Ontology-based approach for analyzing nuclear overall I&C architectures

Antti Pakonen, Teemu Mätäsniemi
VTT Technical Research Centre of Finland Ltd., Espoo, Finland
Email: antti.pakonen@vtt.fi, teemu.matasniemi@vtt.fi

IECON 2021 - 47th Annual Conference of the IEEE Industrial Electronics Society | 978-1-6654-3554-3/21/$31.00 ©2021 IEEE | DOI: 10.1109/IECON48115.2021.9589078

***Abstract*—Nuclear power plants have many different instrumentation and control (I&C) systems. Together, these systems (and their various dependencies) form the overall I&C architecture, which needs to fulfill the principle of defence-in-depth. The safety systems need to be sufficiently independent from the normal operation systems to avoid common cause failure.**

Semantic Web technologies use formal conceptual models—ontologies—to associate meaning with unstructured data. The knowledge base is built on named graphs, allowing complex queries with reasoning. The results are based on more than just statistical patterns.

In this paper, we demonstrate the use of an OWL ontology to represent engineering knowledge about overall nuclear I&C architectures. We show how, using flexible SPARQL queries, we can then analyse the different dependencies between the I&C systems. We have built a public case study based on a proposed pressurised water reactor type. We detected several potential design issues, which suggests the approach could improve nuclear safety and support design work.

***Index Terms*—Control systems, Systems architecture, Semantic Web, Nuclear power generation**

I. Introduction

The overall instrumentation and control (I&C) system architecture of a nuclear power plant (NPP) has to fulfill the safety principle of defence-in-depth (DiD). Defence-in-depth is the primary means of preventing accidents and mitigating the potential consequences of accidents [1]. It is based on multiple successive layers of protection (DiD levels) independent of each other.

However, total independence of the DiD levels is practically impossible. If each I&C system would have its own instrumentation, human-machine interface (HMI), power supply, etc., the overall architecture would not just be prohibitively costly, but also complex, and difficult to operate or maintain—i.e., potentially less safe [2].

In designing the overall I&C architecture, it is nevertheless crucial to ensure that the key safety requirements are achieved and can be justified [1]. The attention to detail needs to be the same as it is for the system of the highest safety class connected to the architecture [3]. As the design proceeds, and new details about the plant and its I&C systems become available, the architecture needs to be continuously re-evaluated [2]. Proper tool support is therefore paramount.

Knowledge management in nuclear organisations is often centered around organisational and thematic structures [4]. Information security concerns, intellectual property rights, and commercial interests of different stakeholders limit the distribution of information [4]. The industry is relatively conservative in adopting new technology, and the operated systems are sometimes "on the brink of obsolescence" [4].

Information related to the overall I&C architecture can therefore be scattered in different documents and systems. Information models, if they exist, can be focused on some particular view (e.g., functional vs. physical). To search and combine the pieces of information into valuable knowledge, we look to the Semantic Web.

The Semantic Web [5] is based on a vocabularies of shared domain concepts and their relationships, i.e., ontologies [6]. An ontology language like OWL [7] can be used to formally express the "meaning" of terms and their logical connections, enabling machine interpretation. A knowledge base based on Semantic Web technology runs on directed graphs, and can answer complex queries.

In a context broader than just I&C, it has already been shown [4] that Semantic Web techniques can be useful in building rich knowledge models in nuclear applications.

In this paper, we present a method for ensuring that the design solutions related to nuclear overall I&C architectures are safe. We use a Semantic Web ontology to represent knowledge over the architectures, in order to analyze properties related to defence-in-depth. We have built a public case study around the proposed US variant of the European Pressurised Water Reactor. We demonstrate how, based on an OWL ontology, we can flexibly specify SPARQL [8] queries addressing the different dependencies between I&C systems in the architecture.

We introduce DiD requirements for overall I&C nuclear architectures in Section II. We then briefly introduce Semantic Web ontologies in Section III, and related research in Section IV. In Section V, we describe our exemplar ontology, and in Section VI, our case study. We discuss our results in Section VII, and present our conlusions in Section VIII.

II. Nuclear overall I&C architectures

According to an IAEA report on the topic [2], the overall I&C architecture of a nuclear power plant is "the organization of the complete set of I&C systems important to safety". This organisations includes the identification, classification and segmentation of the systems, and the communication pathways and signal handling. Architectural decisions include:

- 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
- the degree of separation between the safety channels [2]

The Fukushima Da-ichi accident in 2011 highlighted the importance of properly implementing the DiD principle [2]. Accordingly, the Western European Nuclear Regulators' Association (WENRA) has proposed a refined DiD structure for new reactor designs [1]. The DiD levels (and their associated plant condition categories) are:

1) Prevention of abnormal operation and failures (normal operation)
2) Control of abnormal operation and failures (anticipated operational occurrences)
3) Control of accident to limit radiological releases and prevent escalation to core melt conditions (3a: single initiating events, 3b: multiple failure events)
4) Control of accidents with core melt to limit off-site releases (core melt accidents)
5) Mitigation of radiological consequences of significant releases of radioactive material [1]

The means to achieve independence between the I&C systems on the different layers are *separation* (consisting of *physical separation*, *electrical isolation*, *functional independence*, *independence of communication*, and *independence of supply systems*), and *diversity* [1], [2].

Physical separation is achieved trough distance and/or structural barriers.

Electrical isolation ensures that an electrical fault in one system does not degrade a connected system.

Functional independence means that the system can complete its functions without depending on information derived from another system.

Independence from errors in data communication can be achieved by guaranteed one-way communication, or deterministic data communication protocol.

Independence of support systems ensures that failures are not propagated through, e.g., shared power supply systems, or heating, ventilation, and air conditioning (HVAC) systems.

Diversity—the use of different technologies or design principles in, e.g., backup systems—offers protection against common cause failure (CCF) [9].

In our approach, we aim at checking requirements related to all of the above-mentioned aspects of the design.

III. Semantic Web Ontologies

The Semantic Web [5] aims to derive information from the (often ill-structured and informal) Web through a semantic theory for interpretation. By formally expressing the "meaning" of the terms and their logical connections, we enable 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. The vision is that intelligent software agents could recognise and create new, valuable knowledge by merging, categorizing, and synthesizing scattered information [4].

The Semantic Web relies on the standards organisations like the World Wide Web Consortium (W3C) to specify and develop languages to serve as the foundation [5].

An *ontology* is defined as vocabulary for a shared domain of discourse [6], containing definitions of classes, individuals, and relationships between them. Ontology languages like OWL [7] aim at machine interpretability by having more structures for expressing meaning (semantics) than languages like XML or Resource Description Framework (RDF). OWL supports different types of inference, e.g., subsumption and classification, and several OWL reasoners have been developed [5]. Formally, OWL is an extension of RDF [7]. A *knowledge base* (containing individuals of the classes the ontology defines) can then be built on RDF triples—as a directed, labeled graph. SPARQL [8] is a query language for RDF graph patterns.

A knowledge base consists of two components, sometimes referred to as *TBox* and *ABox* [10]. The TBox statements describe general properties of concepts by defining sets of individuals in terms of their properties. The ABox comprises assertions on individual objects—statements about individuals belonging to the sets described in the TBox.

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. However, Shapes Constraint Language (SHACL) [11] aids in data graph validation against suitable constraints, and a SHACL processor can automatically produce a validation report.

IV. Related research

Ontologies have been applied in the nuclear I&C domain in a few studies, with different viewpoints.

Recently, an ontology for nuclear deployment called DIAMOND is introduced in [12]. To facilitate the integration of plant data from various IT systems, the authors have designed an OWL ontology using the Protégé [13] ontology editor. The ontology also includes I&C specific concepts (instruments such as gauges, their status and current measured value, manufacturer, location, configuration, etc.), but the overall focus is on operations and maintenance, not on design. The design aspect is mentioned in the scope of future work [12].

In [14], controlled natural language is used to express functional requirements for I&C systems, in order to facilitate formal verification of application software design. The experimental tool in [14] relies on a domain ontology to specify the allowed verbs and property names for the controlled language. Compared to our work on the (non-functional) requirements for the overall architecture level, the focus is on (functional) requirements for the control logic within one I&C system.

Other studies on ontologies in the nuclear I&C domain are similarly not focused on overall I&C architectures, and, instead of an expressive ontology language, simply rely on a XML vocabulary (examples include [15] on Safety Analysis Reports (SAR), [16] on the licensing review process, and [17] on managing aging relay equipment).

Reasons why an ontology suitable for our purpose has not yet been developed, could include: (1) the niche market for such an ontology, (2) the nuclear industry being conservative in adopting novel technologies [4], and (3) many architecture level issues only receiving more attention after the relatively recent adoption of digital I&C in safety systems (leading to highly integrated and interdependent architectures) [2].

For a recent overview on semantic technologies in the nuclear domain, see also [4]. For a comprehensive list of I&C related ontology projects in other industrial domains, see [18].

Like this paper, [19] deals with assessing DiD related properties for nuclear overall I&C architectures, but the analysis was based on Architecture Analysis and Design Language (AADL). AADL was found lacking features that would support analysis on the system-of-systems level, and more suited for analysing different aspects of individual I&C systems.

Our work is an example of deterministic analyses, where we check whether or not a certain dependency exists. Another question is the assessing the likelihood that the dependency causes unacceptable risks for overall safety. Probabilistic safety assessment (PSA) methods (e.g., [20]) are useful in identifying weaknesses, and determining risk impacts. Realistic assessment of overall safety would require a balanced combination of both deterministic and probabilistic approaches [21].

V. Overall I&C Architecture ontology

A. Competency questions

The knowledge base is expected to answer queries related to six categories:

1) physical separation,
2) electrical isolation,
3) communication independence,
4) diversity,
5) safety classification, and
6) failure tolerance

For each of these topics, we listed competency questions (CQ) [22]. The full list is available online[1]. Examples of questions in each of the above category are:

CQ1.2: Is there equipment belonging to system A in the same physical space (building / room / cabinet / rack) as equipment belonging to system B, which is meant to be separated from system A?

CQ2.1: Is there electrical isolation in interfaces between safety-classified and non-safety-classified systems?

CQ3.1: Is there an interface between systems in different safety classes, so that information flows from lower to higher safety class?

CQ4.3: Are there support systems common to systems that have been allocated diverse functions?

CQ5.1: If equipment (including support systems) has been allocated a function of certain safety class, is its safety classification the same or higher?

CQ6.2: Are there at least as many redundant components within a system as is the specified number of redundant divisions for that system?

B. TBox—the classes

The ontology class structure and the object relationships are based on previous conceptual work on I&C DiD modelling [23], and a previous case study built around the planned Hanhikivi-1 NPP using UML [24].

As illustrated in Figure 1, there are three main classes: *FunctionalEntity*, *PhysicalEntity*, and *Classification*.

FunctionalEntity covers initiating events, DiD levels, and I&C functions (and their parts and connections).

PhysicalEntity covers I&C systems (and the interfaces between them), I&C devices (e.g., sensors, processors, actuators, HMI panels...), and support systems (e.g, power supply, HVAC...).

Classification has subclasses such as *SafetyClass*, *SeismicCategory*, which can be applied to either the functional or the physical entities. There are also concepts for describing the *Technology* used to implement the systems.

Some key data and object properties are also shown in Figure 1. (See also Figure 4.)

We built the TBox using Protégé [13], and the OWL file is available online[1].

VI. Case study

A. U.S. EPR

We have built our case study around the proposed US variant of the European Pressurised Water Reactor (U.S. EPR). The U.S. Nuclear Regulatory Commission has published sections of the Final Safety Analysis Report (FSAR) online [25].

A simplified view of the overall I&C architecture is shown in Figure 2. Only a part of the I&C systems are shown.

The DiD architecture (Figure 3) consists of three lines of defence [26]:

- Preventive Line
- Main Line
- Risk Reduction Line

An example of a deliberate design choice against total independence of the DiD levels is that a Preventive Line normal operation system (PAS) shares actuators with the Main Line safety systems (PS and SAS). Therefore, the prioritisation logic—PACS—plays an important role ensuring that the Main Line systems can always control accidents.

The Diverse Actuation System (DAS) is not shown in Figure 2. To account for the potential common cause failure of the (software-based) Main Line systems, the non-programmable DAS performs diverse reactor trip and cooling functions. (DAS is actually not a separate system, but a non-safety-classified part of PAS based on hardwired logic [26].)

Failure tolerance within an I&C system is achieved trough redundancy—having several redundant subsystems placed in physically separated divisions. Main Line systems PS and SAS have four redundant divisions, while select systems such as PICS have two.

[1] The competency questions, OWL files, and SPARQL queries for our case study are available at: https://doi.org/10.5281/zenodo.5010644

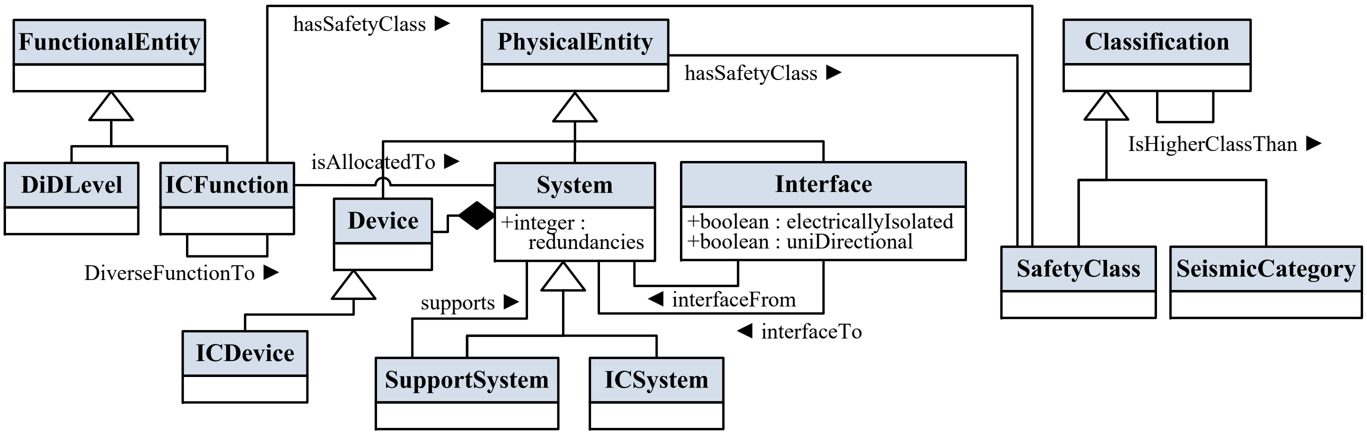


Fig. 1. Key classes and properties from our ontology.

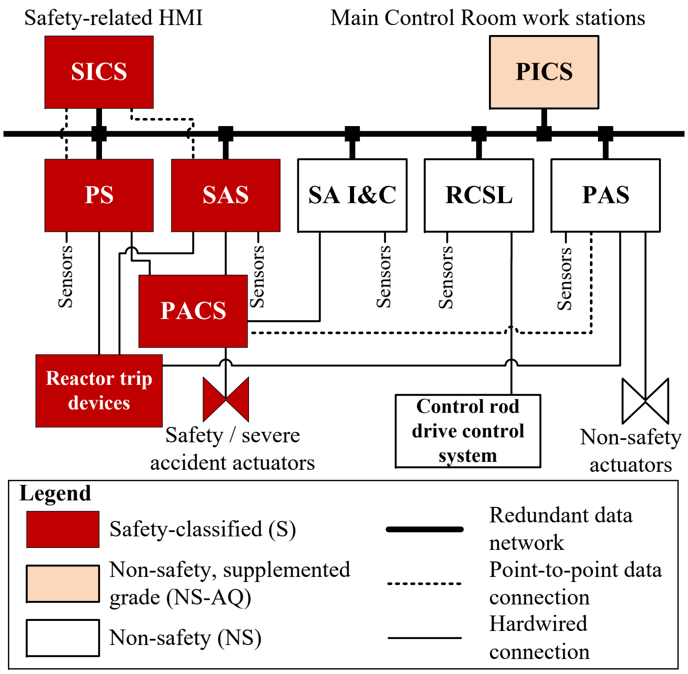


Fig. 2. Overall I&C architecture of the U.S. EPR (modified from [25])
PAS = Process Automation System
PACS = Priority and Actuator Control System
PICS = Process Information and Control System
PS = Protection System
RCSL = Reactor Control, Surveillance and Limitation System
SA I&C = Severe Accident I&C
SAS = Safety Automation System
SICS = Safety Information and Control System

Using WENRA's DiD structure [1], the Preventive Line would correspond with lines 1 and 2, the Main Line with line 3(a), and the Risk Reduction Line with line 4. (As such, the U.S. EPR DiD architecture would not necessarily fulfill the current requirements in Western Europe.)

Although an U.S.EPR project was never commissioned, EPR plants have been built in China, and are under construction in Finland, France, and the UK. The design solutions used in the overall I&C architecture to address DiD requirements are similar in type to those used in other modern reactor types.

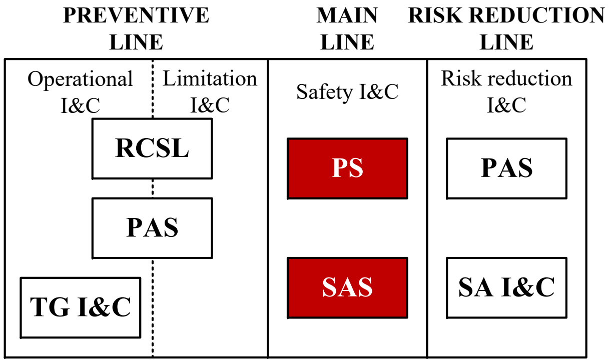


Fig. 3. The Defence-in-Depth lines for the U.S. EPR overall I&C architecture (modified from [26])
TG I&C = Turbine Generator I&C

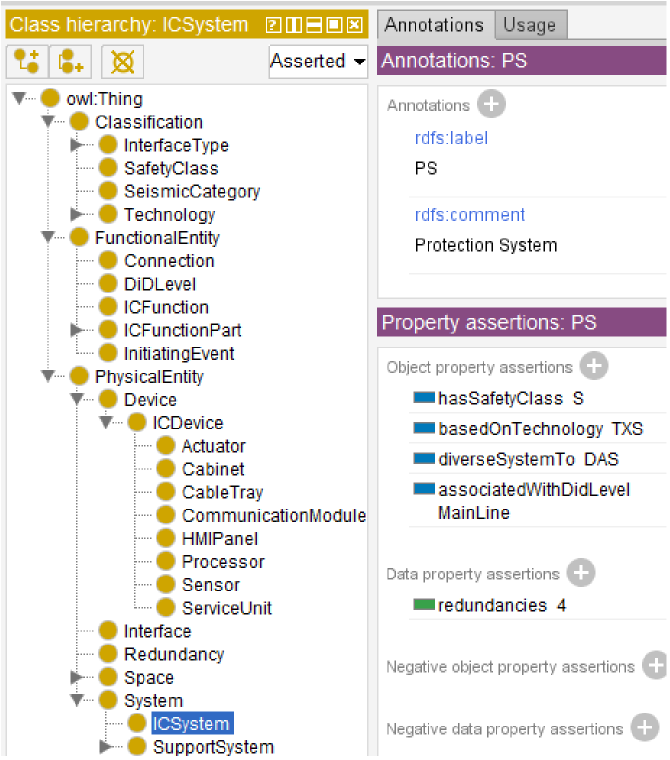
B. ABox—the individuals

From the FSAR, we were able to collect data on 24 I&C systems, 156 I&C functions, 35 system interfaces, and around 400 input/output (I/O) points (not counting the 4-fold redundancy used for many measurements). However, the documents only list the I/O points for two Main Line systems: PS and SAS. We could therefore not base any DiD related checks on the I/O point data.

We assigned identifiers for the functions and interfaces. We assumed, e.g., the safety classification of each function. We also defined requirements for the overall architecture not specified in the FSAR itself.

We collected the data into MS Excel sheets for easy manipulation, and used Excel's string parsing functions to generate the RDF/OWL triplets for the ABox. The OWL file is available online[1].

The property assertions for PS are shown in Figure 4, along with a partial view of the TBox class hierarchy in Protégé.



```
owl:Thing
  Classification
    InterfaceType
    SafetyClass
    SeismicCategory
    Technology
  FunctionalEntity
    Connection
    DiDLevel
    ICFunction
    ICFunctionPart
    InitiatingEvent
  PhysicalEntity
    Device
      ICDevice
        Actuator
        Cabinet
        CableTray
        CommunicationModule
        HMIPanel
        Processor
        Sensor
        ServiceUnit
    Interface
    Redundancy
    Space
    System
      ICSystem
      SupportSystem
```

Annotations: PS

Annotations
rdfs:label
PS
rdfs:comment
Protection System

Property assertions: PS

Object property assertions
hasSafetyClass S
basedOnTechnology TXS
diverseSystemTo DAS
associatedWithDidLevel MainLine

Data property assertions
redundancies 4

Negative object property assertions

Negative data property assertions

Fig. 4. Partial view of the class hierarchy in Protégé, and property assertions for the $ICSystem$ individual PS.

C. SPARQL queries

The full list of SPARQL queries is available online[1], along with our notes on the query results.

The prefixes used in the examples below are:

```
rdf: <http://www.w3.org/1999/02/
      22-rdf-syntax-ns#>
rdfs: <http://www.w3.org/2000/01/rdf-schema#>
```

In addition, the empty prefix : refers to our TBox, and the prefix USEPR: to our ABox.

The first example is for a CQ on electrical isolation: "Is there equipment in support systems that support two different I&C systems that are meant to be electrically separated?". In the query, we look for two I&C systems, where exactly one of them is safety class S, so that there is a single system or device that provides support (power supply, HVAC, etc.—any $subPropertyOf$ $supports$) to both I&C systems:

```
SELECT ?equipment ?systemA ?systemB
WHERE {
  ?systemA rdf:type :ICSystem.
  ?systemA :hasSafetyClass USEPR:S.
  ?systemB  rdf:type :ICSystem.
  MINUS {?systemB :hasSafetyClass USEPR:S}.
  ?supportRel rdfs:subPropertyOf* :supports.
  ?equipment ?supportRel ?systemA.
  ?equipment ?supportRel ?systemB
}
```

The second example is for a CQ on communication independence: "Are there interfaces across DiD lines?". In the query, we look for two I&C systems that have an interface, so that the systems are associated with different DiD levels:

```
SELECT ?systemA ?DidLevelA ?systemB
         ?DidLevelB ?interface
WHERE {
  ?systemA :associatedWithDidLevel ?DidLevelA.
  ?systemB :associatedWithDidLevel ?DidLevelB.
  ?interface :interfaceFrom ?systemA.
  ?interface :interfaceTo ?systemB.
  FILTER (?DidLevelA != ?DidLevelB)
}
```

The third example is for a CQ on safety classification: "Are the components of a system of the same (or higher) safety class as the system?":

```
SELECT ?system ?systemSC ?component
         ?componentSC
WHERE {
  ?system rdf:type :ICSystem.
  ?component :partOf+ ?system.
  ?component :hasSafetyClass ?componentSC.
  ?system :hasSafetyClass ?systemSC.
  ?systemSC :isHigherClassThan ?componentSC
}
ORDER BY ?system
```

D. Results

We ran the SPARQL queries in Protégé.

We did not expect the U.S. EPR architecture to necessarily fulfill the requirements we based our SPARQL queries on. Many of the requirements we wrote were not based on the FSAR itself. The objective was to evaluate a technique, not actually assess a real design. We got the following results:

Physical separation: The FSAR does not contain sufficient information about the placement of I&C systems and equipment in rooms, cabinets, or racks.

Electrical separation: Many of the interfaces between safety-classified and non-safety-classified systems are not stated to be electrically isolated in the FSAR.

Communication independence: There is an interface from DAS (safety class NS-AQ) to PACS, SICS, and reactor trip breakers (RTB) (safety class S). We assume that these are deliberate design choices for, e.g., the prioritisation of commands for shared actuators, and SICS is used for monitoring, only. There are also interfaces from RCSL and TG I&C (NS) to PICS (NS-AQ) for monitoring.

Diversity: DAS performs reactor trip functions that are intended diverse to the trip functions implemented in PS. However, both systems use RTB to trip the reactor, and both rely on SICS to implement the manual trip functions.

Safety classification: PS and SAS (S) have components—Gateway and Service Unit—that are non-safety-classified (NS). DAS (NS-AQ) is powered by a NS power supply system.

Failure tolerance: PAS, SAS and RCSL are specified as four-redundant systems, but each have only one Gateway and Service Unit. DAS and SCDS are also specified as four-redundant, but each have two-redundant power supply systems.

VII. Discussion

A. Our contribution

Our experiments showed that OWL supports the kind of machine reasoning over conceptual relationships that is relevant for analyzing requirements related to defence-in-depth. The user can pose questions that require the computer to deduce different classifications and connections, all of which are not explicitly stated in the source data. SPARQL makes it straightforward to pose questions with graph patterns (but whether SPARQL is a particularly user-friendly query language is a subjective matter).

By publishing the all the case study details, we invite other researchers to repeat, question, or further refine our work.

B. Design optimisation

As already stated above, many of our competency questions or SPARQL queries were not based on any requirements stated for the U.S. EPR I&C architecture in the FSAR documents, but our own experience. Our query results are not meant to be interpreted as criticism. The overall I&C architecture of the EPR built in Finland, for example, is also quite different.

Nevertheless, our results illustrate the challenge of optimising the overall I&C architecture. Fore example, DAS is meant to be diverse from PS and SAS, but DAS also shares actuators and HMI with PS and SAS. Although the chain from the sensors (and HMI) to the actuators is based on hardwired logic (and therefore provides protection against the common cause failure of the software-based PS and SAS), the diverse function—as a whole—still relies on same technology, design principle, supplier, etc..

Still, our query results are not necessarily symptoms of problems, but examples of deliberate design optimisation. The challenge is to build a plant that is economically feasible to construct, operable, maintainable, while also safe. Assessing the safety aspect requires easy access to a large set of data, and running fairly complex chains of reasoning.

C. Further work

In an effort to find the best formal modelling technique for I&C DiD assessment, we will next attempt similar analyses using Prolog [27] and/or algorithms such as Boolean satisfiability (SAT) [28] and Satisfiability Modulo Theories (SMT) [29]. If the Semantic Web approach is found most feasible, we will need to further extend and refine our ontology.

Eventually, we also hope to demonstrate the technique we will find most applicable in the context of real plant project, e.g., the Finnish Hanhikivi-1 NPP.

For the proposed concept to be practically applicable, the query specification and result browsing need to be made user-friendly. An flexible solution is needed for automatically generating the individuals (ABox) based on information that is scattered in different systems, with potentially different interfaces and representation formats.

VIII. Conclusion

In this paper, we demonstrated an approach for analysing safety requirements related to the overall I&C architecture of a nuclear power plant. We used an OWL ontology to facilitate machine reasoning, and then used SPARQL to flexibly specify queries related to defence-in-depth properties—electrical isolation, communication independence, diversity, safety classification, and failure tolerance. In our case study, we detected different potential design issues in the overall I&C architecture design of a proposed NPP type.

The kind of tool we are proposing has a niche market. Defence-in-depth is a principle also applied in other domains (e.g., aviation), but the overall I&C architectures are seldom as complex as they are in a modern nuclear power plant.

Still, safety is not the only justification for paying attention the overall architecture design. In order for the plant projects to be economically viable, the design and the licensing processes need to run smoothly. The overall I&C architecture is an early design input, but it is also constantly updated as the design progresses. Practical tools for analysing and demonstrating that the different iterations all fulfill the DiD principles are a key to success.

Acknowledgment

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

The case study was conducted using the Protégé resource, which is supported by grant GM10331601 from the National Institute of General Medical Sciences of the United States National Institutes of Health.

We wish to thank Akhtar Zeb of VTT for technical support on the case study.

References

[1] WENRA, “Safety of new NPP designs - study by reactor harmonization working group RHWG,” Western European Nuclear Regulators’ Association, Tech. Rep., 2018. [Online]. Available: https://bit.ly/3vHJU1c

[2] IAEA, “Approaches for overall instrumentation and control architectures of nuclear power plants,” International Atomic Energy Agency, Nuclear Energy Series NP-T-2.1, 2018. [Online]. Available: http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1821_web.pdf

[3] STUK, “Safety design of a nuclear power plant,” Radiation and Nuclear Safety Authority, YVL Guide B.1, 2019. [Online]. Available: https://www.stuklex.fi/en/ohje/YVLB-1

[4] IAEA, “Exploring semantic technologies and their application to nuclear knowledge management,” International Atomic Energy Agency, Nuclear Energy Series NG-T-6.15, 2021. [Online]. Available: http://www-pub.iaea.org/MTCD/Publications/PDF/P1899_web.pdf

[5] N. Shadbolt, T. Berners-Lee, and W. Hall, “The Semantic Web revisited,” *IEEE Intelligent Systems*, vol. 21, no. 3, pp. 96–101, 2006.

[6] T. R. Gruber, “A translation approach to portable ontology specifications,” *Knowledge Acquisition*, vol. 5, no. 2, pp. 199–220, 1993.

[7] W3C, “OWL 2 Web Ontology Language Document Overview (second edition),” The World Wide Web Consortium, W3C Recommendation, 2012. [Online]. Available: https://www.w3.org/TR/owl2-overview/

[8] ——, “SPARQL 1.1 Query Language,” The World Wide Web Consortium, W3C Recommendation, 2013. [Online]. Available: https://www.w3.org/TR/sparql11-query/

[9] U.S.NRC, ORNL, “Diversity strategies for nuclear power plant instrumentation and control systems,” U.S.NRC, NUREG-Series Publications NUREG/CR-7007 ORNL/TM-2009/302, 2008. [Online]. Available: https://www.nrc.gov/docs/ML1005/ML100541256.pdf

[10] D. Calvanese, G. De Giacomo, and M. Lenzerini, “Ontology of integration and integration of ontologies.” *Description Logics*, vol. 49, no. 10-19, p. 30, 2001.

[11] W3C, “Shapes Constraint Language (SHACL),” The World Wide Web Consortium, W3C Recommendation, 2017. [Online]. Available: https://www.w3.org/TR/shacl/

[12] LWRS, “Data integration aggregated model and ontology for nuclear deployment (DIAMOND): Preliminary model and ontology,” Light Water Reactor Sustainability Program, Technical Report INL/EXT-19-55610, 2019. [Online]. Available: https://bit.ly/33kGci7

[13] M. A. Musen and Protégé Team, “The Protégé project: A look back and a look forward,” *AI matters*, vol. 1, p. 4–12, 2015.

[14] T. Tommila and A. Pakonen, “Controlled natural language requirements in the design and analysis of safety critical I&C systems,” VTT Technical Research Centre of Finland Ltd., VTT Research Report VTT-R-01067-14, 2014. [Online]. Available: https://www.vttresearch.com/sites/default/files/julkaisut/muut/2014/VTT-R-01067-14.pdf

[15] W.-H. Tseng and C.-F. Fan, “Systematic scenario test case generation for nuclear safety systems,” *Information and Software Technology*, vol. 55, no. 2, pp. 344–356, 2013, special Section: Component-Based Software Engineering (CBSE), 2011.

[16] S. Yih and C.-F. Fan, “Analyzing the decision making process of certifying digital control systems of nuclear power plants,” *Nuclear Engineering and Design*, vol. 242, pp. 379–388, 2012.

[17] A. Dourgnon-Hanoune, T. Dang, P. Salaün, and V. Bouthors, “An ontology for I&C knowledge using trees of porphyry,” in *The 8th IEEE International Conference on Industrial Informatics (INDIN 2010)*, 2010, pp. 86–92.

[18] V. R. Sampath Kumar, A. Khamis, S. Fiorini, J. L. Carbonera, A. Olivares Alarcos, M. Habib, P. Goncalves, H. Li, and J. I. Olszewska, “Ontologies for industry 4.0,” *The Knowledge Engineering Review*, vol. 34, p. e17, 2019.

[19] J. Linnosmaa, A. Pakonen, N. Papakonstantinou, and P. Karpati, “Applicability of AADL in modelling the overall I&C architecture of a nuclear power plant,” in *The 46th Annual Conference of the IEEE Industrial Electronics Society (IECON 2020)*, 2020, pp. 4337–4344.

[20] S. Authén and J.-E. Holmberg, “Reliability analysis of a digital systems in a probabilistic risk analysis for nuclear power plants,” *Nuclear Engineering and Technology*, vol. 144, pp. 471–482, 2012.

[21] S. Martorell, P. Martorell, I. Martón, A. Sánchez, and S. Carlos, “An approach to address probabilistic assumptions on the availability of safety systems for deterministic safety analysis,” *Reliability Engineering & System Safety*, vol. 160, pp. 136–150, 2017.

[22] D. Wiśniewski, J. Potoniec, A. Ławrynowicz, and C. M. Keet, “Analysis of ontology competency questions and their formalizations in SPARQL-OWL,” *Journal of Web Semantics*, vol. 59, p. 100534, 2019.

[23] T. Tommila and N. Papakonstantinou, “Challenges in defence in depth and I&C architectures,” VTT Technical Research Centre of Finland Ltd., VTT Research Report VTT-R-00090-16, 2016. [Online]. Available: http://www.vtt.fi/inf/julkaisut/muut/2016/VTT-R-00090-16.pdf

[24] VTT, “SAFIR2022 – the Finnish research programme on nuclear power plant safety 2019-2022 – Interim report,” VTT Technical Research Centre of Finland Ltd., VTT Technology 383, 2021. [Online]. Available: http://www.vtt.fi/inf/julkaisut/muut/2016/VTT-R-00090-16.pdf

[25] Areva NP. (2013) U.S. EPR Final Safety Analysis Report. [Online]. Available: https://www.nrc.gov/reactors/new-reactors/design-cert/epr/reports.html

[26] ——. (2009) U.S. EPR instrumentation and control diversity and defense-in-depth, ANP-10304, revision 0. [Online]. Available: https://www.nrc.gov/docs/ML0915/ML091540425.pdf

[27] W. Clocksin and C. S. Mellish, *Programming in Prolog*, 5th ed. Springer-Verlag Berlin Heidelberg, 2003.

[28] E. Clarke, A. Biere, R. Raimi, and Y. Zhu, “Bounded model checking using satisfiability solving,” *Formal Methods in System Design*, vol. 19, no. 1, pp. 7–34, Jul 2001.

[29] C. Barrett, R. Sebastiani, S. Seshia, and C. Tinelli, “Satisfiability modulo theories,” in *Handbook of Satisfiability*. IOS Press, 2009, pp. 825–885.