are there measurements shared between functions allocated to diverse systems?

```
PREFIX : <http://www.semanticweb.org/SEARCH/ontologies/2022/12/OICA/Classes#>

SELECT ?signal ?functionA ?systemA ?functionB ?systemB
       WHERE {
              ?signal :signalAssociatedWithFunction ?functionA.
              ?signal :signalAssociatedWithFunction ?functionB.
              ?functionA :isAllocatedTo ?systemA.
              ?functionB :isAllocatedTo ?systemB.
              ?systemA :diverseSystemTo ?systemB
        }
```

4. WORK PROCESS AND USED TOOLS

In the course of our case studies (see section 5), we have developed a work process for the ontology-based analysis of nuclear overall I&C architectures (see Fig. 2), consisting of three main phases; (1) ontology and knowledge base specification, (2) I&C architecture assessment and (3) documentation.

During ontology and knowledge base specification, the first tasks are to specify the competency questions and to start the collection of the needed data. The data may need to be collected from different sources,

[2] https://doi.org/10.5281/zenodo.7690661

e.g., different databases or pdf documents. The competency questions guide what data should be collected. The modelling work starts with the specification of the ontology class structure and the object relationships. The ontology serves as the schema for both the SPARQL query and the declarative rules definition. The declarative rules define how the collected data is mapped into RDF graph format. According to the declarative rules the collected data (i.e. the individuals of the classes the ontology defines) is transformed into RDF graph format that can be imported into a knowledge base.

The specification of SPARQL queries belongs partly to phase (1) and phase (2). The competency questions set requirements for the queries. Thus, the questions and the ontology lay a foundation for the queries. However, since formulating complex queries in SPARQL is quite straightforward, the analyst can during the assessment process formulate and modify queries according to the analyst's needs. The analysis task consists of two subtasks; running the queries in a knowledge base and interpreting the results from the queries. The analysis results may reveal errors or shortcomings in the SPARQL queries, the ontology. or the competency question, in which case the shortcomings are fixed. Finally, the results are documented.

Running the queries in the knowledge base is fully automated. However, the interpretation of the results need to be done manually. Basically any knowledge base provides the functionality to run queries. Different knowledge bases have different properties, e.g., different knowledge bases may support different versions of OWL or SPARQL. Some knowledge bases provide limited support for SPARQL query definition, e.g., in the form of syntax error identification or auto-complete functionality.

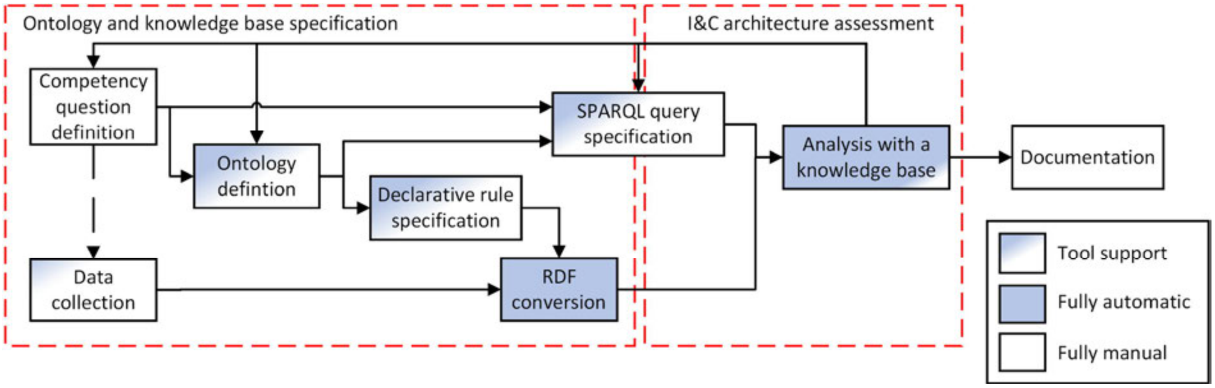
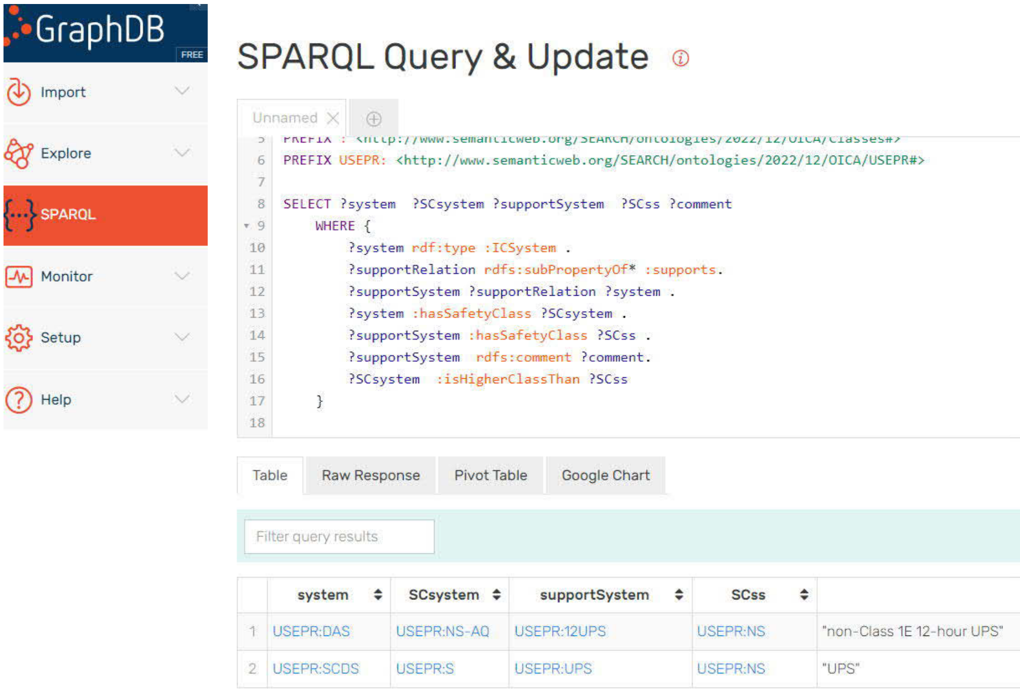

Ontology and knowledge base specification
I&C architecture assessment
Competency question definition
Ontology defintion
Declarative rule specification
SPARQL query specification
Data collection
RDF conversion
Analysis with a knowledge base
Documentation
Tool support
Fully automatic
Fully manual

Figure 2. The overall work process for ontology based I&C architecture assessment

A limitation to the use of Semantic Web ontologies is that the source data needs to be written in (or mapped to) RDF graph format, which can be error-prone. There are dedicated tools to automate the RDF conversion task. To support the mapping of semi-structured data into RDF graph format there exists dedicated tools such as RML.io [26] and OTTR [27]. In addition, some knowledge bases provide their own mapping tool. For example, the GraphDB semantic repository [28] provides its own dedicated tool called OntoRefine for transforming structured data into an RDF graph format. The OntoRefine tool includes also a graphical user interface (GUI) for declarative rules definition. Of the reviewed RDF conversion tools, GraphDB's OntoRefine seems to be the most straightforward tool to use and most stable. For the ontology class structure and the object relationship specification, e.g., Protégé [29] provides a graphical user interface (GUI).

In the case studies, we used MS Word to define the competency questions. We collected the data into several MS Excel files. The ontology was designed with Protégé. We selected Protégé for this task since it was the only encountered tool that provided a GUI for the ontology definition.

We used the GraphDB knowledge base for the analysis and, thus, the SPARQL queries were specified in the same tool (see Fig. 3). In [9], Protégé was used as the knowledge base. However, after measurement data was added to the U.S.EPR case study (see section 5.1) Protégé tool was no longer able to solve the queries and we needed a more scalable solution. We decided on GraphDB, since it is easy to use, scalable, efficient, and it provides simple support for SPARQL query specification. In addition, as discussed earlier, it provides a GUI for declarative rules definition and enables transforming data from MS Excel format into RDF. Therefore, it was self-evident for us to use GraphDB also for the declarative rule specification and RDF conversion.



```
PREFIX : <http://www.semanticweb.org/SEARCH/ontologies/2022/12/OICA/Classes#>
PREFIX USEPR: <http://www.semanticweb.org/SEARCH/ontologies/2022/12/OICA/USEPR#>

SELECT ?system  ?SCsystem ?supportSystem  ?SCss ?comment
    WHERE {
        ?system rdf:type :ICSystem .
        ?supportRelation rdfs:subPropertyOf* :supports.
        ?supportSystem ?supportRelation ?system .
        ?system :hasSafetyClass ?SCsystem .
        ?supportSystem :hasSafetyClass ?SCss .
        ?supportSystem  rdfs:comment ?comment.
        ?SCsystem  :isHigherClassThan ?SCss
    }

```

	system	SCsystem	supportSystem	SCss	
1	USEPR:DAS	USEPR:NS-AQ	USEPR:12UPS	USEPR:NS	"non-Class 1E 12-hour UPS"
2	USEPR:SCDS	USEPR:S	USEPR:UPS	USEPR:NS	"UPS"

Figure 3. A view of GrapDB showing a SPARQL query and results

5. CASE STUDIES

5.1. U.S. EPR

For our first case study, we used the same example system as in [9]. However, here, we used the refined ontology, and the updated competency questions and SPARQL queries. In addition, we have extended the scope of the data to include measurements. In the description below, we focus on the new features of the ontology. For a more in-depth description of the example case, we refer the reader to [9]. The case study is built around the proposed US variant of the European Pressurized Water Reactor (U.S. EPR). The U.S. Nuclear Regulatory Commission has published sections of the Final Safety Analysis Report (FSAR) online [30].

From [30], we collected data on 24 I&C systems, 156 I&C functions, 35 system interfaces, and around 870 measurements. We assigned identifiers for the functions, interfaces, and measurements. We assumed, e.g., the safety classification of each function. We also defined requirements for the overall architecture not specified in the FSAR itself, but inspired by Finnish YVL Guides and [3].

Most of the results from the analysis are identical to those discussed in [9]. Thus, we focus on presenting the results that are new. All results are available online. Regarding communication independence, Process

Automation System (PAS) (DiD preventive and risk reduction lines) sends turbine generator actuation signals to Turbine Generator (TG) I&C (DiD preventive line). TG I&C sends turbine generator information needed by PAS functions. Reactor Control, Surveillance and Limitation System (RCSL) (DiD preventive line) sends commands signals used in RCSL functions (other than control rods, e.g., boron control) to PAS. These issues were identified, since PAS belongs to both preventive and risk reduction lines. Thus, the query identifies a match between I&C systems belonging to preventive line and PAS. Depending on if and how the Process Information and Control System and the Safety Information and Control System actually share measurements, there could be issues in sensor sharing. Regarding failure tolerance, RCSL is four-redundant, but power is supplied by the two-redundant 12 UPS.

5.2. NuScale SMR

The example system of our second case study was the overall I&C architecture of the NuScale small modular reactor (SMR). The U.S. Nuclear Regulatory Commission has published sections of the Design Certification Application (DCA) online [31]. The “echelons of defence” [32] concept is applied for the DiD principle. The four echelons are control system, the reactor trip or scram system (RTS), the engineered safety features actuation system (ESFAS), and the monitoring and indicator system [32]. In the NuScale SMR, the module protection system (MPS) belongs both to the RTS and ESFAS echelon (see Fig. 4). The module control system (MCS) belongs to the control system echelon, and partly to the monitoring and indicator system echelon. The safety display and indication system (SDIS) belongs to the monitoring and indicator system echelon.

From [31], we collected data on 9 I&C systems, 44 I&C functions, and 19 system interfaces. We assigned identifiers for functions and interfaces. We assumed, e.g., the safety classification of each function. We used the same set of competency questions and SPARQL queries as in the U.S. EPR case.

Regarding physical separation, the DCA does not contain sufficient information about the placement of I&C systems and equipment in rooms, cabinets, or racks. Regarding electrical separation, some of the interfaces between safety classified and non-safety-classified systems are not stated to be electrically isolated in the DCA. In addition, safety classified (S) and non-safety-classified (NS) systems are powered by the same power supply system. Regarding communication independence, there is an interface from MCS and in-core instrumentation system, and SDIS (safety class NS) to MPS (safety class S). We assume that these are deliberate design choices. Regarding diversity, the DCA contains only a limited amount of information on diversity. However, there are interfaces between MCS and MPS. Regarding safety classification, MPS and neutron monitoring system (safety class S) are powered by the non-safety-related highly reliable DC power system (module specific). MPS has, e.g., components gateway and maintenance workstation that are non-safety-classified. Regarding failure tolerance, MPS is basically a two redundant system.

5.3. Case study conclusions

Neither of the DiD concepts applied in the example systems of the case studies corresponds to DiD structure proposed by Western European Nuclear Regulators’ Association (WENRA) for new reactor designs [3]. We did not expect either of the architectures to necessarily fulfill the requirements we based our competency questions and SPARQL queries on. Many of the requirements we wrote were not based on the FSAR or Design Certification Application themselves but inspired by Finnish YVL Guides and [3] as mentioned earlier. In addition, striving for total independence between DiD levels is not practical. But they should be sufficiently independent and the adequacy of the independence should be justified by deterministic and probabilistic means, and by engineering judgement [3]. Our approach is deterministic.

Our query results are not meant to be interpreted as criticism. The objective was to evaluate our approach and not to actually assess a real design. The results are likely to be examples of deliberate design optimization, rather than symptoms of problems.

The case studies showed that OWL supports analyzing requirements related to defense-in-depth. Based on queries defined by the analyst, the semantic knowledge base enables the computer to infer different classifications and connections that have may not have been explicitly stated in the source data. The revised ontology enabled us to analyze especially communication independence more thoroughly. The source material did not contain enough information to assess the applicability of the diversity attribute section of the ontology. The diversity attribute part was the second major refinement in the ontology compared to [9].

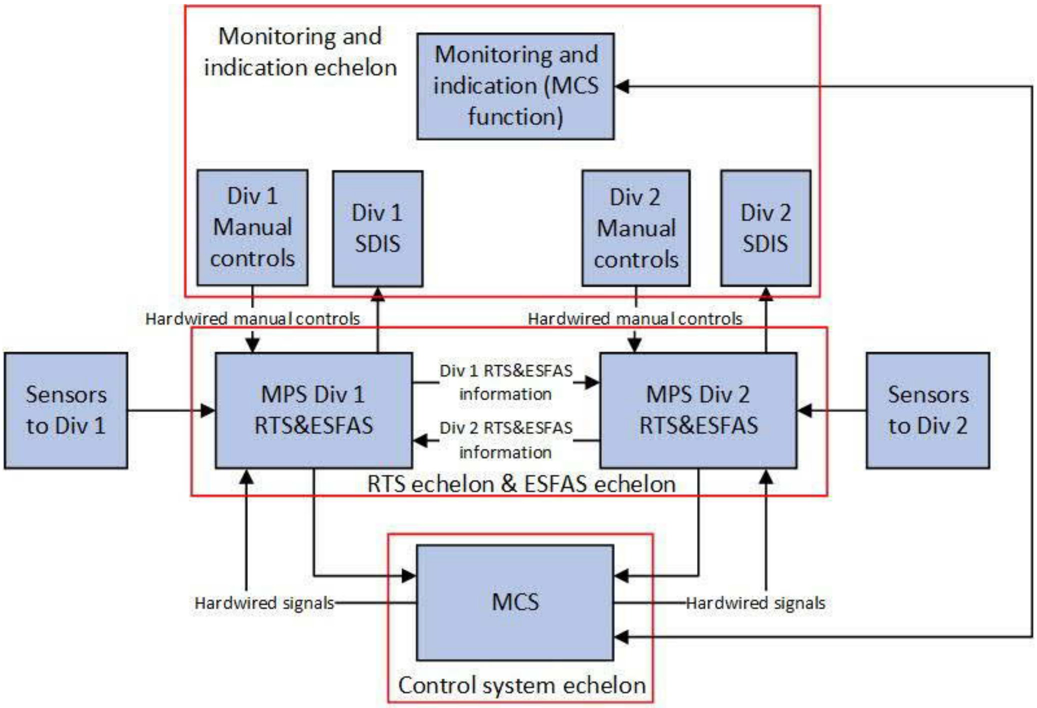

Monitoring and indication echelon
Monitoring and indication (MCS function)
Div 1 Manual controls
Div 1 SDIS
Div 2 Manual controls
Div 2 SDIS
Hardwired manual controls
Hardwired manual controls
Sensors to Div 1
MPS Div 1 RTS&ESFAS
Div 1 RTS&ESFAS information
Div 2 RTS&ESFAS information
MPS Div 2 RTS&ESFAS
Sensors to Div 2
RTS echelon & ESFAS echelon
Hardwired signals
MCS
Hardwired signals
Control system echelon

Figure 4. The echelons of defense of the NuScale SMR I&C architecture (modified from [31]).

6. CONCLUSIONS

In this paper, we presented a refined ontology for analyzing safety requirements related to the overall I&C architecture of a nuclear power plant. We demonstrated the approach with two cases studies, in which we detected different potential design issues in the overall I&C architecture designs. In the case studies we analyzed different DiD properties, e.g., electrical isolation, communication independence, diversity, safety classification, and failure tolerance.

The development of the overall I&C architecture is an iterative process. The architecture is constantly updated as the design progresses. A well-defined work process and practical tools for analyzing and demonstrating that the different iterations all fulfill the DiD principles are imperative. In this paper, we also outlined a work process and presented different tools used during the case studies.

ACKNOWLEDGMENTS

Our work has been funded by the Finnish Research Programme on Nuclear Power Plant Safety 2019-2022 (SAFIR2022).

REFERENCES

1. International Atomic Energy Agency, "Approaches for Overall Instrumentation and Control Architectures of Nuclear Power Plants," Nuclear Energy Series NP-T-2.1 (2018). https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1821_web.pdf.
2. Multinational Design Evaluation Programme, Common Position on Safety Design Principles and Supporting Information for the Overall I&C Architecture. Tech. Rep. DICWG No. 9. OECD (2015).
3. WENRA, "Safety of new NPP designs - Study by Reactor Harmonization Working Group RHWG," Technical Report, Western European Nuclear Regulators' Association, (2013).
4. N. Shadbolt, T. Berners-Lee, W. Hall, "The Semantic Web revisited," *IEEE Intelligent Systems* **21**, pp. 96–101 (2006). doi:10.1109/MIS.2006.62.
5. W3C, SPARQL 1.1 Query Language, W3C Recommendation. The World Wide Web Consortium URL: https://www.w3.org/TR/sparql11-query/ (2013).
6. T.R. Gruber, "A translation approach to portable ontology specifications," *Knowledge Acquisition* **5**, pp. 199–220 (1993). https://doi.org/10.1006/knac.1993.1008.
7. W3C, OWL 2 Web Ontology Language Document Overview (2nd Edition), W3C Recommendation, The World Wide Web Consortium, https://www.w3.org/TR/owl2-overview/. (2012).
8. International Atomic Energy Agency, "Exploring Semantic Technologies and Their Application to Nuclear Knowledge Management," Nuclear Energy Series NG-T-6.15 (2021). http://www-pub.iaea.org/MTCD/Publications/PDF/P1899_web.pdf.
9. A. Pakonen, T. Mätäsniemi, "Ontology-based approach for analyzing nuclear overall I&C architectures," *in: The 47th Annual Conference of the IEEE Industrial Electronics Society* (IECON 2021) (2021). doi:10.1109/IECON48115.2021.9589078.
10. P. Humalajoki, I. Niemelä, "NPP failure analyses in Finland," in *PSAM 14 - Probabilistic Safety Assessment and Management, International Association for PSAM* (2018).
11. STUK, "Safety design of a nuclear power plant," YVL Guide B.1, Radiation and Nuclear Safety Authority (2019). URL: https://www.stuklex.fi/en/ohje/YVLB-1.
12. U.S.NRC, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems", NUREG-Series Publications NUREG/CR-6303, UCRL–ID–119239, U.S.NRC (1994). https://www.nrc.gov/docs/ML0717/ML071790509.pdf.
13. EPRI, "Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital Upgrades: Applying Risk-Informed and Deterministic Methods," NUREG-Series Publications 1002835. EPRI, Palo Alto, CA. (2004). URL: https://www.nrc.gov/docs/ML0505/ML050540262.pdf.
14. H.W. Huang, C. Shih, S. Yih, M.H. Chen, "Integrated software safety analysis method for digital I&C systems," *Annals of Nuclear Energy* **35**, pp. 1471–1483 (2008). doi: 10.1016/j.anucene.2008.01.009.
15. J.E. Holmberg, O. Bäckström, M. Porthin, T. Tyrväinen, "Application of PRA for the assessment of defence-in-depth of a nuclear power plant," in: *Walls L, Revie M, Bedford T, editors, Risk, Reliability and Safety: Innovating Theory and Practice*. CRC Press, pp. 728–735 (2016). doi:10.1201/9781315374987-110.
16. J.E. Holmberg, A. Helminen, M. Porthin, "Using PRA to assess defence-in-depth — case study on level 2 of defence-in-depth," Risk Pilot Report 14127_R002. Risk Pilot, (2017).

17. J. Kim, M.G. Park, "Formal development of an operation monitoring and control system for nuclear reactors using event-b method," *International Journal of Energy Research* **44**, pp. 8170–8180 (2020). https://doi.org/10.1002/er.5262.
18. N.M. Meenachi, M.S. Baba, "Development of Semantic Web-based Knowledge Management for Nuclear Reactor (KMNuR) Portal," *DESIDOC Journal of Library & Information Technology* **34**, pp. 426-434 (2014). 10.14429/djlit.34.7002.
19. Y. Choi, M.D. Nguyen, T.N. Kerr, "Syntactic and semantic information extraction from NPP procedures utilizing natural language processing integrated with rules," *Nuclear Engineering and Technology* **53**, pp. 866–878 (2021). https://doi.org/10.1016/j.net.2020.08.010
20. A. Pruttianan, N. Lau, S. Anders, M. Weinger, "Ontology to guide scenario design to evaluate new technologies for control room modernization," in: *10th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies,* NPIC and HMIT 2017, pp. 206–214 (2017).
21. Z. Ma, M.J. Schultz, K. Christensen, M. Værbak, Y. Demazeau, B.N. Jørgensen, "The application of ontologies in multi-agent systems in the energy sector: A scoping review," *Energies* **12** (2019). doi:10.3390/en12163200.
22. P. Shi, J. Huo, Q. Wang, "Constructing ontology for knowledge sharing of materials failure analysis," *Data Science Journal* **12**, pp. 181 – 190 (2014). https://doi.org/10.2481/dsj.12-047
23. U.S.NRC, ORNL, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," NUREG-Series Publications NUREG/CR-7007 ORNL/TM-2009/302. U.S.NRC (2008). https://www.nrc.gov/docs/ML1005/ML100541256.pdf .
24. D. Wiśniewski, J. Potoniec, A. Ławrynowicz, C.M. Keet, "Analysis of ontology competency questions and their formalizations in SPARQL-OWL," *Journal of Web Semantics* **59**, (2019). doi:10.1016/j.websem.2019.100534.
25. W3C, Resource Description Framework (RDF). The World Wide Web Consortium URL: https://www.w3.org/RDF/ (2014).
26. RML.io, "Easily generate high-quality knowledge graphs with RML.io," IDLab - imec - Ghent University, https://rml.io/ (2022).
27. OTTR, "Reasonable Ontology Templates (OTTR)," https://www.ottr.xyz/ (2021).
28. GraphDB, "Semantic Graph Database," Ontotext, https://graphdb.ontotext.com/ (2022).
29. M.A. Musen, Protégé Team, "The Protégé project: A look back and a look forward," *AI matters* **1**, pp. 4–12 (2015). doi:10.1145/2757001.2757003.
30. Areva NP. U.S. EPR Final Safety Analysis Report (2013). [Online]. Available: https://www.nrc.gov/reactors/new-reactors/design-cert/epr/reports.html
31. NuScale SMR, "Design Certification Application – NuScale", https://www.nrc.gov/reactors/new-reactors/smr/nuscale.html (2022).
32. U.S.NRC, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems," USNRC STANDARD REVIEW PLAN NUREG-0800, Chapter 7, Branch Technical Position (BTP) 7-19,Revision 5. U.S.NRC, (2007). https://www.nrc.gov/docs/ML0705/ML070550072.pdf.