Challenges in licensing safety automation

Björn Wahlström
Systems Analysis Laboratory
Aalto University
Otakaari 1F, FI-02150 Espoo
Finland

Abstract: Safety automation is used in most technical systems where errors and failures can mount threats to human health and/or the environment. Such systems are for instance transportation (air, sea, rail, roads), energy (electricity generation, mines, offshore) and health (hospitals, pharmaceutics, radiation treatment). Safety automation is used as a component in engineered defence-in-depth that brings systems back to safe states if errors or failures in controls or equipment have taken systems into dangerous states. Over the years regulatory oversight has been used to ensure that technical systems will not introduce undue risks to third parties or the society. Safety automation, which today almost exclusively is implemented using digital programmable systems, is one important target for regulatory oversight. With a comparison to safety automation designed and implemented in the 1980ies, which mostly were analogue, it seems that efforts to prove that designs are acceptable has increased to unreasonably levels. The paper goes through some of the problems connected to systems engineering processes required for new nuclear power plants, where current licensing practices have caused cost escalations and delays. In a conclusion it tries to identify causes and remedies for identified problems.

Keywords: Automation, digital systems, nuclear safety, regulatory oversight, systems engineering

1 Introduction

Safety automation is used in most technical systems where errors and failures can mount threats to human health and/or the environment. Such systems are for instance transportation (air, sea, rail, roads), energy (electricity generation, mines, offshore) and health (hospitals, pharmaceutics, radiation treatment). Safety automation, an integrated part of instrumentation and control (I&C), is used as a component in an engineered defence-in-depth (DiD) that brings systems back to safe states if errors or failures in controls or equipment have taken the facility to a dangerous state. Over the years regulatory oversight has been used to ensure that technical systems will not introduce undue risks to third parties or the society. Regulatory oversight is therefore targeted to details of safety automation, which today almost exclusively is implemented using digital programmable systems. With a comparison, safety automation designed and implemented in the 1970ies and 1980ies were mostly analogue. Today it seems that efforts to prove that designs are acceptable has been increased to unreasonable levels. The paper brings up some of the problems that are connected to the systems engineering processes used for new nuclear power plants, where practices for design and construction have caused cost escalations and delays.

In safety science a major conception has been that different industrial areas can learn from each other. To some extent this is certainly true as long one looks at general principles to be applied. The nuclear domain is, however, different from others, which in my mind has introduced additional burdens in providing and accepting proofs of safety. One has even heard from nuclear power opponents that "we shall make nuclear power so expensive to build that will make them to disappear due to their own impossibility". Such ideology-based arguments can only make it more difficult to react on global needs to decrease use of coal-based fuels for energy production, i.e., trading one risk for another, which may not be wise in a longer perspective. My paper draws on my own half a century experience from nuclear power and automation, where the nuclear industry at some point in time moved away from practices that were applied in building the nuclear power fleets in Finland and Sweden (Wahlström, 2020). The current situation seems to me, in

view of the needs to move away from fossil energy sources, as miserable, despite an awakening of interests for small modular reactors (OECD/NEA, 2021).

In the text below I start with a consideration of processes of systems engineering, which outline efforts to move from design and construction to commissioning and operation, where difficulties may hamper realisations of later phases of the engineering process. In the third section I discuss differences between analogue and digital I&C systems, which is the technological change that occurred from the nuclear power plants built in the twentieth century. In the fourth section I bring up regulatory oversight, which by some people is seen as the main culprit for delays and cost escalations. I think however, that regulatory oversight is an important component in ensuring nuclear safety. In the fifth section I go more in detail into processes of I&C design and construction, in a search for possible problems and their remedies. In the sixth section I consider structure and content of the safety case related to safety automation. Systems of requirements and the need for presenting acceptable claims and evidence for safety, has shown to be a stumbling block in the licensing process. In the conclusions I discuss reasons for earlier success, current obstacles to nuclear and present my own vision for the future.

2 Systems engineering

Systems engineering refer to the processes of design and construction that start with specifications and proceeds from conceptual and detailed design to construction and implementation. The process starts with abstract concepts to be refined and concretised in consecutive steps that build on each other. This makes it difficult to see how early design decisions will influence the result. An often-cited picture illustrates how a decreasing design freedom transfers into increasing costs of design changes as the project proceeds in time (Wahlström et al., 1985). A successful process of systems engineering relies on accurate project plans together with an understanding of managing large projects (Flyvbjerg, 2014).

Systems engineering relies on an extensive use of models (Madni, Sievers, 2018). Available design space is sometimes described two-dimensionally in abstraction and details, where design activities move towards larger concreteness and details (Wahlström, 2017). There are models for how to carry out the design process and the design itself relies on different models that are used in phases of the process (Wynn, Clarkson, 2018). Considering changes in the systems engineering processes Sheard (2018) provides interesting information from the maturing of software engineering. Her lexicographic trend analysis provides thoughts on evolving industry segments that most likely apply also to the nuclear domain.

2.1 Specifications

Specifications tell designers what one want to have. A well standardised product on existing markets may have short specifications, but when a product will require considerable number of adaptations, specifications may include hundreds of written pages. For nuclear power plants ordered in the 1970ies the specifications were not too voluminous. The company ordering the plant understood that if would be a FOAKE (first-of-a-kind-engineering) project and the supplier estimated that they had the necessary knowledge and skills to fulfil reasonable expectations. This implied mutual efforts in producing specifications, drawings, descriptions and plans for the project from placing the order to taking the plant into operation. Projects found a large trust between owners and suppliers of the plants. Regulators involved in the projects at that time, wrote the safety requirements often after main design decisions had already been made. As compared with the situation today, there are many more parties involved, a strict set of safety requirements to adapt to and extensive tendering documents to be read and understood before any estimates of time schedules and costs could be given (Ruuska et al., 2011). Lessons learned in the three major nuclear accidents (TMI, Chernobyl, Fukushima) have also led to increased bureaucracy as compared with the early plants.

Looking at current practices and lessons learned by the nuclear industry, at least issues like site selection (nearby cities, seismic zones) are better taken care of now. Selected plant technology may also have made some of the old plants impossible. Competition between plant vendors to build the most profitable plant

led to technical solutions on the verge of acceptability. Adaptations to new requirements that emerged after the three major nuclear accidents also led to expensive safety improvements of which some were not urgent. All that implied increased complexity in projects and their management.

The specification of safety automation was, due to the complexity of the projects, influenced in proportion. An additional problem regarding I&C is that specifications will depend on final solutions for plant buildings and major components (reactor, steam generators, turbine, generator). To some extent the specifications of the I&C and the safety automation can be carried out on a functional level before this information is available, to expedite the finalisation of design and implementation. In addition, trust between parties involved in new builds seems also to have declined, with a need to specify everything contractually in large details. Large projects have in addition an inbuilt feedback mechanism, where problems detected are due to generate increasing costs and delays.

2.2 Design and construction

From a project perspective the move from specifications to design and construction is large, because it means that costs start to collect. The design starts either from a reference plant or from a conceptual design that has been selected. A new plant project is mostly a FOAKE project because it is at a new site, with different contributors and perhaps new regulatory requirements. Costs of the plant and project schedule are defined at the signing of the delivery contract. If it is a fixed cost delivery, the vendor will most likely try to find the cheapest alternatives everywhere in an optimisation of the design. There are various options to optimise the plant in subfields such as buildings, major components and subdeliveries, which all carry uncertainties. In making changes in the design, it is always difficult to assess their final impacts. Because changes are dependent on regulatory approval, possible needs for clarifications can influence time schedules.

When the specifications of I&C and the safety automation are reasonable complete, the I&C vendor can be selected to initiate detailed design and functional testing . Allocations of equipment to specific locations, cable routes to be selected and power supplies can be started. This also enables the control rooms designs to be brought to a larger concretisation and human factors considerations to be initiated. Changes in functional designs may be necessary to reflect information obtained in testing the increasingly concrete I&C design. The benefit of digital technology is that most design changes can be taken care of by software changes.

2.3 Implementation

Moving from design and construction to implementation takes another large step after which changes will imply increasing costs and additional project delays. Now it is time to update project plans including plans for preparing the safety case. This includes review of the safety classification instrument and ensuring that it is consistent with physical locations within the plant and with preliminary documents concerning plant operation. The factory acceptance tests (FAT), and site acceptance tests (SAT) are important steps before equipment start up tests in preparation of initial fuel loading. Towards the end of this phase the plant operational staff should be fully trained and licensed for commissioning activities and the start up.

For the safety automation interfaces to other parts of plant design should be finalised together with functional test using a plant simulator. That means detailed assessment of required scenarios, which may challenge plant safety. If anomalies are detected they will require urgent changes in the design, which in favourable cases may be implemented in software. The main difficulty in this phase is to see beyond immediate problems and finalise the design through careful assessments of I&C functionality. Somewhere in the middle of this phase it may be helpful to use the so called SADT-method to evaluate plans and their applicability (Benard et al., 2008). All this should be documented in the safety case and presented to the regulatory body for approval.

3 Analogue and digital I&C systems

There are several benefits of digital automation as compared with analogue systems (Wahlström et al., 1983). The first digital I&C system, the Honeywell TDC-2000 system, was introduced in 1975. Looking at the 45 years of development, digital I&C systems have matured, but the nuclear industry still is faced with expectations to use analogue systems for certain safety critical control loops. This requirement cannot in my mind be considered motivated from a technical cost-benefit point of view, especially considering a projected plant life of sixty years. The difficulty with digital I&C as compared with analogue systems is the rise in complexity, which is associated with programmable systems. This property however brings the advantages of digital system and should be fully used to build safety features into the I&C. Functionality in digital I&C systems is built using software, which makes it easier to test and change before implementation. In retrospect it is however also clear that the new technology together with the benefits also brought possibilities for new types of design errors.

3.1 Analogue versus digital

People that were not involved in early digital I&C system have sometimes difficulties to understand current problems in licensing digital safety automation. With some simplifications one may say that analogue I&C are restricted by their frequency responses, where digital systems are restricted with respect to execution times (Wahlström, 2015a). One may also say that analogue systems functions are executed in parallel and that digital functions are executed as serial processes. This introduces new failure modes in digital system, i.e., a controller could fail just by software to be non-responding, or it could start to produce erroneous signals. The first problem is usually solved by monitor controllers with watch dog timers, which have the task to switch over from a failing unit to a standby unit. Spurious activation is possible in digital systems, but not in analogue due to their functioning in continuous time and with a continuous state space.

Analogue and digital systems have their own pros and cons, which one may try to try to combine. It will mostly imply restricting the design space considerably for the digital systems, for example to restrict the complexity of the software as much as possible. It also implies the use of specialised hardware for time critical tasks, a deliberate aim for restrictedness and simplicity, a use of early experiments with specifications and early versions of intended software together with a far driven modularisation of both hardware and software (Bosch, 2017). It also implies a use of advanced engineering methods and tools that we have seen emerging (de Weck et al., 2016). The perhaps largest safety impact of the use of digital systems in nuclear power is the possibility to construct a digital twin of the plant to be used in in design, construction, and operation.

3.2 Necessary and sufficient conditions for safety

Assessments of safety automation should in principle build on necessary and sufficient conditions for safety (Wahlström, 2015b). This unfortunately often is expressed as expectations on the licensing process, in terms of consistency, completeness and correctness (C^3), which can be ensured only in restricted cases (cf. Appendix). More generally none of them can be ensured in practice, which restricts the generality of evidence that can be presented.

For the necessary requirements, a set of existential requirements of the following types can be suggested,

- processes of design and construction should have a commitment for high safety,
- design and construction should be carried out with skilled, motivated and committed people,
- systematic work practices and best available technologies should be applied for design methods and tools,
- enough resources should be available for all phases of design, construction, and implementation.

For the sufficient requirements there is a need for an early agreement of requirements to be considered in the safety case. This should also include an agreement between the plant owner and the plant vendor that

changes in system specifications during the design process would imply renegotiation of costs and project duration. More specifically requirements could cover the following issues.

- a graded approach to safety is used, which means that more important safety threats should get larger emphasis in the design and construction (safety classification),
- safety will be taken care of using the principles of defence in depth (DiD) applied in processes of risk analysis, safety engineering and verification and validation (V&V),
- a safety management system, which is compliant with applicable regulatory requirements, should be used in design, construction, and implementation.

3.3 Managing complexity

Complexity is often blamed as the culprit for design errors, delays, and cost overruns. This is in my mind a bad argument, which often is used trying to hide incompetence. If our methods of systems engineering are not able to handle complexity, there is a need for basic research (Koehler, 2014). In my understanding complexity has to do with a simultaneous understanding of systems, their parts, and interactions (Wahlström, 2018). It has to do with a system of systems (SoS) approach, where state variables to be considered may be difficult to manage just due to their large number and/or nonlinear dependencies. De Weck et al., (2016) argue that used levels of abstractions can serve as an indicator of system complexity. They base their argument on the about 7±2 chunks that people can keep in mind at the same time (Miller, 1956) and propose that complexity is proportional to $C=c(m)=(7\pm2)^m$, where m is the number of abstraction levels used in the design. Complexity that has not been considered from the beginning may introduce requirements for late changes during the design process, with increasingly difficulties to keep projects within plans (Fernandes et al., 2015).

The design process should be governed with a safety management system, which is understood, documented, and followed. This may be seen as a part of a delivery system (Li et al., 2017) by which it is ensured that,

- common design errors are avoided e.g., by,
  - defining used variables and setting them initially to specific values,
  - ensuring that interfaces between modules are well specified and understood,
  - testing modules thoroughly in early versions of design and when they are finalised,
  - testing larger entities when two or several modules have been integrated,
- collecting data from the design process in audits to verify that the management system has been used and adhered to,
- documenting design decisions together with their background when they are made,
- collecting and documenting results from intermediate and final tests.

More generally the principle of KISS (keep it simple, stupid), points to the need to avoid unnecessary complications in the design processes and in selected solutions.

4 Regulatory oversight

Regulatory oversight can be seen as a safety principle of its own. Already the need to reconsider safety provisions in a process of arguing with a third party that selected design solutions are good enough, has the potential for improving design. The existence of a system of safety requirements has also the benefit of making plant specifications explicit and concrete. Unfortunately, national systems of requirements have a large diversity. Just the cases of UK and USA are illustrative. In the UK it is enough if licensees can ensure that 36 licensee conditions are fulfilled. The USNRC requirements can instead be seen as a jurisprudential system, which contains thousands of pages. There is certainly a large need for harmonisations between countries (IAEA, 2002), because the burden and costs for a vendor delivering a plant to a new country may be large (OECD/NEA, 2015). Going into details in the differences between nuclear regulators one may also detect differences in views (Raetzke, Micklinghoff, 2006). Efforts by IAEA and WENRA have had positive influences in a path to larger harmonisation, but large efforts remain. In the area of safety automation

there is an important European document, which establishes a common position regarding digital system of international nuclear regulators and their authorised technical support organisations (SSM, 2018)

4.1 Requirements

A new nuclear power plant would need a stable system of requirements to be applied. This has been difficult to achieve especially in the light of historical development in Finland and Sweden (Wahlström, 2020). When the first plants were ordered in Finland and construction projects were started no system of requirements existed, which implied that the system was created in parallel with the construction of the plants. In Sweden, the situation was similar, because the regulatory body SKI was established in 1974 and their first nuclear power plant Oskarshamn 1 was connected to the grid already in 1972. Sweden was applying American requirements, which was not possible in Finland with the first plant delivered from the Soviet Union. The regulatory system in Finland has been kept updated from the beginning to cover needs for the Finnish nuclear industry to be able to start new plant projects. A major update of the Finnish YVL-guides was finished in 2014. Despite this effort many changes have been made to the current guides.

A system of requirements is crucially depending on the level of details. The 2014 version of the Finnish regulatory system contained more than 8000 instances of requirements. Looking at how systems of requirements have developed over the years, the three major nuclear accidents (TMI, Chernobyl, Fukushima) have introduced many of the changes. The Finnish requirements considering safety automation have two issues that are difficult to ensure with digital systems. The first is connected to the quantitative design targets for frequency of core damage less than 10^{-5}/a and frequency of releases of radioactivity more than 100 TBq less than $5*10^{-7}$/a. These requirements would need providing probability estimates of software failures. The second is the need for making the possibility of spurious activations of the safety automation almost impossible[1] to restrict the scope of the probabilistic safety assessments.

The selection of what to automate and the allocation of functions between operators and automation are important issues in licensing (Taylor et al., 2013; Roth et al., 2019). It is also true that automation if wrongly applied may bring in undesirable and unintended effects (Rozzi, Amaldi, 2012). In hindsight it is somewhat astonishing that human and organisational factors came into the requirements relatively late. A classic paper pointing out the ironies of automation (Bainbridge 1983) is still relevant. Nuclear power plants may in the future require both robots and mobile applications in their operation (Ijtsma et al 2019), which puts specific needs to consider human and organisational factors (Schöbel et al., 2021).

4.2 Licensing

The licensing process in Finland relies on the following three steps,

- DiP (Decision in Principle) establishes that it is possible to build a safe plant (the selected site is OK, there are vendors willing to undertake the project, estimates of time schedules and costs are OK),
- CLA (Construction License Application) establishes that the plant has been constructed on paper can be considered safe,
- OLA (Operating License Application) establishes that the plant has been built and tested and is ready to be taken into operation.

My own interpretation of the three-step procedure is that it gives the vendor and the licensee time to build the design organisation and processes by which the safety case is developed. If the plant is identical with an earlier one on the site, the move from an accepted DiP to an accepted CLA can be rather straightforward. Looking at the Finnish requirements for the licensing of the safety automation is from my point of view acceptable for practical purposes, provided that an early agreement on the content of the safety case can be agreed on before a hard commitment regarding costs and time schedules are made. The Finnish regulatory requirements follow to a large extent IAEA requirements and European practices (IAEA, 2016; SSM, 2018).

[1] This formulation is sometimes used to say that the probability of a certain sequence of events is below the accepted rest risk.

4.3 The safety case

The content of the safety case is the most crucial part of the efforts to prove that the safety automation is acceptable. This would imply clear views at least on the following issues,

- the plant has been constructed with a consistent safety philosophy, i.e., the set of identified threats is reasonably complete and sequences of event can be expected to end in safe and stable conditions,
- a reasonable number of scenarios have been simulated using computer codes and sequences are proved to end in acceptable conditions,
- the design has been governed by a management system, that is shown to have been used,
- claims and evidence for safety have been documented from the beginning of the project.

Claims and evidence have in addition been presented that investigated scenarios to a reasonable extent cover the following situations,

- normal operation including start-ups and shutdowns,
- a set of disturbances such as loss of external power supplies, adverse weather conditions, seismic events, minor equipment failures, etc.,
- disturbances and failures in major control loops (reactor, pressuriser, steam generators, turbine, condenser, generator),
- emergency situations that are caused by major pipe breaks and other similar failures,
- beyond design base conditions, such as serious fuel damages including major hydrogen generation.

A final part of the safety case should include claims and evidence that the design has an ability to withstand common cause failures (CCF) in normal, disturbed and emergency situations. This would explicitly be aimed at demonstrating that the plant is resistant to single failures or errors regardless of their cause (technical failures, human errors, external events). This would imply a suitable diversity in critical functions of the safety automation and that possible domino effects have been removed. The grace time[2] requirement should apply in all transients (OECD/NEA 2019).

5 Design of safety automation

Nuclear safety builds on the principle of defence in depth (DiD), where several independent barriers towards unwanted chains of events ensure safety despite unreliability of used components. This principle is functional when independence between components can be assured, because otherwise common cause failures (CCF) may offset several barriers at the same time. Threat of CCF can be combated in the design process using diversity and separation. A specific observation is that automation build designed dependencies into the systems, where conditions in one part of the plant are used to introduce control actions in another parts. A general description of design processes can be found in (Wahlström, 2017) and the application of processes of systems engineering in (Wahlström, 2021).

A typical solution for the design of safety automation is to separate between two different design processes, the platform, and the application. The design of the platform may have taken place several years before it is applied to the design and construction of a specific plant. The relevance of this separation can be seen in considering the complexity of the platform $C_p = c(m_p)$ and the application $C_a = c(m_a)$, which if they are designed independently would be $C_p + C_a$ and would have the complexity $C = c(m_p + m_a)$ if they are designed intermixed. In addition, the possibility of earlier experience with the platform and its specific solutions for increased dependability provides an even larger incentive to use predeveloped platforms for the safety automation.

IAEA guidance for I&C design gives reference to the so-called V-model for moving from requirements through design and integration to installation and operation (IAEA, 2016, p.12). A recent book on software

[2] The time after an initiating event during which the operators are not required to act (sometimes called the 30-minute rule).

design (Goericke, 2020) declares this model as outdated and promotes the use of early experiments with candidate designs to provide paths of good design. The IAEA working group TWG-NPPCI has engaged in a process to create guidance for the design process of digital IC (IAEA, 2021), which to a large extent would rely on the standard ISO/IEC/IEEE 15288. To what extent this effort will solve problems of maintaining I&C systems over the long-life cycles of nuclear installations is difficult to say. Could the use of open source (Ventä, Wahlström, 2007) applications perhaps provide a solution?

5.1 Architecture

System architecture implements system requirements on a high level of abstraction (Raz et al., 2018). In a nuclear project it is the step of design, where a safety philosophy (Hansson, 2018) is implemented[3]. In this phase of design relationships between separate parts of the I&C is implemented to ensure proper independence between functional islands, redundancy in support functions and diversity for important safety functions. It is also the step where functions are allocated between automation and manual controls (Taylor et al., 2013; Roth et al., 2019). More practically it implies that parts of the I&C are allocated to specific physical locations, hardware, power supplies, cooling systems, etc. The architecture therefore takes a stand on,

- plant automation and islands of functions,
- main components and systems (separation regarding locations, used I&C platforms, power supplies, cabling, etc.),
- diversity as needed for ensuring that design errors are not introducing CCFs,
- relationships between plant protection, systems protection, and component protections,
- redundancies as implemented as specific engineered control loops and in the use of platform functions,
- control room design to ensure compliance with the grace rule.

An important part of achieving dependable architectures lies in the reuse of earlier designs. An important component in using that opportunity is trust in earlier designs (Alarcon et al., 2017) and a thorough assessment of possible needs for their modification. For an I&C vendor that has a worldwide set of customers, it may be easy to establish this kind of trust, but for smaller actors in national environments it may be more difficult. Actual projects will however rely on a local cadre of engineers to support the project with capabilities such as fluency in local language, practices, and industrial connections. These engineers can in the project acquire an understanding of used platforms and their inherent capabilities and continue their careers in plant commissioning and operations.

5.2 Platforms

Digital I&C systems were from the beginning implemented as platforms to be used for a large range of applications (Wahlström et al., 1983). The platforms were built on concepts that made it possible for I&C engineers to work with concepts from the analogue I&C they were familiar with. The Damatic system built on this concept and its development was started in August 1978 and its first application was taken into operation in a board mill in September 1979. Used hardware was configured with software to perform required functions using a kind of application-oriented programming. Current platforms use these principles but are more sophisticated and provide various support functions for design and testing.

The suitability of a platform for use in safety automation is crucial in applications design. Application programming is today implemented with high-level language programming languages, where standardised functional blocks are interconnected to form required functions. The allocation of functions to specific units of hardware is also taken care of by software. Available support systems help in the structuring of I&C applications into modules and submodules that can be reused. Support for documentation and naming of equipment and functional modules is also available. When the first design proposals are available, they can already then be tested for required functionality.

[3] Here I use the word philosophy as an abstract understanding of how safety can be built into physical systems.

Available support systems for platforms are used for allocation of power supplies, communication, field equipment, control room indications and manual controls. Error detection and management may suggest use of platform functions combined with specific application algorithms to achieve robust solutions to disturbances and emergencies. If the platform in addition could support the needs for providing reliability estimates for functions such as timing, failure management, possibilities for spurious activation, etc. many lengthy arguments in the licensing process could be avoided.

5.3 Detailed design

V&V functions can evolve along a natural path from specifications, through initial explorative design to final designs. From there it could go through several steps of refinements and integration to end up into plans for a FAT and SAT (factory and site acceptance) processes. A continuous collection of data from simulations and tests helps in building evidence for achieved design quality.

Current platforms place emphasis on human factors in the design. Due to the need to give the operators a solid understanding of plant behaviour, a full scope simulator should be ready at least two years before the planned start-up of the plant. That implies that it also can be used for V&V efforts. Due to the ease of implementing even relatively large changes in the control room design, resulting human machine interfaces may be tested to a large degree of detail before taken into operation. Different kinds of displays may be suggested, putting for example emphasis on situations or processes to be operated. The verification of the grace rule is easy to carry out using a simulator.

Utilising a full spectrum of opportunities with presently available I&C platforms may even make it feasible to build in functions relying on artificial intelligence into design and operations. It may provide possibilities to build monitoring functions that use many variables and estimates of uncertainty to building resilience against disturbances in the plant (Curran et al., 2018). Similar provisions may be available to give control room operators possibilities to assess vulnerabilities and opportunities in operational situations. My feeling is that all functions of which we only dreamt of in my youth, are available today for implementing advanced safety functions.

6 The safety case

A plan to produce the safety case should be prepared early in the project. In the communication between the project and the regulatory body it can be considered as a document of intent to be agreed on between plant owner, plant vendor and regulatory body. It should contain information to place borders on what can be considered as necessary and sufficient requirements for safety. It may also contain descriptions of methods and tools of the systems engineering processes to inform the regulator. The document should adopt a system of systems approach, with descriptions of interfaces between engineering professions and between involved parties. The plan should also describe the management system to be used during the design and construction process, together with statements on how design errors are avoided. An agreement on feasibility of the plan for developing the safety case would also contain a time schedule for delivering documents.

The safety case should build on agreed requirements that should define used norms and standards. One may assume that it will consider chains of claims and evidence as suggested in Figure 1 of the document (Common position, 2018). The evidence supplied can be of two types either structural or empirical. Structural evidence can be collected from how the design process has responded to requirements with chosen design solutions. Empirical evidence could similarly be collected from the V&V processes as tests results obtained from preliminary and completed designs. Audits of design construction and implementation processes can provide proofs of compliance with the safety management system.

6.1 Arguments and evidence

A regulatory review of the safety case can be assumed to follow a systematic assessment of the validity of claims in the format of "the requirement xyz is fulfilled, because of evidence abc" (SSM, 2018, p.34). If a claim is not accepted the response would be "we cannot accept your claim (xyz, abc), because of ($\alpha\beta\chi$), to which the response would be to provide additional evidence. According to Hybertson et al., (2017) evidence presented could be of the following types,

- Relevant—to the issue at hand,
- Authentic—of undisputed origin or basis,
- Dispositive—resolves the issue; or at least discriminative—makes clear the pros and cons,
- Fact-based—not just opinion or habit,
- Uncontaminated,
- Fair—not prejudicial or biased,
- Consistent, replicable, reliable,
- Actionable,
- Recursively grounded.

If this list is difficult to reach for all requirements it may be necessary to accept judgements from independent experts.

Do we need a quantification of the rest risk? To some extent I would agree with setting a design target below which identified risk estimates can be considered acceptable. What such a target should be and what kind of evidence would be required that target has been reached, may still be difficult to agree on. We know that the risk concept itself is connected to controversies especially when there is a need to consider issues connected to human and organisational factors (Aven, Ylönen, 2018). A sound approach is to consider only non-dominated[4] scenarios, which implies that only the most serious transients in groups of scenarios are considered. This would allow for an ordinal comparison of non-dominated scenarios between groups to based on qualitative criteria. In my view current discussions on the need for generating numbers to prove safety must concentrate on efforts to improve their believability.

6.2 I&C requirements

In considering requirements placed explicitly on the I&C and safety automation, I do not expect too large difficulties provided that the platform has been considered suitable. After that most of the argumentation will follow normal QA/QC and V&V activities. Where to introduce redundancy, separation and diversity is a matter of systems engineering. Where there is a need for quantitative reliability assessments it may be necessary to rely on diversity. Signal diversity would be a viable approach for the most serious scenarios, and it would in most cases be sufficient to use the standard platform if algorithms, signalling and outputs to control elements are located into separated units. My feeling is that the need for diverse platforms for the safety automation and the rest of the I&C may be minimised using innovative architectures. If enough arguments can be created for such a solution, it would be wise in a plant life-cycle perspective.

The requirement of quantitative estimates for certain scenarios are difficult to reach with software-based system. Suggestion to estimate to number of remaining faults in a piece of software (Eom et al., 2013) are however doomed to fail, because even a single fault may in special situations lead to disaster. Possibilities for spurious activation (Jigar et al., 2016) can perhaps be shown to be almost impossible for processor-based platforms, by using software markers with which paths of execution can be traced and shown not to stray into unexplored regions. For field programmable gate arrays (FPGA) based systems spurious activation would be restricted to the input and output parts of used algorithms.

A question to agree on is the assumptions to be used for I&C oriented scenarios. Not to stretch the burden of providing evidence for safety, a sound practice might be to design for N+2 failures of the I&C for

[4] A non-dominated scenario in a group of similar scenarios has the highest probability in the group not to lead to an acceptable steady state in a reasonable time.

sensitive controls, which would mean one hidden and one initiating I&C failure. This would put a focus on ensuring that almost all I&C failures are alarmed.

6.3 Common cause failures

Looking at the three major nuclear accidents it is immediate obvious that the plants in retrospect did not fulfil the common safety requirements such as the single failure criterion (Schöbel et al., 2021). There is in my knowledge one case where the industry has reacted with an immediate pre-emptive approach on the discovery of an event sequence presenting such a challenge (Teperi et al., 2019). This illustrates the need for a strong regulator, but also that the nuclear industry tends to protract expensive improvements to a point where costs of an accident may easily become several orders of magnitude larger than the costs of improving plant safety would have been.

The DiD principle is a way by which reliability can be built with unreliable components to give a reliable system. The precondition for this to succeed, is that component failures can be considered stochastically independent. It is therefore of utmost importance that the safety case has taken due consideration of this possibility in chains of events. It is perhaps not necessary to provide quantitative probability estimates, if one due to qualitative reasoning can show that serious sequences have been made almost impossible. This approach may also be considered for sequences involving human errors and organisational deficiencies, if it can be argued that there are alerting alarms and enough time for recovery.

For the safety automation the arguments connected to the absence of CCF should in most cases be possible to handle through redundancy and diversity on a platform level. For more serious scenarios specialised engineered control actions could be used. Special considerations should also be directed to power supplies, physical locations, information networks and appropriate consideration of human and organisational factors.

7 Conclusions

Nuclear power has in retrospect had its ups and downs. The situation in Finland is currently better than in many other countries in Europe. We have new capacity to be taken into operation in a few months' time. The Olkiluoto-3 plant has been seriously delayed and hampered with cost escalations, but it is now only a matter of finalisations before it takes a major part of electricity production in Finland. In addition, we have a second project, the Hanhikivi-1 plant, which is preparing its CLA for regulatory approval. These two plants are expected to operate far into next decades. Depending on experience collected after sixty years of operation they may even be operated into the next century. There is a research programme called SAFIR (Hämäläinen, Suolanen, 2018), which has an important function in ensuring cooperation between academia and the industry. This means that skill and knowledge in the nuclear field can be maintained in Finland at least on a medium term.

The nuclear has in my mind responded poorly to promises made some fifty plus years ago. The perhaps largest blunder of the industry is how it has tried to sell the technology to politicians and the public. The industry has been arrogant in claiming to know what is best for society and have not cared to listen to expressed objections. Not considering Hiroshima and Nagasaki in the introduction of the technology and the consecutive nuclear arms race also the three major accidents at civilian nuclear power plants have caused a widespread fear of the technology. The result is that the industry seems not to be given the position it could take in moves away from fossil energy sources. Below I expand my views on reasons for earlier success, discuss current obstacles and present my vision for moving forward.

7.1 Reasons for earlier success

One reason for the success of early nuclear projects was linked to their uniqueness at the time they were ordered and built. They were implemented by the best engineers the countries could provide. They were seen as national undertakings in which local industries had important parts. Vendor companies had small

groups of young talented designers that were given far reaching authorities to make design decisions. The designers themselves took personal responsibility for their projects and did not spare efforts in bringing things forward. The participating companies and institutions had vested interests in the success of the projects, and they trusted the capabilities of each other.

The transfer from analogue to digital technology for the I&C should have made it possible to design smarter protection functions and thereby make the plants safer. Instead, the new technology made it difficult to get regulatory approvals. The technology required new ways of thinking, new design methods and processes for ensuring design quality. In a growing obsolesce of spare parts for I&C system, steps were taken to introduce digital I&C systems in modernisation projects. Unfortunately, however, some projects came across difficulties, which tended to increase the distrust regulators showed in the new technology.

The perhaps largest difference however between the last century and the current, is the disappearance of many of the large vendors of nuclear power plants. When building new plants stopped after the Chernobyl accident, research and development activities also stopped at the same time when regulatory oversight become stricter. Aftermarkets of plant deliveries were evidently not big enough for vendors to stay in business, which led to disappearing capability in managing large nuclear construction projects. A growing optimism of a nuclear renaissance around the year 2010 was killed by the Fukushima accident.

7.2 Current obstacles to nuclear

The Fukushima accident was a serious blow for the nuclear industry In Europe. Germany decided to phase out its nuclear fleet by the year 2022, Italy decided to stay non-nuclear, Spain and Switzerland banned the construction of new reactors and Sweden shelved plans to replace old nuclear plants with new nuclear. The stress tests that were required for all operating nuclear plants in Europe put a large emphasis on technical safety and not so much on human and organisational factors (Schöbel et al., 2021). Countries with plans to build nuclear were often delayed with their projects due to design changes that were required.

The largest obstacle for new nuclear is the difficulty to give realistic estimates for costs and time schedules. Projects today may even be seen as the last breath of a dying industry. Companies appear to opt for minimum cost solutions and projects are prepared in haste without compassion. When projects are sold at fixed price, incentives mount to search for the cheapest subdeliveries on a large scale. At the same time subdeliveries may stretch through chains of five or even more, which creates a burden of managing contractual interfaces. The need for producing believable safety cases in such networks of contractors, may cause problems that are not detected or may even be deliberately concealed. Regardless of how problems in project management are handled, they will always need negotiations and time before they are resolved.

Experience obtained for example from South Korea indicates that there still are organisations able to build large nuclear power plants, but a global move towards more nuclear cannot rely on single vendors. There are promises to achieve saving in costs and delivery times by improved project management (OECD/NEA, 2015, 2020). Electric grids with a high share of renewable energy would need load following, which can be implemented with large NPPs. The possibility for small modular reactors (SMR) may open and many different types have been proposed (IAEA, 2020; OECD/NEA, 2021). SMRs provide viable alternatives if they can compete with the electricity price of large nuclear power plants. Savings in construction costs can be obtained both for large plants and for SMRs by standardisation and moves of construction tasks from the sites to factories. In addition, it seems that exemptions in current regulatory requirements are necessary at least for SMRs to make concrete projects possible.

7.3 A vision for the future

Today there is a large acceptance of the need to replace fossil-based energy sources. In this endeavour nuclear would have an obvious position, which does not seem to be utilised accordingly. Nuclear power can take a position in the electric grids to stabilise fluctuations in availability and demand of power. A change of the transportation sector would imply reliance on electricity and perhaps hydrogen produced with coal free sources. A large use of bioenergy may not be feasible due to impacts on agriculture and forests. The need

for heat and cooling depends on geographical locations but can for many applications rely on utilisation of low temperature heat. If plenty of fossil free energy sources are available, one may even use coal capture from the atmosphere for production of hydrocarbons or to compensate for old sins of CO_2 release. The nuclear industry would be able to supply adapted solutions for most of these needs.

For the systems engineering of I&C design, there are ongoing development activities IAEA (2021). A draft document was presented on a workshop of the IAEA working group TWG-NPPIC in March this year and it described efforts by major I&C vendors in developing design approaches adapted digital data in all forms. When these approaches are available nuclear plants could get a full lifetime support, which would make it easier to modernise their I&C platforms during plant life. Proposed remedies for current problems of licensing I&C and safety automation include approaches such as:

- careful architecture engineering for both platforms and applications to account for needs of separation and diversification as well as for redundancy and fault management,
- digital twins of the plants to be used to support specifications, design, testing and operator training,
- support systems for requirements engineering, formal specifications and model-based design together with tools for documentation and V&V processes,
- virtual and augmented reality is already in use for plants recently completed, but this technology provides many more opportunities.

I see systems engineering and I&C platforms as important components of providing solutions that would streamline the design of safety automation and the I&C systems at new nuclear power plants. Considering the long-life cycles of NPPs, a careful documentation of requirements and selected design solutions, would make it feasible to automate software generation. The need for providing believable failure probabilities of crucial safety functions seem difficult to obtain without a thorough consideration of platform software. A widespread use of common platforms within nuclear and neighbouring industries would provide benefits of experience sharing. Especially it would be important to remove a commonly perceived need to use nuclear graded equipment for I&C in non-safe classified system. Finally, I foresee a larger international cooperation and more women engineers in nuclear engineering.

Acknowledgement

This contribution was prepared as based on a draft paper on safety automation, which I wrote together with my colleague Dr. Jan-Erik Holmberg. Any faults or mistakes in this paper are however not his, but solely mine.

Appendix

In this appendix I provide short arguments for the impossibility to meet the C^3 requirements (Wahlström, 2015b). I base my reasoning on theoretical results by Alan Turing, Kurt Gödel, and W. Ross Ashby.

I&C can be regarded as an instance of a Turing-machine. According to the theorem of Alan Turing it is impossible to determine if a Turing-machine will stop or not based only on an inspection of its programme. This can for digital I&C be interpreted as it being impossible to conclude if a computer will reach a certain state only by inspecting its software. The only way to do it, is to run the program and see if it was reached or not. Again, this is in most cases practically impossible because the program may contain paths that cannot be executed in a reasonable time.

The theorem of Kurt Gödel states that the set of possible theorems that can be formulated with a finite set of axioms either is incomplete or inconsistent. If it is incomplete there are theorems that cannot be proved with the axioms and if it is inconsistent there exists at least one theorem such as that both the theorem and its negation can be proved. I interpret this in such a way that a system of requirements is either incomplete

or inconsistent. To be practical a system of requirement should not contain conflicting requirements, which implies that it will be incomplete.

The law of requisite variety as formulated by W. Ross Ashby says in principle that a controller of a system should be equally complex as the system it is placed to control. This can be used as an argument that a controller has to contain a model of the system it is placed to control. An ideal I&C system of a plant has therefore to include a model of not only the plant, but also models of the I&C system together with its failure modes. If specialised I&C is added to compensate for failures of the I&C, this will cause an ever-increasing complexity and therefore there will always be failure modes that cannot be composed for.

References

Gene M. Alarcon, Laura G. Militello, Patrick Ryan, Sarah A. Jessup, Christopher S. Calhoun, Joseph B. Lyons (2017). A Descriptive Model of Computer Code Trustworthiness, Journal of Cognitive Engineering and Decision Making, Volume 11, Number 2, June, pp. 107–121.

Terje Aven, Marja Ylönen (2018). A risk interpretation of sociotechnical safety perspectives, Reliability Engineering and System Safety, 175, 13–18.

Lisanne Bainbridge (1983). Ironies of Automation, Automatica, Vol. 19, No. 6. pp. 775-779.

Vincent Benard, Laurent Cauffriez, Dominique Renaux (2008). The Safe-SADT method for aiding designers to choose and improve dependable architectures for complex automated systems, Reliability Engineering and System Safety, 93, 179–196.

Jan Bosch (2017). Six Practices Transforming Systems Engineering, Accessed 210507 at http://janbosch.com/blog/index.php/2017/03/11/six-practices-transforming-systems-engineering/.

Qinxian Chelsea Curran, Douglas Allaire, Karen E.Willcox (2018), Sensitivity analysis methods for mitigating uncertainty in engineering system design, Systems Engineering, 21:191–209.

Common position (2018). Licensing of safety critical software for nuclear reactors: Common position of international nuclear regulators and authorised technical support organisations, Revision 2018.

Olivier L. de Weck, Daniel Roos, Chrstopher L. Magee (2016). Engineering systems; meeting human needs in a complex technological world, The MIT Press.

Heung-seop Eom, Gee-yong Park, Seung-cheol Jang, Han Seong Son, Hyun Gook Kang (2013). V&V-based remaining fault estimation model for safety–critical software of a nuclear power plant, Annals of Nuclear Energy 51, 38–49.

Joao Fernandes, Elsa Henriques, Arlindo Silva, Michael A. Moss (2015). Requirements change in complex technical systems: an empirical study of root causes, Res Eng Design, 26:37–55.

Bent Flyvbjerg (2014). What You Should Know About Megaprojects and Why: An Overview, Project Management Journal, Vol. 45, No. 2, 6–19.

Stephan Goericke (ed.) (2020). The Future of Software Quality Assurance, Springer Open.

Sven Ove Hansson (2018). What Is Philosophy, Really? THEORIA, 84, 221–227, doi:10.1111/theo.12163.

Duane Hybertson, Mimi Hailegiorghis, Kenneth Griesi, Brian Soeder, William Rouse (2018). Evidence-based systems engineering , Systems Engineering.; 21:243–258.

Jari Hämäläinen, Vesa Suolanen (eds. 2018). SAFIR2018 – the Finnish research programme on nuclear power plant safety 2015-2018, Final Report, VTT Technology 349.

IAEA (2002). Harmonization of the licensing process for digital instrumentation and control systems in nuclear power plants, IAEA-TECDOC-1327.

IAEA (2016). Design of Instrumentation and Control Systems for Nuclear Power Plants, Specific Safety Guide No. SSG-39, International Atomic Energy Agency, Vienna.

IAEA (2021). Introduction to systems engineering – nuclear power plant instrumentation and control aspects/perspectives, IAEA Nuclear Energy Series No. NP-T-x.xx, draft V3.9, 19 Feb 2021

Martijn IJtsma, Lanssie M. Ma, Amy R. Pritchett, Karen M. Feigh (2019). Computational Methodology for the Allocation of Work and Interaction in Human-Robot Teams, Journal of Cognitive Engineering and Decision Making, Vol.13, No.4, pp. 221–241.

Abraham Almaw Jigar, Yiliu Liu, Mary Ann Lundteigen (2016). Spurious activation analysis of safety-instrumented systems, Reliability Engineering and System Safety, 156, 15–23.

Gus Koehler (2014). Defining and exploring a complex system's relational spaces, Emergence: Complexity & Organization, 16(1): 100-130.

Yuling Li, Frank W. Guldenmund, Olga N. Aneziris (2017). Delivery systems: A systematic approach for barrier management, Safety Science, http://dx.doi.org/10.1016/j.ssci.2017.02.007.

Azad M. Madni, Michael Sievers (2018). Model-based systems engineering:Motivation, current status, and research opportunities, Systems Engineering, 21:172–190.

Miller, G. A. (1956). The magical number seven, plus or minus two: some limits on our capacity for processing information. Psychological Review, 63(2), 81–97.

OECD/NEA (2015). Nuclear New Build: Insights into Financing and Project Management, NEA No. 7195.

OECD/NEA (2019). Multi-Stage Validation of Nuclear Power Plant Control Room Designs and Modifications, NEA No. 7466.

OECD/NEA (2020). Unlocking Reductions in the Construction Costs of Nuclear: A Practical Guide for Stakeholders, NEA No. 7530.

OECD/NEA (2021). Small modular reactors; challenges and opportunities, No. 7560.

Christian Raetzke, Michael Micklinghoff (2006). Existing nuclear power plants and new safety requirements – an international survey, Carl Heymanns Verlag.

Ali K. Raz, C. Robert Kenley, Daniel A. DeLaurentis (2018). System architecting and design space characterization, Systems Engineering, 21:227–242.

Emilie M. Roth , Christen Sushereba, Laura G. Militello , Julie Diiulio, Katie Ernst (2019). Function Allocation Considerations in the Era of Human Autonomy Teaming, Journal of Cognitive Engineering and Decision Making, , Volume 13, Number 4, December, pp. 199–220.

Ruuska, I., Ahola, T., Artto, K., Locatelli, G., Mancinic, M., 2011. A new governance approach for multi-firm projects: lessons from Olkiluoto 3 and Flamanville 3 nuclear power plant projects. Int. J. Project Management. 29, 647–660.

Simone Rozzi, Paola Amaldi (2012). Organizational and Inter-Organizational Precursors to Problematic Automation in Safety Critical Domains, https://www.researchgate.net/publication/262316210.

Marcus Schöbel, Inmaculada Silla, Anna-Maria Teperi, Robin Gustafsson, Antti Piirto, Carl Rollenhagen, Björn Wahlström (2021). From insights to implementation: A fifty-year perspective on Human and Organizational factors in Nuclear Safety, draft submitted for publication.

Sarah A. Sheard (2018). Evolution of systems engineering scholarship from 2000 to 2015, with particular emphasis , on software, Systems Engineering.;21:152–171.

SSM (2018). Licensing of safety critical software for nuclear reactors: Common position of international nuclear regulators and authorised technical support organisations – Revision 2018, SSM 2018:19.

Grant S. Taylor, Lauren E. Reinerman-Jones, James L. Szalma, Mustapha Mouloua, Peter A. Hancock (2013). What to Automate: Addressing the Multidimensionality of Cognitive Resources Through System Design, Journal of Cognitive Engineering and Decision Making, Vol. 7, No. 4, December, pp. 311–329.

Anna-Maria Teperi, Björn Wahlström, Robin Gustafsson (2019). Human and Organisational Factors in Perspective, Nuclear Science and Technology Symposium - SYP2019, Helsinki, Finland, 30-31 October.

USNRC (2019). Human-System Interface Design Review Guidelines, Draft Rev. 3, NUREG-0700.

Olli Ventä, Wahlström Björn (2007). Investigating the case of Open Source applications within nuclear power, EHPG meeting of the OECD Halden Reactor Project, Storefjell, Norway, 12-15 March.

Wahlström Björn, Juusela Arto, Ollus Martin, Närväinen Pekka, Lehmus Ismo, Lönnqvist Pertti (1983). A distributed control system and its application to a board mill, Automatica, vol.19, No.1.

Wahlström Björn, Heinonen Rauno, Ranta Jukka, Haarla Jyrki (1985). The design process and the use of computerized tools in control room design, Nordic liaison committee for atomic energy, Stockholm, Sweden, NKA/LIT(85)4. 110p.

Wahlström Björn (2015a). Differences between analog and digital I&C, NPIC & HMIT 2015, Charlotte, NC, February 22-26, 2015

Wahlström Björn (2015b). Safety principles and I&C design, NPIC & HMIT 2015, Charlotte, NC, February 22-26, 2015.

Wahlström Björn, Alex Duchak (2015). The IAEA safety principles applied to NPP instrumentation and control, NPIC & HMIT 2015, Charlotte, NC, February 22-26, 2015.

Wahlström Björn (2017). Safety automation, in Niklas Möller, Sven Ove Hansson,Jan-Erik Holmberg, Carl Rollenhagen, eds. (2017). Handbook of Safety Principles, John Wiley & Sons, Inc.

Wahlström B. (2018). Systemic thinking in support of safety management in nuclear power plants, Safety Science, 109 , 201–218.

Wahlström B. (2020). Human factors in nuclear power; reflections on 50 years of development in Finland , in A.-M. Teperi, N. Gotcheva (eds.), "Human Factors in the Nuclear Industry; A Systemic Approach to Safety", Elsevier, Woodhead Publishing Series in Energy.

Wahlström B. (2021). Systems engineering for nuclear I&C, IAEA Technical Meeting on Adoption of Systems Engineering Principles for Nuclear Power Plant Instrumentation and Control, 23-26 March.

David C. Wynn, P. John Clarkson (2018). Process models in design and development, Res Eng Design, 29:161–202.