# *Harmonization of IEEE 1012 and IEC 60880 standards regarding verification and validation of nuclear power plant safety systems software using model-based methodology*

# Title

Harmonization of IEEE 1012 and IEC 60880 standards regarding verification and validation of nuclear power plant safety systems software using model-based methodology.

# Author names and affiliations

Stanislav Rudakov[1], Charles E. Dickerson[2]

[1]School of Electronic, Electrical and System Engineering, Loughborough University, Epinal Way, Loughborough, Leicestershire, UK, LE11 3TU. Email: Rudakov.Stanislav@gmail.com

[2]School of Electronic, Electrical and System Engineering, Loughborough University, Epinal Way, Loughborough, Leicestershire, UK, LE11 3TU. Email: C.Dickerson@lboro.ac.uk

# Corresponding author:

Stanislav Rudakov

Email: Rudakov.Stanislav@gmail.com

# 1 Introduction

The current civil nuclear market situation is being called a “nuclear renaissance” (World Nuclear Association, 2014) due to the increased number of orders on hand after the long period of market recession and stagnation. Since a nuclear power plant is the object of high-inherited risks, special licensing processes are needed for safety justification. The significance of the licensing for the licensee is important due to the reasons related to regulatory risks presented in table 1 (Söderholm, 2013):

| **Regulatory risks** | **Consequences** |
|---|---|
| License(s) delayed | Delay in schedule, cost overrun (financing costs) |
| Substantial re-design required in licensing process | Cost overrun, delays, trouble with vendor, contract disagreement |
| Construction license not granted | Loss of investment incurred until then |
| Regulatory approvals during construction not granted | Cost overrun, delays |
| Operating permit not granted | Stranded investment |
| License(s) cancelled by court of law | Delay (if amended license is issued) loss of investment (if not) |

Table 1. Regulatory risks and theirs consequences

Weak preparation for the licensing and improper following of the standards by a project participant and/or ambiguous requirements set by the regulatory documents might lead to significant revenue losses. Such an example is a current construction of the Olkiluoto nuclear power plant (NPP), Finland, where reactor instrumentation and control (I&C) system architecture was approved years later than it was expected, which led to reputational and financial damages (World Nuclear Industry Status Report, 2014).

Current trends of the commercial nuclear industry include:

- Cost overruns and operation delays due to the licensing issues;
- Emergence of the countries with a lack of the nuclear experience;
- Extreme growth of international collaboration within new nuclear build projects.

Clearly, these trends either directly or indirectly relate to legislative issues. A unified, transparent legislative base might then be a solution for the whole market, which would:

- Decrease the overall cost of the project due to the lack of necessity of compliance to several regulation environments;
- Facilitate the enactment of regulation for countries without nuclear experience;
- Facilitate the mutual work and understanding between international partners;
- Establish unified common practices of legislation compliance evaluation.

Calls for transparent and unified regulations have been made for years by the establishment of working groups such as MDEP, WENRA, and CORDEL. Despite all efforts, Söderholm (2013) states

that harmonization of regulations is a very challenging and slow process in Europe, which is even slower on the world-wide scale.

In keeping with this multinational movement of regulations convergence, the aim of this paper is to create a harmonized core between IEC and IEEE regulations with regard to the verification and validation processes (V&V) of safety systems software. Heimdahl (2007) claims that V&V processes usually constitute up to 50-70 % of development life cycle. Thus, V&V processes can be regarded as the most important aspect during the development of critical software. In this paper, it will be assumed that the V&V life cycle spans the phases from requirements engineering to the start of operation.

Thomson (2012) claimed that no one-to-one mapping between IEC and IEEE regulations within I&C software can be found since they cover different topics. At the same time, a group of Russian experts (Anokhin et al., 2009) noticed some intersections amongst them.

The objective of the paper is to define a common ground (shared processes and objects) between IEC and IEEE regulations in the context of software verification and validation, as well as their correlation, and to show how the rigorous model-based methodology can be applied for the legislation harmonization in the rest of the subjects.

## 2 Nuclear power plant instrumentation and control systems

I&C systems measure and assess technological parameters of nuclear power plant processes, initiate and control equipment actuation, provide forecasts and post analysis. The significance of I&C systems can be different since each of them addresses different functions in terms of overall plant safety and importance. The International Atomic Energy Agency (IAEA), the top-level governing body for all participants of the civil nuclear market, breakdowns all I&C systems in two broad classes: systems important to safety and systems not important to safety. The first one in its own turn is divided to safety and safety related systems (IAEA NS-G-1.3, 2002).

In accordance with IAEA, the principle of distinguishing between safety and safety related system is as follows (IAEA NS-G-1.3, 2002):

1. ‘I&C safety systems’ are I&C systems important to safety that perform the primary safety functions i.e., they assure the safe shutdown of the reactor or the removal of residual heat from the core, or they limit the consequences of anticipated operational occurrences and design basis accidents;
2. ‘Safety related I&C systems’ are I&C systems important to safety that perform other functions important to safety which are not performed by I&C safety systems.

The IAEA classification of the NPP I&C systems is not the only one. There are at least dozen others, which are implemented in particular regions or countries. Next table 2 shows other classifications with rough comparison among them completed by IAEA (IAEA NP-T-3.12, 2011):

<table>
<tr><th>National or international standard</th><th colspan="4">Classification of the importance to safety</th></tr>
<tr><td rowspan="2">IAEA NS-R-1</td><td colspan="3">Systems Important to Safety</td><td rowspan="2">Systems Not Important to Safety</td></tr>
<tr><td colspan="2">Safety</td><td>Safety Related</td></tr>
<tr><td rowspan="2">IEC 61226 Functions</td><td colspan="3">Systems Important to Safety</td><td rowspan="2">Unclassified</td></tr>
<tr><td>Cat. A</td><td>Cat. B</td><td>Category C</td></tr>
</table>

| Systems | Class 1 | Class 2 | Class 3 | |
|---|---|---|---|---|
| Canada | Category 1 | Category 2 | Category 3 | Category 4 |
| France N4 | 1E | 2E | SH / Important to safety | Systems Not Important to Safety |
| European Utility Requirements | F1A (Auto) | F1B (Auto and Man.) | F2 | Unclassified |
| Japan | PS1/MS1* | PS2/MS2 | PS3/MS3 | Non-nuclear Safety |
| Rep. of Korea | IC-1 | IC-2 | | IC-3 |
| Russian Federation | Class 2 | Class 3 | | Class 4 (Systems Not Important to Safety) |
| Switzerland | Category A | Category B | Category C | Not Important to Safety |
| UK Functions Systems | Systems Important to Safety | | | Unclassified |
| | Cat. A Class 1 | Cat. B Class 2 | Category C Class 3 | |
| USA and IEEE | Systems Important to Safety | | | Non-nuclear Safety |
| | Safety Related, Safety or Class 1E | (No name assigned) | | |

Table 2. I&C systems/functions classification

Comparison can be made only within similar boundary of the functional determination. From table 2, it is seen that the classes listed above do not strictly correspond to each other; but at least they share a subset of the most critical I&C systems.

The most noticed, quoted and widely applied regulatory documents can be found within IEEE and IEC families of standards. IEC is mostly popular throughout the European market, whilst implementation of IEEE standards usually can be found in the USA and other parts of the world.

Attention from the regulatory bodies to the software is caused by software hidden complexity, which are summarised in the following issues (Yastrebenetsky and Kharchenko, 2014):

1. Software as a part of bigger system shall comply with system regulations;
2. Software defects are likely to occur, which makes them a common cause failure;
3. The use of a software tools for software development can introduce errors;
4. Reliability of software seems to be impossible to calculate.

The International Electrotechnical Commission covers issues related to the software executing “A” category functions in the corresponding standard IEC 60880. Institute of Electrical and Electronics Engineers addresses software issues in the umbrella standard IEEE Std 7-4.3.2, where diverse topics including software & hardware quality, reliability, and common cause failure protection are discussed. However, in terms of V&V aspects, it prescribes to use IEEE 1012.

Wood, Halcomb, Johnson, Korsah have built standards’ profiles for both IAEA/IEC and IEEE/NRC regulations where in the context of V&V requirements for safety systems software they made a correspondence between IEEE 1012 and IEC 60880 (Wood et al., 2009). Those standards have been chosen for the common ground determination by implementation of a rigorous methodology

# 3 Methodology

It is commonly known that the reading of standards can easily lead to misunderstanding and loss of some important aspects of meaning: standards can often be inconsistent with themselves and contain many errors and much ambiguity; furthermore, it can be almost impossible to follow the standards when they are read in groups due to diversity of interpretation (Holt and Perry, 2008).

Due to listed drawbacks of the standards, one approach which can be taken to address the issues is model-based systems engineering (hereinafter, modelling), as models can provide information in a more intuitive and less entangled manner. Holt and Perry (2008) state that modelling could serve as a common language of standards creation. Their proposed so-called seven-view approach to the modelling processes can be also applied to the modelling of standards.

A group of experts from Finland (Lahtinen et al., 2010) conducted research related to the search for a common ground amongst some civil nuclear standards, comparing textual requirements by subject-matter expertise analysis. In such a case, the way proposed by Holt and Perry for using a model-based approach to describe standards could support consideration and analysis of existing standards and be more rigorous.

In this paper, a model-based approach will be used for the analysis and harmonization of V&V systems embodied in two different IEC and IEEE standards discussed above. We propose the following methodology:

1. Select a standard to be used as a reference model;
2. Perform requirements analysis of both standards;
3. Develop behavioural and structural SysML models of the reference standard based on the requirements analysis (modelling of the process flows and objects);
4. Verify the SysML model of the reference standard;
5. Apply requirements of another standard to the reference model.

IEC 60880 has fewer requirements regarding V&V processes; hence, modelling of the IEC 60880 V&V system seems to be more efficient in terms of common core determination. Thus, IEC 60880 is therefore selected as a reference model, whereas IEEE 1012 is used as a source of requirements to compare two V&V systems

# 4 Rules establishment

High-level constraints and limitations are introduced in order to facilitate the consideration of the text of each of these standards and to stay within the paper's scope. To this end, the following main rules of clause filtering are introduced (see Table 3):

| Tag | Description | Example |
|---|---|---|
| MR1 | Only "shall" statements are considered, "should" statements are not considered | Code verification activities should begin with module source code analysis followed by module testing |
| MR2 | Statements related to enabling processes are not considered | There shall be adequate provision for the processing and resolution of all safety issues raised during the verification activities performed either during software |

| | | |
|---|---|---|
| | | development by the supplier or by a third-party assessment |
| MR3 | Statements, which describe something from the production life cycle viewpoint rather than from the V&V viewpoint, are not considered | This plan shall specify the standards and procedures to be followed in the system integration |
| MR4 | Statements, related to the V&V methods or techniques instead of the V&V process itself, are not considered | The source code analysis may be performed using verification methods such as code inspection, possibly with the assistance of automated tools |
| MR5 | Statements, which have references to another standards or appendices, are not considered | For further guidance concerning the verification of data produced using application data tools, see 14.3.5. |
| MR6 | Statements considered not relevant such as an examples or explanations are not considered | Other aspects of data may have to be developed from the system requirements, for example the allocation of signal inputs to specific input cards, the contents of message buffers |
| MR7 | Statements with regard to V&V performed by the system V&V team (not the software V&V team) are not considered | The integrated system test shall be reviewed and the test results evaluated by a verification team with a good knowledge of the system specification. |

Table 3. Main rules

The primary problem of text understanding is semantics: some words can be interpreted differently depending on the reader experience in a subject area. Dickerson and Mavris (2009) have presented a practice, where they transformed natural language into the UML class diagrams in order not to introduce any additional information to the model.

Due to the nature of the V&V systems considered, we require that the modelling language needs to allow the modelling of: requirements, operations, control flows, object flows, and objects and actors with their attributes. Based on these needs, the SysML language was chosen for modelling activities throughout a V&V project, using activity, block and requirements diagrams.

The IEC 60880 narrative alternately addresses operations and objects issues; therefore, it is necessary to establish rules for semantical representation of both operations and objects using SysML activity and block diagrams. This transformation must be consistent; otherwise, it would be just a free interpretation done on a case-to-case basis.

Following the ideas proposed by Dickerson and Mavris, the next rules, presented in Table 4, were introduced to represent operations and objects:

| **Tag** | **Description** |
|---|---|
| AR1 | “shall do” statement written in a verb-form is represented as an activity node |
| AR2 | “shall do” statement written in a noun-form is represented as an activity node |

| | |
|---|---|
| AR3 | Statement with two or more operations connected by conjunctive “and” without explicit declaration of their separate execution is considered as a single activity node |
| AR4 | An event interrupting the workflow is represented as interruption node with corresponding control flow and interruptible region |
| AR5 | Options selection regarding any operation is considered as a decision node with corresponding control flows to available options |
| AR6 | Objects representing an information flow are considered as an activity input/output pins |
| BR1 | A set of people, described as a team, or even single individuals, are considered as an actor represented as a block node (in activity diagrams represented as a swim lane if necessary) |
| BR2 | Communication amongst actors is represented as an association relation with attached block describing the attributes of that relation (see BR3) |
| BR3 | A property of a considered association relation amongst actors is considered as an attribute of that relation (see BR2) |
| BR4 | A property of actor, that describes it, or things that actor has in possession, is considered as an attribute of the block representing the actor |
| BR5 | An object mentioned throughout the standard is represented as a block node |
| BR6 | A property of an object that describes it, is considered as an attribute of the block representing the object |
| BR7 | If an object / actor is considered as an important/primary/inalienable part of something, then the part association relation (composition) is used |

Table 4. Interpretation rules

The rules listed in Table 4 define a general transformation from the natural language to the graphical form. However, due to the ambiguity and vagueness of natural language, the certainty of operations/objects/actors considered must be under control, and accordingly represented as well.

An algorithm of object certainty determination and its graphical representation within activity diagrams is presented in Table 5:

| **Decision (to be made)** | **Description** | **Tag** | **Graphical representation** |
|---|---|---|---|
| Was the object defined in the definition chapter? | Reference is given in the definition chapter | D | Filled pin with bold black borders |
| Was the object defined in the text? | Properties are described in the text | DT | Filled pin with regular black borders |
| Was the object separately defined in the definition chapter? | All of N words of the term are defined in the definition chapter, but separately | SD | No representation due to lack of the IEC 60880 SD terms |
| Was the object partly defined in the definition | Equal or less than N-1 words of the term are defined in | PD | White pin with regular black |

| | | | |
|---|---|---|---|
| chapter? | the definition chapter | | borders |
| Was the object implied? | No explicit definition is given | I | White pin with white borders |

Table 5. Objects certainty determination algorithm

This algorithm proceeds downwards through the table until a “yes” answer is achieved. Execution of such an algorithm gives a foundation for dictionary creation, objects certainty, and the corresponding graphical representation in the model. A similar graphical representation has also been developed in the context of block diagrams to distinguish the level of certainty.

Not only objects can have different levels of certainty; but also, the same can be said about operations. Rules regarding the certainty of operations are listed in Table 6:

| **Tag** | **Description** | **Graphical representation** |
|---|---|---|
| DI | Decision is implied | Diamond node with regular contour |
| DE | Decision is explicitly defined | Diamond node with bold contour |
| AI | Activity is implied | Activity node with regular contour |
| AE | Activity is explicitly defined | Activity node with bold contour |
| SI | The sequence of operations is not specified (parallel sequence is assumed with use of forks/joints nodes) | Regular control flow lines and fork/join nodes |
| SE | The sequence of operations is explicitly specified | Bold control flow line |
| SCS | If a sequence of operations is not explicitly specified, but a right sequence is dictated by common sense, then consecutive control flow is used | Regular control flow line |

Table 6. Operations certainty tags determination

# 5 Modelling

## 5.1 IEC 60880 V&V system

All of these rules made a foundation for rigorous graphical representation and further analysis of the IEC 60880 V&V system. The process of IEC 60880 textual requirements analysis is specified by the following three step algorithm by allocation of the:

- Main rules tags if there are any;
- Operation/object tags;
- Certainty level tags.

The next example, presented in Table 7, shows how the allocation of tags proceeds based on clause 8.1.9 from the IEC 60880 standard:

“8.1.9 The software verification activities shall confirm the adequacy of the software requirements specification in fulfilling the system requirements assigned to the software by the system specification.”

| № | Set of words | Type | Tag |
|---|---|---|---|
| 1 | Software requirements specification | Object | BR5, AR6, DT |
| 2 | System specification | Object | BR5, AR6, PD |
| | System requirements | (constituent of system specification) | |
| 3 | Shall confirm the adequacy of the software requirements specification in fulfilling the system requirements assigned to the software by the system specification. | Activity | AR1, AE, SE |

Table 7. Natural language analysis example

As a result, the skeleton of IEC 60880 V&V system model contains the following views:

- Requirements;
- Actor;
- Object;
- Process.

The “Process view” corresponds to a so-called “process behaviour view” in the terms of Holt and Perry approach. The “Actor view” corresponds to the “stakeholder view”, and the “Object view” corresponds to “process-structure view”. The last view, which is not represented in the Holt and Perry structure, is the “Requirements view”, which contains a requirements tree formed of IEC 60880 clauses.

The graphical model in figure 1 shows how the modelling process was performed for the IEC 60880 requirements verification process using the rules established in Tables 4-6 and provides an example of how the graphical elements were drawn based on the allocated tags in Table 7.

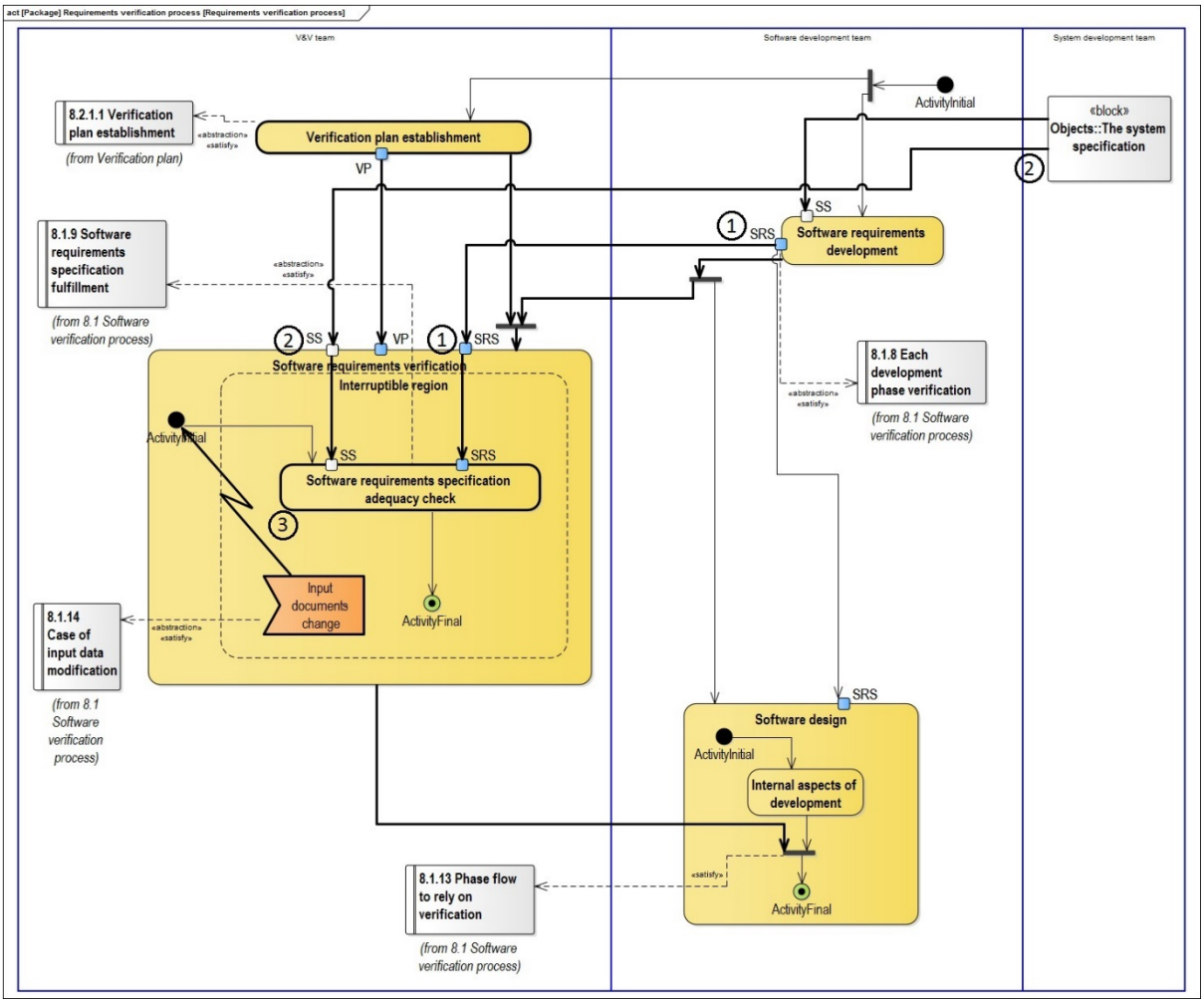



Figure 1. Requirements verification process model

The requirements verification process model was developed by consideration of the following IEC 60880 clauses: 8.2.1.1, 8.1.9, 8.1.8, 8.1.14, 8.1.13. It is shown by white rectangles, with a line inside, connected to the model elements, which act as an integrity check. It was done in order to check that the model does not contain any errors, and therefore is ready for the IEEE 1012 requirements allocation and harmonization.

Next, the following two methods for model verification are introduced:

- An integrity check;
- A consistency check.

The integrity check implies the examination of the model against the requirements on which the model was built. This kind of examination has a reverse character as it allows allocating requirements from the IEC 60880 requirements tree to the model. Allocation is performed by a connection of the requirements nodes to the corresponding model element using the abstraction class of “satisfy”. These connections enable a full traceability between the model and the requirements. To exclude the chance of missed requirements, all of the requirements were scanned one by one using a special specification manager function embedded in a commercial modelling tool. This allows for checking whether each of the requirements is allocated to any element.

The term ‘consistency check’ means the ability to execute processes from the IEC 60880 V&V system model, since this would be the guarantee that the processes are meaningful, coherent and consistent within themselves in terms of formal logic. Such check is performed by special function embedded in the modelling tool, which allows a user to execute created model in an interactive way to ensure the model is correct.

### 5.2 IEEE 1012 V&V requirements tree

In order to allow application of IEEE 1012 requirements nodes to the reference model, the requirements tree of IEEE 1012 chapter 9 “Software V&V activities” was modelled.

It should be mentioned that during the modelling of the IEEE 1012 V&V system requirement tree, requirements related to criticality assessment were omitted due to already defined criticality class by the parent standard, IEEE 7-4.3.2, which is equivalent to the software integrity level 4 (SIL 4) (IEEE 7-4.3.2, 2010).

An IEEE 1012 V&V system dictionary similar to IEC 60880 was developed following the same algorithm described in the table 5.

## 6 V&V systems comparison

Before application of the requirements can be done, a step back should be taken in order to look at the standards from the highest level of consideration in order to understand features. This will affect harmonization.

### 6.1 IEC 60880 V&V system

IEC 60880 standard considers software as a part/element of the bigger I&C system and specifically not as a system in terms of systems engineering concepts (IEC 60880, 2006). Another important aspect of the IEC 60880 standard is the differentiation of software by the type of method used for its creation. These are:

- General-purpose languages;
- Application-oriented languages;
- Configuration of pre-developed software.

### 6.2 IEEE 1012 V&V system

A distinct feature of the IEEE 1012 standard is an existence of four separate phases of software V&V: construction, integration, qualification, and acceptance. The IEEE 1012 standard considers software as a system in terms of systems engineering concepts, and not as an element like it is in IEC 60880. This is based on a strict alignment of the standards to the development processes described in ISO/IEC/IEEE 15288 and ISO/IEC 12207, and due to the life cycle proposed by the IEEE 1012 (IEEE 1012, 2012).

### 6.3 V&V systems correspondence

A significant mismatch among life cycle phases of two V&V systems is observed, although logically they represent the same period of software verification and validation: from the requirements up to the start of operation. Due to the specific features of the standards mentioned above, their life cycles phases correspond to each other in a way depicted in figure 2.

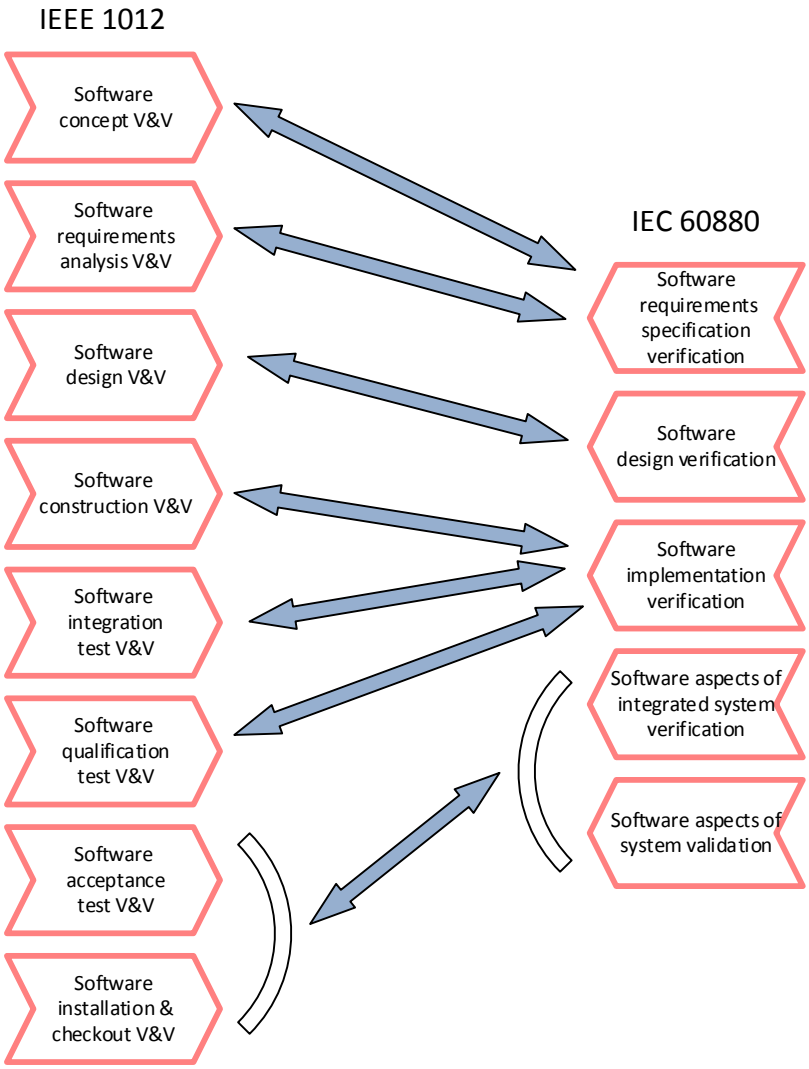



Figure 2. Logical correspondence between two V&V systems

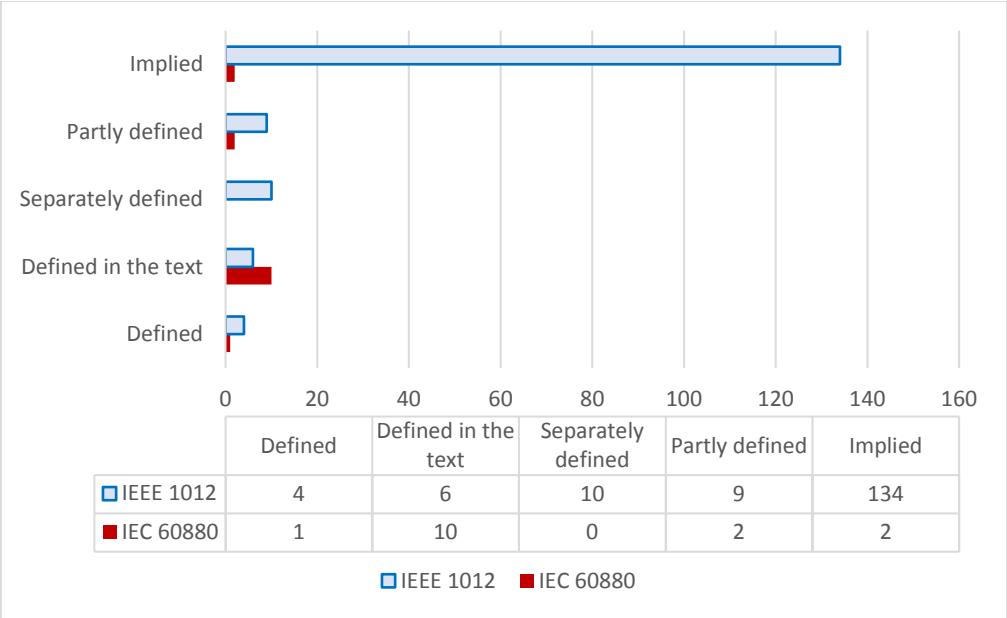
The “IEC 60880 Software requirements specification” phase corresponds to the “IEEE 1012 software requirements analysis V&V” phase; but no direct matching between “IEEE 1012 Software concept V&V” and any of the IEC 60880 phases is found, as IEC 60880 is not concerned about software concept in the context of its semantical meaning taken from the IEEE 1012. One of the most transparent conformities, observed among two V&V systems, is the design phase since “IEEE 1012 Software design V&V” fully corresponds to the “IEC 60880 Software design verification”.

Based on a logical analysis it was found that three IEEE 1012 phases, namely, “software construction V&V”, “software integration test V&V” and “software qualification V&V” could correspond to IEC 60880 implementation verification phase.

The next phases are even more complicated, as no direct connection between the phases can be made. The last phases on both sides correspondence can then only be considered in a blended manner, which is depicted by arcs in figure 2. Such complexity grows from the different approaches regarding the software. IEC 60880 considers it as an element; but IEEE 1012 looks at it as a system. Therefore, it is impossible to untangle the two phases on both sides and match them to another side.

## 6.4 Dictionaries comparison

The last aspect of standards feature considerations is their dictionary comparison. Figure 3 shows the distribution of objects involved in V&V processes in the context of their certainty in accordance with table 5.




| | Defined | Defined in the text | Separately defined | Partly defined | Implied |
|---|---|---|---|---|---|
| IEEE 1012 | 4 | 6 | 10 | 9 | 134 |
| IEC 60880 | 1 | 10 | 0 | 2 | 2 |

Figure 3. IEEE 1012 V&V system objects certainty distribution

It can be seen that IEC 60880 has higher proportion of the overall certainty compared to IEEE 1012. Another factor worthy of attention is the significant difference in number of objects involved.

Comparison between the two dictionaries shows that 10 of 15 IEC 60880 V&V system objects have some relevant IEEE 1012 V&V system objects. These correspondences are not one-to-one relations, as IEEE 1012 has 163 objects and sometimes several objects from IEEE 1012 V&V system can correspond to one of the IEC 60880 V&V system objects.

# 7 IEEE 1012 requirements application to IEC 60880 V&V system model

The process of harmonization in mathematical logic corresponds to the operation “AND”. Hence, strict exact similarities must be found between the IEC 60880 V&V and IEEE 1012 V&V systems if they are to support harmonization.

Following our proposed methodology and analysis of the possible common ground amongst the standards, the application of IEEE 1012 V&V system requirements to the verified IEC 60880 V&V system model using the SysML connection abstraction “satisfy” was performed.

An example of such an allocation is shown in figure 4 where, for instance, “software requirements specification adequacy check” satisfies the requirement 9.2.1.a.1 of the IEEE 1012 V&V system:

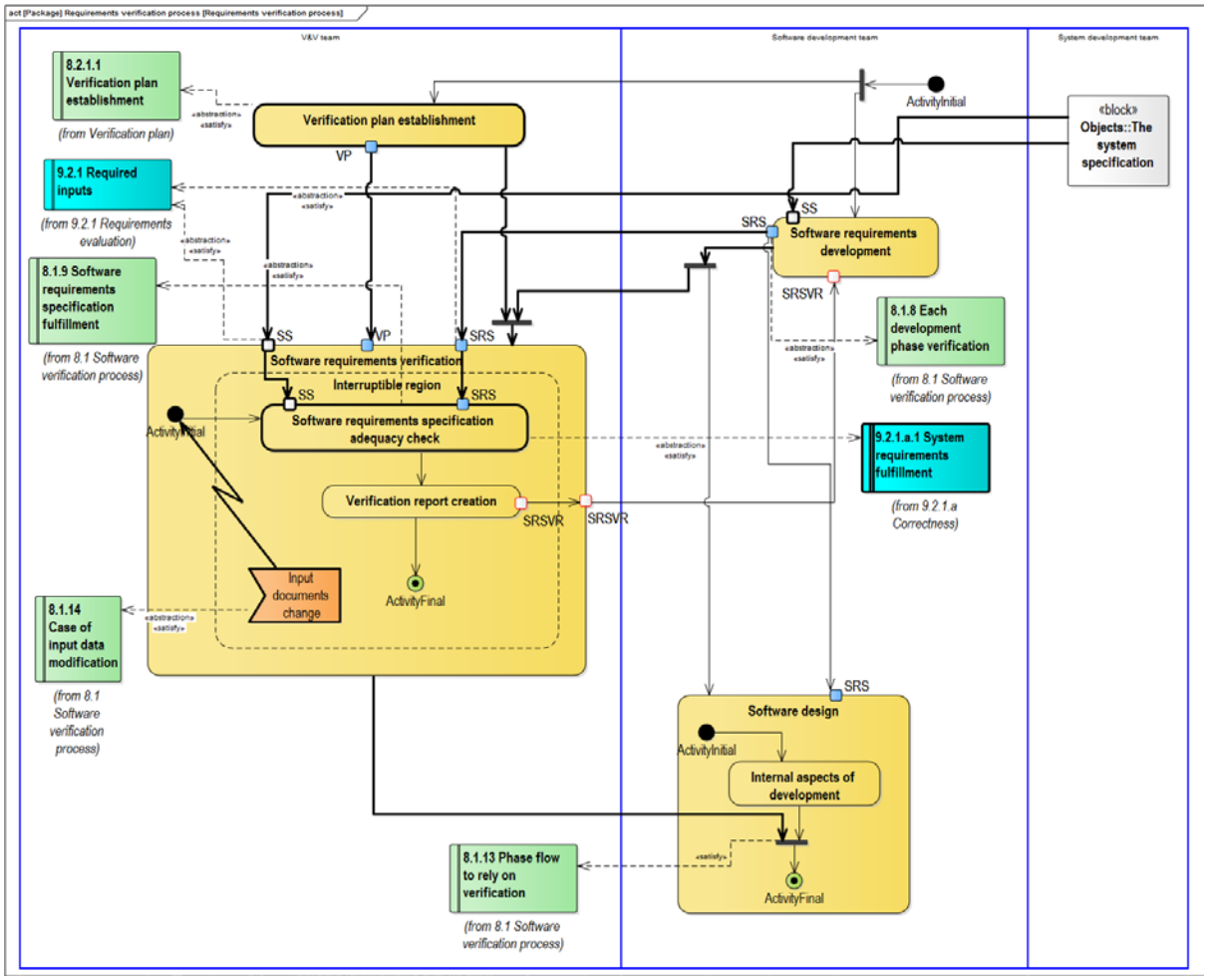



Figure 4. IEEE requirement allocation example

IEEE 1012 requirements are represented as a requirement node with filling; and IEC 60880 requirements are represented as white rectangles. The requirements of the IEEE 1012 standard are not atomic and describe several things in one clause. Hence, to distinguish this level of correspondence, two types of border width were introduced. The bold contour means that IEEE 1012 requirement is fully satisfied by the IEC 60880 V&V element/elements; whereas a regular contour means that IEEE 1012 requirement is only partly satisfied by the IEC 60880 V&V system element/elements.

# 8 Harmonized core modelling

The introduction of three different types of software and different approach regarding system/element consideration led to the fact that no place was found for the implementation verification and for the integrated system verification and validation phases. This is attributed to the use of the logical operand “AND”.

Thus, only some of the phases of requirements and design verification can be harmonized easily, which is due to their transparent correspondence amongst the standards. These phases are the requirements verification and the design verification.

From the objects viewpoint, the core is elaborated from the developed dictionaries. The core objects can be found in the table 8. The logical operand “AND” requires selecting only those that strictly correspond to each other in a one-to-one multiplicity relation.

| **IEC 608880 V&V system object** | **IEEE 1012 V&V system corresponding object** |
|---|---|
| System specification | Concept documentation (system requirements) |
| Software requirements specification | Software requirements specification |
| Software design verification report | Task report |

Table 8. The core objects

Actors view of the core is absent since IEEE 1012 does not use any explicit naming of the actors involved. An example of the harmonized requirements verification process is depicted in figure 5. Note that where the adopted graphical rules that were implemented throughout the paper are no longer relevant; the default notation is used.

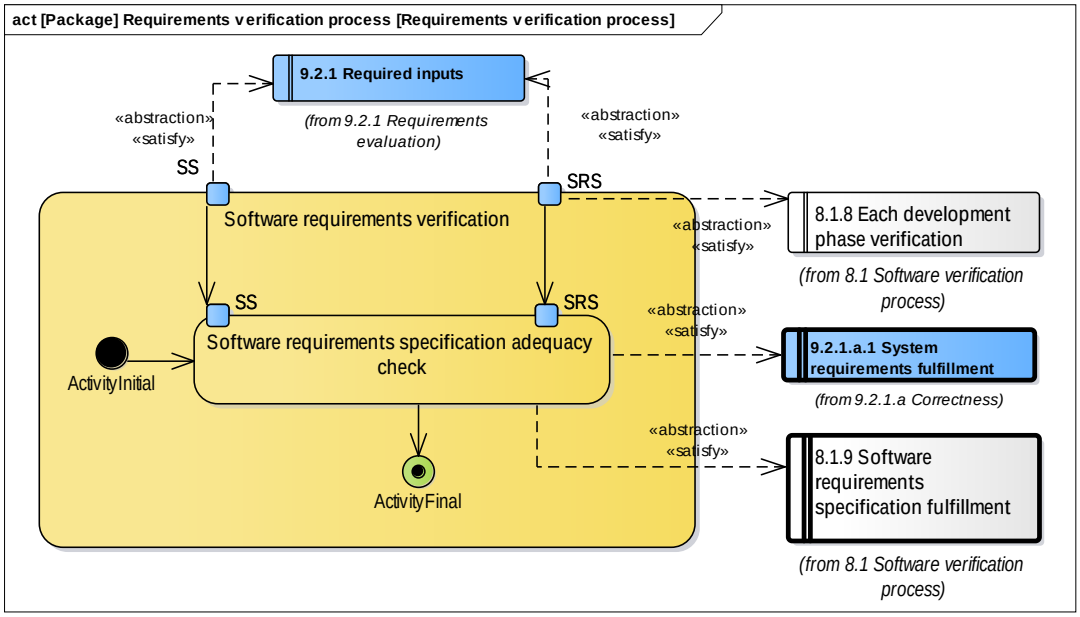



Figure 5. The harmonized software requirements verification process

## 9 Quantitative analysis of the core

Despite the fact that the IEEE 1012 standard was not modelled, it is still possible to calculate the correlation between the core and IEEE 1012 standard based on the outcomes of harmonization process.

Firstly, based on the modelling of requirement tree of the IEEE 1012 standard, it is possible to count a number of unique requirements (each unique requirement that is equivalent to each clause of the IEEE 1012). Secondly, based on the introduction of the requirement satisfaction level, it is possible to define how many of IEEE 1012 unique requirements were fully satisfied by the core. Therefore, by matching these two numbers, the ratio of how the core corresponds to the IEEE 1012 standard has been calculated.

The number of IEEE 1012 requirements taken into consideration within the adopted assumptions is equal to 414; whereas, only eight correspondences can be found in the core. Of these, only four are fully satisfied.

The same indicator was calculated for IEC 60880. Total number of IEC 60880 unique requirements taken into consideration is 64; whereas only five correspondences can be found in the core. Of these, only three are fully satisfied.

Values of the calculated indicators are depicted in figure 6.

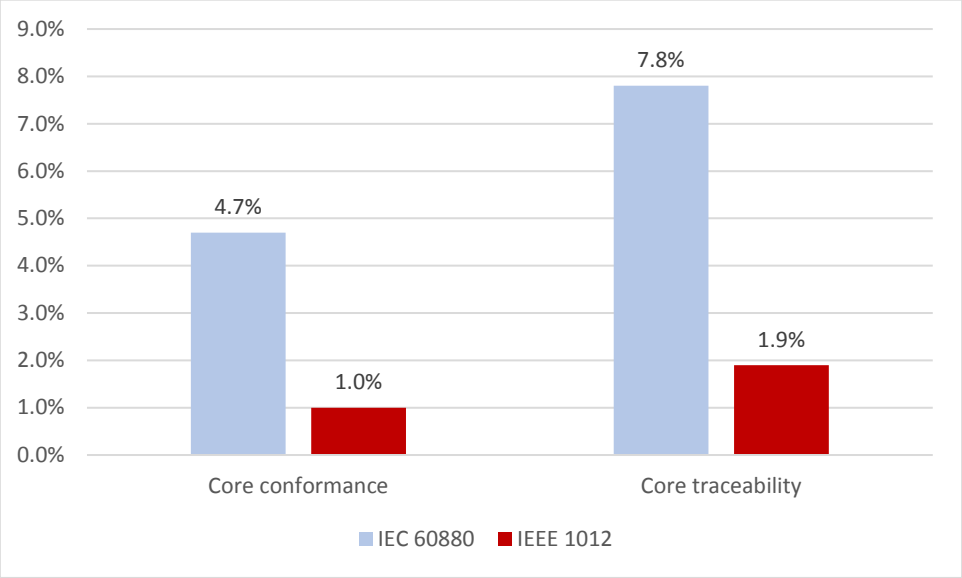



Figure 6. The core conformance and traceability to IEC 60880 and IEEE 1012

Based on the dictionaries developed and the harmonized core, several different quantitative indicators describing the traceability between the standards can be calculated. Viewpoints such as objects traceability, phase traceability, general object-independent traceability, and traceability within the phase can be explored.

# 10 Conclusions

The indicators show that the two standards have very little directly in common in a strict sense. This is attributed to the completely different approaches and the emphasis implemented throughout them.

However, the cross-relation of correlation numbers gives some interesting results: by satisfaction of the particular 1% IEEE 1012 requirements, the 4.7% conformance to IEC 60880 will be achieved. The opposite statement is also correct: by satisfaction of the particular 4.7% IEC 60880 requirements, the 1% conformance to IEEE 1012 will be achieved. Certainly, these numbers are correct only within all of the assumptions that were made during the research, which are:

1. V&V timeframe that was considered contains only phases from the requirements consideration up to the start of operation;
2. Criticality analysis requirements of IEEE 1012 standards were not included in the amount of total considered requirements;
3. Those requirements of IEC 60880 were considered, which were not filtered in accordance with the rules established in the table 3.

The extension of the current results to analysis of broader portions of the standards and due to imposed limitations is an opportunity for future research.

Such results have been achieved by the rigorous implementation of the harmonization operand "AND". If some concessions were made, then the results in terms of the numbers might be slight higher. Examples of such possible concessions include:

1. Equalizing of the objects, which have one-to-many correspondence;
2. Recognition that software type differentiation is negligible.

If such concessions had been adopted, the results would change quantitatively; but not qualitatively since these standards, as it was shown, are completely different. This supports Thomson (2012) claim that there is no one-to-one mapping between major IEEE and IEC standards. Nevertheless, some intersections between them do exist, which supports the opinion of the group of experts from Russia (Anokhin et al., 2009).

The results of this research clearly show the challenge of establishing a harmonized core and the difficulties of formal transferability amongst a standards family. Finally, a viewpoint that suppresses harmonization can be taken. For example, Mark J. Burzynski (2015), who was responsible for the licensing of the Rolls-Royce SPINLINE I&C system with US NRC, has stated that conformance to standards is more about liaison with the regulatory body and the ability to explain what has been done, than strict adherence to the standards. Even so, when multiple standards must be adhered to, a lack of harmonization between them can only lead to conflict and misinterpretation.

Thus, the outcomes of this research (the core and/or method itself) can be used by:

- I&C vendors (to plan licensing activities and to define associated risks);
- Regulators (to conduct reviews of the submitted licensing documentation);
- Customers of I&C vendors (to conduct audit of the suppliers);
- Standards committees (to work on further legislation environment unification).

# 11 Critical analysis and recommendations for future work

A key characteristic of our proposed methodology is the adoption of the logical operand "AND" and by unquestioning compliance to it. This level of compliance led to a limited harmonized core. As noted above, the quantitative results would be different if some concessions had been made. However, qualitatively the results would remain the same.

The model-based methodology implemented in this research shows how a rigorous approach can be used to compare standards and determine a common ground between them. Based on the qualitative conclusions, it might be helpful in future research to shift the aim more towards unification of standards through blending.

Blending process can benefit from the results of the found common ground. For example, dictionaries developed for two V&V systems can facilitate the determination of necessary and sufficient terminology for blended standard. Detailed analysis of each of the two V&V systems might then point to possible directions for a blending of general IT and more specific nuclear requirements.

## Funding statement

The authors received no direct financial support for the research, authorship, and/or publication of this article.

## Conflict of interest

The Authors declare that there is no conflict of interest.

## References

Anokhin A, Bozhenkov O, Rakitin I, et al. (2009) The development of legislative documents for development, implementation and operation of new generation I&C systems with programmable components. Obninsk.

Dickerson C and Mavris D (2009) *Architecture and Principles of Systems Engineering*. Hoboken: CRC Press.

Duthu A and Burzynski M (2015) Lessons Learned in Nuclear I&C Modernizations. Rolls-Royce Civil Nuclear SAS.

Holt J and Perry S (2008) *SysML for Systems Engineering*. London: The Institution of Engineering and Technology.

IAEA NP-T-3.12 (2011) Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants.

IAEA NS-G-1.3 (2002) Instrumentation and Control Systems Important to Safety in Nuclear Power Plants. Safety guide.

IEC 60880:2006 (2006) Instrumentation and control systems important to safety — Software aspects for computer- based systems performing category A functions.

IEEE 1012:2012 (2012) Standard for System and Software Verification and Validation.

IEEE 7-4.3.2:2010 (2010) Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.

Lahtinen J, Johansson M, Ranta J, et al. (2010) Comparison between IEC 60880 and IEC 61508 for certification purposes in the nuclear domain. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 6351 LNCS: 55–67.

Söderholm K (2013) Licensing model development for small modular reactors- focusing on the finnish regulatory framework. PhD thesis, Lappeenranta University of Technology.

Thomson J (2012) Key Threats and Issues for High Integrity C&I in 2011 and Beyond. *Measurement + Control* 45/3.

Wood R, Halcomb D, Johnson G, et al. (2009) Transitioning to Digital I&C Technology: Licensing Processes, Best Practices, and Regulatory Issues.

World Nuclear Association (2014) The Nuclear Renaissance. Available from: http://www.world-nuclear.org/info/Current-and-Future-Generation/The-Nuclear-Renaissance/ (accessed 12 January 2015).

World Nuclear Industry Status Report (2014) Finnish Regulator Approves Olkiluoto-3

Instrumentation & Control System. Available from: http://www.worldnuclearreport.org/Finnish-Regulator-Approves.html (accessed 30 August 2015).

Yastrebenetsky M and Kharchenko V (2014) *Nuclear Power Plant Instrumentation and Control Systems for Safety and Security*. Hershey, PA: IGI Global.