Systems engineering for nuclear I&C[1]

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

Abstract: Systems engineering is an important process by which safety is constructed into nuclear power plants (NPPs). Its application especially in the instrumentation and control (I&C) has become increasingly significant since the advent of digital automation systems. Technical development has brought forward high quality I&C platforms with which reliability and safety of the NPPs should be easy to assure. Unfortunately, however, the licensing process of safety automation has proved to contain obstacles that cause both delays and cost escalations of projects in the nuclear domain. This paper arguments that careful systems engineering of both safety and non-safety I&C together with a parallel process by which a safety case is developed, can change the situation. Provided that processes are planned in advance and plans are followed, it should be possible to respond to applicable requirements and to collect evidence that completed I&C design fulfils them. The paper considers practical problems we have seen and possibilities to respond to them in the I&C engineering process with a focus on concepts, models and tools proposed in academic literature.

1 Introduction

Nuclear power could support a transfer of electricity production to non-fossil energy sources, but concrete projects, both modernisations and new builds, have been problem ridden with overruns in costs and time schedules. Compared with building new nuclear at the end of the 1980ies and beginning of the 1990ies something has happened. Difficulties have been claimed to be connected to a tighter regulatory climate and to the introduction of digital I&C for the plants. At least for the part of accusing digital I&C it seems unfair to an old-timer in control engineering that in his youth was involved in several projects connected to digital computers and nuclear power.

Taking a closer look on difficulties with recent projects, one thing is clear. Three nuclear accidents have tilled the grounds for nuclear opposition, which through several feedback loops have led to vicious circles of increased complexity in regulatory systems, decreasing interest by major actors and decreasing attractiveness of the nuclear domain as careers for young people. The immediate consequence has been increased uncertainties in estimates of costs and project durations that have influenced investor interests in the nuclear domain. In this larger picture digital I&C has played only a minor part, but also here circles of nuclear opposition have made it possible to propagate increasing doubts regarding the safety of nuclear power.

Proposals to overcome the present situation have been given (OECD/NEA, 2020), which assess possibilities for reducing costs for new builds. According to the report a 55% reduction of cost could be achievable for total plant costs, which applies also to electrical, I&C and software as well as to construction and commissioning of these systems. The adaptation to new national regulatory systems is estimated to lead to a 30% increase in plant costs, which points to the need for an increased harmonisation between national requirements. In addition, the report (OECD/NEA, 2020) suggests, that the use of a mature design and construction processes, which are supported by computers to the largest extent, may further decrease labour costs and increase design

[1] Paper presented at the IAEA Technical Meeting on Adoption of Systems Engineering Principles for Nuclear Power Plant Instrumentation and Control, 23-26 March 2021.

quality. This puts the focus on needs for taking a closer look on processes of systems engineering that are used in in the design and construction of nuclear power plants and their I&C systems (de Weck et al. 2016).

In this article I report on searches within academic literature for concepts, models and tools that may help, the nuclear in general and the I&C more specifically, in concrete projects on one hand to create accurate estimates of costs and time schedules and on the other hand possibilities to streamline their design processes. I think there are many subfields of the design of nuclear I&C that could benefit from specific research and development (R&D) projects of which some issues are considered below. The need for this type of work is based on assessments of how the nuclear industry has been able to utilise results from a research project[2] executed in the years 2001 to 2004 (Wahlström et al. 2005). Considering the situation of the nuclear industry today, it is however easy to understand that people, in a situation with increasing pressures from regulators and the society, do not have time to search for and read relevant academic articles in the multiple domains of nuclear engineering, management practices and safety science.

In the sequel I start with a consideration of design in general and how of general principles of systems engineering can be applied. From there I move to consider I&C design and implementation to assess typical applications in the nuclear domain. In the fourth section I discuss the move from analogue to digital solutions that occurred before the millennium shift and how it influenced both thinking and needs for developing processes for I&C design and implementation. In the fifth section, I take a broad brush to paint possibilities for specific support systems that provide possibilities for improved safety for nuclear power plants during their whole lifecycle. In the sixth section, I try to identify challenges and needs for development to enable nuclear power to have a role in decreasing CO_2 emissions connected to electricity production. In the final section, I conclude with some general remarks, which the IAEA Technical Working Group on Nuclear Power Plant Instrumentation and Control (TWG-NPPIC) may use for guiding future activities.

2 Systems engineering

A recent conception of design is that it should be based on systems engineering in the broadest sense (de Weck et al. 2016). System engineering has to do with the application of models both of and in design processes and product development (Wahlström, 1994; Madni, Sievers, 2018). The use of models makes it possible to use a counterfeit reality to test alternative paths in the design process and/or solutions for finalised products. Well designed product development processes can reduce costs and development time (Unger, Eppinger, 2011). Eckert, et al. (2017) argue for an integration of models to be used to support design and product development in making decisions on paths to take. Early tests of proposed designs can support design quality and help in collecting evidence that selected solutions fulfil required specifications. Exactly what one means with quality of a design process or of products may however vary (Stylidis et al. 2020). One may define a larger set of so called -ilities (de Weck et al. 2016) for guiding the design process.

Design is traditionally seen as a question of form and function (F&F), but for plants and I&C design it is mostly questions of functionality, although many designers see simple and efficient designs as beautiful. Specific domains rely on their own methods and requirements, but it is still instructive to search for characteristics of design on a general level. Paths of inquiry can be found in journals such as Design Issues, Design Studies, and Research in Engineering Design, which often talk about design thinking as distinct skill. Especially when the task is connected to the design of a first-of-a-kind-engineering (FOAKE) system, it is recommendable to consider the design project as unique and its design organisation to be an object of its own design (Buchanan, 2008).

[2] LearnSafe, Learning organisations for nuclear safety, NUC (Euratom), FIKS-CT-2001-00162, https://www.bewas.fi//learnsafe.html.

2.1 Design as an art

Taking a broad view on design, it is certainly an art, which relies on finding successful combinations of form and function (F&F). It starts from a vision of something new and leads the ideation of a process by which one proceeds from abstract visions to something concrete to be built (Rasmussen, 1985). One may also see design as something that correlate with a trajectory of artificiality (Krippendorff, 2011). Especially in engineering design it can be seen as being between product design and technology development (Horváth, 2004). In his paper Horváth gives a more detailed views on components of design science and the management of design processes. In engineering design, one may ask the extent how much design principles can be brought from one area of design to another. Kannengiesser and Gero (2015) address this question and develop models of the design process that gives possibilities to compare practices in different domains. My view is that such models help in considering the design process in a top-down fashion, which can be useful when looking at needs for I&C design to be modified. Design in general may be viewed as starting with some candidate design (imagined, known, described), which is analysed regarding requirements placed on the system to evaluate its acceptability. From there various improvements may be suggested for a new candidate to be synthetised and the loop is started anew (Wahlström, 2018).

Important when looking at general aspects of design, is also to evaluate what can be considered as necessary knowledge and skills designers should have. According to Heisig et al. (2014), "Capturing information and knowledge in engineering work is not a new endeavour. Historically, designers were encouraged to use and retain their personal logbooks during their apprenticeships. Experienced designers thus possessed a wide range of successful design solutions." Cross and Cross (1998) try in their article to shed light on what separates design experts from novices. This may be dependent on the domain of design, but their study can at least propose this question to be researched in more detail. Kunrath et al. (2020AB) follow up on similar questions by exploring views on the professional identity of designers. A strong identity can help designers to withstand pressures from project managers who enforce shortcuts, which may challenge design quality. The two papers can also support selection and training of designers to concrete projects. My own view (Wahlström, 2018) is that systems thinking is an absolute necessity in all design activities. A crucial question is if systems thinking for design can be considered as an innate talent or could be learned in suitable training programmes.

The domain of I&C design has to do with the creation of an interface between an industrial process and its operators, which include, but are not restricted to, control room operators and maintenance people. More generally one should require an adaptation of available indications and controls to all tasks that are important for safe and efficient operation of the plant in consideration. Present I&C technologies are not cost restricted in the same way as they were when nuclear plants were built some forty years ago. One may envision improved interfaces between design and cognitive science (Flach et al. 2017), who in their paper use three concepts, i.e., specifying – affording – satisfying, to stress that process supervision is intended to be used by people. Ciavola and Gershenson (2016) see affordance theory to be of large interest in design science. This implies that the nuclear domain should take human and organisational factors (HOF) broadly into account within plant and I&C design (Teperi, Gotcheva, 2020).

The reuse of old designs (Fortune, Valerdi, 2013), whenever that is possible is an essential principle in all design activities, but care should still be exercised to ensure that the functionality of selected design is understood and applicable. Possible application may be found in handbooks or among earlier projects of plant and I&C vendors. So called *design patterns* or *use cases* are created and available for commonly seen control applications. Transfer between domains may be possible in some cases (Busby, 1998). A common understanding is that safety must be introduced into the design from the very beginning (Fadier, De la Garza, 2006). A simple assurance that this will be done, is to plan the creation of the safety case[3] to run in parallel with the design process. An enlarged consideration of a design process is to see it as a representation of a system of systems (SoS), where actors in socio-technical systems cooperate within their own organisations to create a new nuclear power plant to serve the society in its need for electricity.

[3] I use the concept of a safety case in the British understanding. It may also be called the final safety analysis report (FSAR).

2.2 Expectations on designs

A common expectation is that designers are professionals and that they in their work can select the best solutions to problems that are encountered. That may have been true at another time, in another domain or in a country that I have not visited. People do make errors and when they do in a project with tight cost frames and with tight time schedules, the result can be disastrous (Love et al. 2012). Experience from process industries demonstrate that more than half of the disturbances in the operational phase are due to deficiencies or errors in the design (Kinnersley, Roelen, 2007; Taylor, 2007A). Setting up a design project will need precautions, to increase the probability of success. As a list of recommendable precautions, one may start with:

- plan for contingencies,
- use a management system for the design process,
- avoid design projects, which are bought at a fixed price,
- avoid late changes in product specifications,
- ensure continuing processes of verification and validation (V&V) as well as documentation during the whole design project,
- ensure close coordination and communication with neighbouring design projects (plant, buildings, major components, I&C).

In starting a new design project there is a large span of stakeholders that expect good results. If the I&C vendor has experience from earlier design projects of the same type, there is usually a pool of experience that can be used for the planning of the project (Locatelli et al. 2014). An important question for projects in the nuclear domain, is if the intended vendor has earlier experience with the regulatory approach to be applied. If not, it is extremely important that a familiarisation process is initiated early to ensure that the three parties, the plant owner, the plant and I&C vendor and the national regulator, have a shared understanding of requirements to be applied and documents expected to be produced in the licensing process.

An important issue in placing expectations on the result of a design process, is to accept that some important quality may not have got proper attention when the design process was initiated. A typical example is the substance DDT that was designed and adopted as a multipurpose pesticide. The gradual accumulation of this compound in all living matters, which was detected later, forced the authorities to ban its use. De Weck et al. (2016) speak of systems that are partially designed and partially evolving. When a system is designed and put on the market, it may be detected that it will demand new systems in its environment to function properly or to take care of waste it is producing.

A common problem in all types of design seems to be that designers seldom get feedback on their designs. Partly this may be because quality of design (Stylidis et al. 2020) is an evading concept. Similarly, what is to be defined as a design error or deficiency is also problematic. The management system used in the design project is however the place where remedies should be issued. Integrating knowledge on errors made and how they could be prevented (Hamill, Goseva-Popstojanova 2015) into the design management systems, should make it possible to increase design quality. By requiring design support systems to be used, regular audits to be carried out and well-defined milestones for following progress, necessary conditions for a successful project should be at hand. Basically, the design management system should specify interactions between design domains, groups, and individuals, to ensure that they through processes, tasks and V&V activities participate in reaching successful solutions.

2.3 Architecting

Architecting can in the design process be a first step in which a general outline of selected solutions is defined. The resulting architecture is also the first step from a vision towards a concrete structure and parts of the system to be designed. Architecting can also be the beginning of a conceptual phase of design, where things are defined in functional terms in response to high level requirements. Eisenbart et al. (2017) consider in their article different functional models that are applied in the industry. They stress the importance that different aspects of the selected conceptual design are understood by all participants and correctly linked to appropriate

engineering disciplines. The conceptual design phase has a large influence on the success of later design activities, because it defines big lines of the solution (Hay et al. 2017). Raz et al. (2018) suggest a process for systems architecting that involves a definition of a design space, which in turn comprises of identifying major variables and their feasible regions. For I&C the design space would be specified by the analogue and binary signals to be handled and used in field equipment, by major components and in control rooms.

Already in the process of architecting applicable safety requirements will enter the design process. The selected architecture should reflect general safety principles such as defence in depth (DiD), separation, diversity, redundancy, fault detection and correction as well as the grace[4] time given to operators in the case of disturbances. Practically the safety principles should be implemented at all levels in the design to remove, control, isolate and mitigate possible threats, which may be initiators of unwanted sequences of events. By introducing resilience in the design to make it possible for systems, subsystems, and components to achieve a graceful recovery (Woods, 2018) from disturbances in the plant and its I&C system.

Functional models of the architecture give a frame for further breaking down functions into modules that can serve as design tasks for individuals or groups of designers (Heydari et al. 2016). Paparistodimou et al. (2020) describes a methodology to assess robustness and modularity of system architectures, which they apply to ships industry. It should not be too difficult to transfer their ideas to the nuclear domain. An initial structure of modules may before finalising be optimised by removing unnecessary interdependencies (Sangal et al. 2005; Zhang et al. 2006). Ferrante et al. (1987) propose for that purpose the creation of program dependence graphs, which make both data and control dependencies visible. A successful architecture relies on finding suitable structures and modules that stress reliability and independence of functional entities. If potential I&C vendors have platforms that offer believable assurance that failure detection and management is reliable and that undesired excursions of the software have been made practically impossible, it should not be difficult to find suitable architectures.

2.4 V&V processes

Verification and validation (V&V) are key concepts related to design and construction in the nuclear domain. Loosely defined one may say that verification ensures that system specifications are fulfilled and validation that designed systems are appropriate for their tasks. Due to the complexity of computer-based systems requirements are placed both on the design process and on the product that is the result of the design. Absence of design errors cannot be proven, which implies that a belief in product quality must be built partly on a belief in the quality of the design process itself and partly on inspection and testing efforts during design. Avoiding errors in the final design can in principle be made in the design using various support system and, in the V,&V phase using efficient methods for error detection and correction.

V&V processes build on references to a system of requirements that forms a basis for the design process. Arguments that the designed system fulfils applicable requirements build in principle on assertions that refer to clauses in the system of requirements together with evidence for their truthfulness (Hybertson et al. 2017; Common position, 2018). An efficient collection of evidence for a safety case relies on realistic plans for V&V activities and on data collection throughout the design process. Supporting evidence may be structural or empirical based on:

- facts concerning the design process that have been verified in audits,
- design goals as verified in system specifications and their supporting tests,
- tests of single modules initially and along their stepwise creation and integration,
- tests with scenarios of situations in which the I&C system should respond properly,
- results obtained in factory and site acceptance tests (FAT, SAT).

Disturbances and emergencies for which the plant should be able to reach safe and stable conditions, can be checked with simulations from selected initial conditions. The extent this method is necessary also for I&C

[4] The time available for operators to analyse a new event before they are forced to intervene.

related scenarios depends on internal safety provisions of selected I&C platforms. If trust in the protective functions of used I&C platforms can be established, the set of test scenarios can be made comparatively small. A consideration of requirements on human factors is another important part of the V&V efforts that must be carried out using experiments with simulators (IAEA, 2019).

3 Applications for nuclear I&C

The digitalisation of earlier analogue I&C systems that took place during the 1970ies changed I&C design from being hardware based to be mostly software based. At the same time this development made it possible decrease the cost of single control loops by implementing them in software. However, it also made it also possible to build almost arbitrarily complex software, which puts a large burden of proof that the software implements all intended but no unintended functions (Wahlström, 2015). This has caused confusion in the licensing of digital safety system and correspondingly problems with time schedules and costs for nuclear I&C projects. An overview of safety automation as applied in nuclear power plants can be found in (Wahlström, 2018).

Among other safety critical domains, the same difficulty can be seen in the flight industry, but nuclear regulators seem to have adopted more stringent approaches. The basic problem is that it is often assumed that the created software should be complete, consistent, and correct (C^3), which is not possible to prove, in other than restricted cases. If this fact is not recognised and accepted it can lead to endless discussion, especially if there is a requirement that the I&C should be proved not to initiate spurious activities.

3.1 A life cycle approach

Design and construction in the nuclear domain are regulated on an international level using safety standards that have been developed by the International Atomic Energy Agency (IAEA). The standards take a clear lifecycle approach to cover design, construction, commissioning, operation, and decommissioning. This approach is clearly seen also in the documents that address I&C design and implementation (IAEA, 2016). This document contains a total of more than eight hundred clauses that the I&C system should comply with. Already a sweeping consideration of the document makes it clear that the design process must be governed by a management system, which can ensure compliance. Requirements placed on the management of the design project forms a considerable (20%) part of the document.

The need for a life cycle approach for the plant itself makes it necessary to apply approaches that were not taken into account when our present plants were built and taken into operation. At that time, one could even hear that it was possible to buy at nuclear plant with or without documentation. A plant without documentation cannot be modernised when it becomes difficult to get spare parts. Today it is common to assume a sixty-year lifetime for a new plant, which may imply that its I&C must be modernised two times. A modernisation of the I&C system would be expensive without a comprehensive documentation, but far easier to do if requirements, specifications, functional descriptions, configuration information and test records are available.

The development of computer technology made it possible to rethink the I&C life cycle from the beginning to ensure that various support systems are available from the beginning and are updated whenever plant changes are made. Ensuring that this data, including records of tests that have been performed, is available in digital form is an asset whenever plant changes are contemplated. This applies also to the training simulator that is used for the initial and continuing training of control room operators. For the plant design a large help can be obtained with accurate 3-D model of buildings, room, and components (Camburn et al. 2017).

3.2 Safety principles

Nuclear safety is based on a broad application of the defence-in-depth (DiD) principle (Möller et al. 2018). The principle is implemented by building sequential barriers against unwanted events. which means that a high

safety can be reached provided that the barriers are independent. To ensure independence the safety principles of separation and diversity can be used. A commonly used safety principle is the single failure criterion by which one tries to ensure that no single failures can pose a threat towards safety. The single failure criterion is typically built on redundancy, where a switch over to a standby unit is initiated if the primary unit is failing. The principle of a graded approach to safety is used to stress that attention to structures, systems and components should be given according to their importance for safety. The DiD concept is sensitive to common cause failures (CCF) that may bring two or more barriers to fail simultaneously. The protection against CCFs is therefore a major concern in efforts of safety engineering.

The separation principle is for example used in engineered safety systems with a 2/4 redundancy, in such a way that the four trains are clearly separated. For the I&C system diversity could be used to protect against CCFs by introducing two or more functions, which use different input signals and different control elements. Another way of introducing diversity is to use two or more different I&C platforms for certain parts of the protective functions. For an increased reliability of implemented I&C functions it is possible to use standby units with an automatic change over in the case of unit failures. One typical use of redundancy is to have at least duplicate buses for data transfer between field units, data concentrators and control rooms. In designing the I&C architecture, it is also beneficial not to put too many functions in the same units and to design the power supplies for the I&C carefully.

Verifying the grace rule can in principle be done during operator training, but it may be more efficient to create scripts that will simulate operator actions. If the grace time is set to 30 minutes, then the script would be delayed with that amount and the acceptance criterion is that simulated transients end in safe and stable states.

3.3 Automation design

Automation design has changed considerably in the move from analogue to digital systems (Wahlström et al. 1983). The most important difference has to do with the transfer of design from hardware to software. The common approach was to separate between the design of an I&C platform and the design of the I&C application. That enabled I&C vendors to build advanced functions into their platforms that were not possible to implement with analogue systems (Wahlström et al. 1983; André et al. 2017). The approach to use a general-purpose platform makes it also possible to serve a range of applications over their life cycles (Han et al. 2020). At the same time software implementation of the platform provides the benefit of a modular architecture, which has benefits for both design and testing as well as for later changes and modifications of the platform (Paparistodimou et al. 2020). The use of platforms for I&C design implies that the I&C design splits into two separate design processes, the platform design and the design of the I&C application that may be several years apart.

Already when the first nuclear power plants were built, an obvious solution was to introduce automation for functions that required rapid initiation and reliability. Reactor power is the most pertinent example of these controls, but other controls were mostly manual. The division between automatic and manual controls was based on the selected control philosophy for the plants, which in turn relied on the so called Fitts list (de Winter, Dodou, 2014). The selected solutions could however often be criticized (Bainbridge, 1983), when automated tasks often were simple and correspondingly manual tasks were difficult. A special issue of the Journal of Cognitive Engineering and Decision Making provides a comprehensive discussion of what to automate and where manual controls are acceptable (Roth, Pritchett, 2018; Kaber, 2018 A&B). For the nuclear domain, the grace rule requirement and corresponding human factors considerations resolves this question in the design of the I&C architecture.

3.4 The safety case

The safety case is the document in which arguments are presented to the regulator that the designed plant is safe to take into operation. The safety case consists of several parts of which some are of structural nature and other are based on empirical evidence from actual tests. It is important that plans for the content of the safety

case and the time schedule for delivering preliminary parts to the national regulator has been agreed on early in the project.

In Finland, the national requirements system assumes that the safety case is produced and delivered in three major phases, which in turn can be further subdivided into separate deliveries when the design and construction project proceeds. These major steps are the following

- An application for a decision in principle (DiP). This document aims at illustrating that a new nuclear power plant is in the national interest of Finland and that there are vendors willing to design and build a plant that can be considered safe.
- An application for a construction license (CLA), this document is created in a cooperation between the plant owner and the selected vendor, which demonstrates that the plant as designed on paper is safe and fulfils Finnish regulatory requirements.
- An application for an operational license (OLA), which demonstrates that the plant is ready to be taken into operation according to start-up plans, it is safe and fulfils projected and agreed conditions.

My view is that there are many benefits of splitting up the production of the safety case in this way. In the DiP phase it is rather crude, but still based on information that has been obtained from potential plant vendors. It also means that the plant owner can challenge vendors on details of the safety philosophy they propose. In this phase it is enough that proposed I&C is described in functional terms. Already in the preparation of the CLA a far larger degree of detail is required. It may not be necessary to make the final decision on the I&C platforms to use, but now should already details of the I&C architecture be available. Between the CLA and the OLA the I&C architecture is refined into modules, which provides a basis for defining and testing their interfaces. In moving towards the OLA, modules are integrated into larger entities, which provides possibilities for additional tests. Finally, the OLA will contain information from the FAT and SAT, which also confirm that cabling and connections have been properly carried out.

In the Finnish regulatory requirements, the design target for core damage probability (CDP) less than 10^{-5} and for large releases of radioactivity (LRR) less than 10^{-7} per year, have implications for the I&C design. With these requirements, there is an obvious need to include also the I&C systems into the probabilistic safety assessments (PSA) of the plant. The required numbers are small, which makes it challenging to present believable calculations for compliance, but the use of diverse high reliability I&C platforms can provide a solution. The inclusion of software-based systems in the PSAs is a remaining controversy despite approaches that have been proposed (Pasquini et al. 2011; DiMaio et al. 2016). The possibilities for spurious activation (Jigar et al. 2016) of functions in the I&C systems is a related issue. One paper (Eom et al. 2013) proposes to use an estimate of the number of remaining faults in the software for calculations. This approach is not useful, because even if there is only one remaining fault, it can in principle introduce a malfunction of the I&C in some critical situation. Aven and Ylönen (2016) propose a modelling of uncertainties rather than probabilities in the PSAs, which proposes a reconsideration of the believability of present models. The same two authors are in a later paper (2019) bringing up dangers of standardisation activities with which I cannot agree. Without giving any specific solutions for how to calculate failure probabilities for selected I&C platforms, it seems to be an issue for future research activities.

The need for presenting quantitative probability estimates for human and software errors and failures in the PSAs is in my mind is overstated. It is necessary to present scenarios containing both software and human errors and give qualitative assessments for why they will end in stable and safe states. The argumentation could use statements that certain errors and failures are made almost impossible due to empirical (based on tests) or structural (based on design) evidence. For software, the argumentation might build on paths of execution in the state space of I&C functions, where it can be shown that no unexpected execution paths have been observed during tests. Similarly, for human errors is may be argued that sensitive actions most likely will be executed correctly, given available instructions and interfaces to the plant through I&C systems. A similar argumentation would be used to argue that planned arrangements for ensuring diverse power supplies within 72 hours of a total grid blackout are satisfactory.

4 Processes of I&C design and construction

Processes of design and construction rely on systems engineering in many ways. To improve processes for design and construction of new nuclear power plants it is necessary to build an understanding of problems that have been encountered and solutions that may be used to circumvent these problems. One important condition for success is planning, which is reflected by the saying "good planning is a task half done". The planning of a plant design and construction project contains many independent sub-projects that require their own plans and schedules. Communication between them, therefore, becomes a major task that may require its own efforts (Pirzadeh et al. 2020). There will also exist complex relationships between tasks in sub-projects that may influence their order of execution. The preparation of the buildings, the installation of major components and the necessary cabling as well as the preparations for plant commissioning will all need their own planning.

Processes of I&C design and construction are only one small part that will require own efforts to fit into the larger picture that is governed by a management system. I&C design today will most likely rely on at least two different actors of which the first is the vendor of the I&C platform and the second the designer of the I&C application using selected platforms. Installation and commissioning of the I&C system is a major task that relies on detailed plans for installing process inputs, cables, cubicles, control rooms and control elements as well as ensuring that signal and power interconnections are correct. As the final step before start-up, the safety case should be finalised and approved.

4.1 Design management

A management system for the design process is an important precondition for a successful project. Depending on the character and size of the project one may consider using a set of standards or a specially designed management system. A company specialised in design and construction most likely has its own management system, but it should still be amended with conditions that apply to projects at hand. The intent of the management system is to ensure that all possible means are used to ensure a smooth accomplishment of the project. This also includes an avoidance of late design changes, which always pose a threat due to needs for tearing up earlier design decisions and redoing parts of the design. An important part of the management system is the V&V processes by which design quality can be ensured. Deliberate activities to avoid design errors is an important part of the management system. Taylor (2007B) gives in his paper an overview of design activities in the chemical industry together with a characterisation of typical design errors. Kinnersley and Roelen, (2007) point especially to the need to invest enough resources in requirements capture and specification, from which more than 40% of design errors seem to emerge.

A commonly used model of the design process is the so-called V-model (IAEA, 2016B, p.12). According to the model there is a path leading from abstract concepts to modules and concrete solutions. The upward leading path covers the gradual integration of finalised modules to larger entities. The V-model has its origin in software engineering, but it has been subjected to criticism (Bosch, 2016). Authors have stressed that the model gives impression of sequential processes and that it does not utilise early prototyping with executable specifications and parallel development activities.

The definition of modules occurs on various levels of abstraction. The use of levels of abstraction promotes a better understanding of structure and relationships and can thereby make it easier to concentrate on control flows and interfaces between modules. De Weck et al. (2016) argue that levels of abstractions can serve as an indicator of the complexity of a system and its subsystems. 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 $(7\pm2)^m$, where m is the number of abstraction levels used in the design of the system.

The management system used should stress the importance of avoiding design errors, because the later they are detected the larger are the efforts to correct them. A good practice is that the management system defines several barriers that help in avoiding errors. Such barriers may stretch from simple checks to be executed before a module is characterised as completed. After that it should be exposed to a semi-formal review by a

second person before it is released as a base to be built on. It is also a good practice to have regular audits of used design practices to ensure that requirements in the management system are followed. When errors are detected after modules have been released, the changes should be carefully investigated to assess needs for updating modules that rely on the faulty module. The corresponding revisions of dependent modules should be implemented carefully because corrections of late errors can easily generate new errors.

4.2 HW and SW design

I&C systems will have two parts, hardware (HW) and software (SW). Since the development of digital I&C the share of HW has shrunk in favour of increased use of SW. Present I&C platforms are the result of an earlier design process in which the HW and the SW of the platform were designed as a product, which is applied in design projects that may take place many years later (André et al. 2017). This means that there may exist substantial experience bases with existing platforms. Considering presently available platforms two major types are available, one processor and one HW based approach. The HW based approach can be realised with application specific integrated circuits (ASIC) or with field programmable gate arrays (FPGA). Processor-based platforms are more flexible than HW based systems, which instead have the benefit of having no practical limitations in calculation capacity. From a functional point, of view most platforms combine floating point calculations and logic circuitry, which make them largely interchangeable. Differences in platforms are however found in their sets of basic functions, in their internal failure detection and correction capabilities and the amount of nuclear experience the platform vendor has collected. The I&C platform is in my view the proper place to tackle possible PSA concerns.

One specific quality that may be important to consider, is whether the platform has capabilities to make it possible to adapt to future modifications. As an example, one may consider the need to exchange the used microprocessor from an older to a newer generation (Bock, Richter, 1998). Despite arguments of the platform vendor, it may be difficult to get regulatory acceptance for platform upgrades without redoing earlier certification tests. A platform that is designed with a well-structured modular architecture can be assumed to be relatively easy to update with new components (Bonvoisin et al. 2016). The selection of the programming languages to be used in a platform can have some influence on the final product (Halang, Zalewski, 2003; Motet, 2009), but can at least in principle be compensated by the creation of additional hierarchical levels in the used software (Wahlström et al., 1979). Han et al. (2020) presents a general overview of benefits for both platform vendors and users.

The perhaps largest differences between I&C platform are connected to their applicability for nuclear applications. Due to the need to get regulatory approval their functional implementation is often discussed at length. If the platform from a licensing point of view has to be considered as a black box, it may be difficult to argue for the absence of certain types of SW failures, but even some transparency may change the situation. To take an example, a processor-based platform has a sequencing mechanism that executes the I&C application in an endless loop. A crucial question is to what extent this loop is influenced by process events and operator actions. Is it possible that the execution due to a SW fault deviates from the loop and introduces spurious activities? If one can provide transparency regarding this loop and how it has been tested, it may be possible to single out spurious activation as a threat to be considered in the safety case.

The tacit understanding in the nuclear domain has been that components need to have a nuclear acceptance. For the I&C that is not safety graded, a simple solution could be to use standard industrial systems. Could it even be possible to get some sort of certification for such system under the heading of commercial of the shelf (COTS) systems (OHalloran et al. 2017; IAEA, 2020). At least it would make it easy to use field buses, smart sensors, wireless interfaces, radio frequency identification (RFID) as well as configurable interface units to valves and pumps.

4.3 Installation and commissioning

The design should not only be functioning, but it should also be possible to install, commission, maintain and update. This makes it important to ensure effective communication and documentation in all phases of design and construction (Pirzadeh et al, 2020). An important step in these tasks is a successful execution of the agreed FAT and SAT. A common requirement for the I&C systems is that they should have spare capacity for later additions. The easiest way to take care of this requirement is to execute the FAT and SAT with installed dummy functions that spend the required spare capacity. It is a good idea to have additional equipment available that could simulate actual physical interfaces to the plant.

For the installation of I&C modules it would be beneficial to integrate them as far as possible. That would also facilitate the SAT after installations at the plant. The availability of a full scope simulator of the plant could not only support operator training, but also the production of data describing expected outcomes from FAT and SAT. An important part of the commissioning tests for I&C cables is to ensure that they are connected correctly at both ends. For this purposed it is proposed to use specialised interface units that can do this testing, to avoid manual testing as far as possible. For major components, the expectation is that have their own interface units to internal sensors in a support of condition monitoring.

4.4 Regulatory acceptance

Regulatory acceptance relies on national laws and regulations. There are, however, considerable variations in applicable regulatory systems (Wahlström, 2007). This implies a large burden for vendors and suppliers working in a global context, because solutions that are acceptable in one country may not be acceptable in another country. There have been steps taken towards an increasing harmonisation of nuclear requirements thanks to efforts by IAEA and WENRA. In Europe one document regarding requirements on software has got a large support (Common position, 2018). Despite the level of general harmonisation of the requirements that are placed on I&C systems, there are still large differences in the oversight strategies and practices that are applied in different countries.

Present national systems of nuclear regulation have since the new millennium in an increasing amount relied on international standards that have been created and maintained by IAEA as well as by bodies such as IEC, ISO, and IEEE. If this development continues, the relevance of the national systems of requirements may gradually be taken over by these bodies. Such development would at least in a practical sense be desirable in view of the nuclear technology being increasingly global and it may even promote harmonisation between national requirements.

Basically, on may say that all V&V activities that have been agreed on should be described in triplets of requirement, evidence, and conclusion. Unfortunately, many of the systems of requirements contain arguments concerning completeness, consistency, and correctness (C^3), which must be restricted if any valid claim would be possible to give (cf. Appendix). Important is still to argue also for why the tests can be considered sufficient for claims that are made (Lv et al. 2014). In planning for the tests to executed during the design process, it is necessary acknowledge the need for involving right people for the results to be correctly interpreted (Mäntylä et al. 2012). In the safety case, there will be separate chapters on issues such as

- plant responses to selected disturbances and accident conditions,
- I&C responses to various fault conditions such as failing inputs, transmission failures, failing hardware, failing power supplies, etc.,
- possibilities for CCF and how they are abated (IAEA, 2009),
- validation of the requirements for operability (OECD/NEA, 2019).

Looking at the requirements placed on I&C and the possibilities to provide evidence for safety claims, my impression is that expectations often are unrealistic in their requirements for C^3. It is theoretically and practically possible to ensure such arguments only when they are restricted to quite simple cases. Early agreements on necessary and sufficient requirements to be considered in the safety case, must be reached early

between plant owner, plant vendor and the licensing body. To take one example, the set of scenarios for which safety should be demonstrated has to be agreed on before details of I&C design are defined.

5 Support systems

I&C systems have over the last fifty years gone through an exceptional development. This can be seen both in the I&C systems themselves and in the computerised support systems that are installed in all industrial plants today. For the nuclear power plants this implies that the I&C as well as the support systems should be granted a lifetime that may exceed eighty years. This requirement is exceptional when we look backwards to our plants that were planned and designed fifty years ago. Already to keep them up to date with present standards has required extensive modernisations that sometimes made it necessary to reconstruct and computerise their original design base that was available only on paper, gives an impression of needs to plan.

The support systems will be keys for future success of plants that are planned and built today, which means that they should be designed and built for an increasing set of users that have quite different demands. It is therefore likely that support systems will be built on computer platforms that may or may not be considered as safety or safety related systems to be targeted for regulatory review. One possibility to look forward is to consider the ideas that were the basis for design fifty years ago and compare them with thoughts on what would be feasible today. For the nuclear power plants built in Finland in the 1970ies and 1980ies an important step was to use process computers to support plant operation using monitoring and display. Today computers are used in all phases of design, construction, commissioning, operation, modernisations, decommissioning and restoring of plant sites, which gives an impression of the support people will need over the years in decisions regarding safety.

One simple approach is to say that all support systems that were used in the design and commissioning of the plant will be needed also later. This applies to support systems, which are used years before the first concrete has been poured at the plant site. The report (EPRI, 2016) argues for the need for an information turn over strategy to stretch over the intended lifecycle of a plant. One may even argue that a digital twin (Bickford et al. 2020) of the plant, which is kept updated, can during plant life provide help to various groups of people to test out action alternatives before they are implemented. This gives a possibility to ensure that plant safety can be checked virtually before planning and design activities. Using an integrated set of support systems, it is possible to avoid errors by detecting and correcting them even before steps to implementation are taken. With due updates after plant changes such a digital twin can ensure the existence of a stable basis for later activities. Below I discuss specific support systems for applications design, operations and maintenance and the possibilities, which artificial intelligence may provide as support for these activities.

5.1 A safety philosophy

The I&C design for a new nuclear power plant is anchored in a safety philosophy that is applied for the plant. The safety philosophy can in a way be mapping appropriate functions in a two-dimensional design space consisting of the DiD level (1,2,3a3b,4,5) on one axis and the I&C layers (information management, supervisory control, process control, field control, sensors, and attenuators) on the other axis. This mapping serves as a guide for the I&C architecture (IAEA (2018A), where the functions in a second step are associated with selected platforms and computerised support functions. The next important step is to set the division between automatic and manual operation i.e., the level of automation (Scheridan, 2000). Already in this stage an important step is to evaluate the need for various support during plant operation.

A common separation between safety systems is to speak about plant, system, and component levels of safety. The algorithms that are supposed to react om problems on a plant level have to collect signals from a large frame of systems and may be due to their complexity be seen as operator support systems, i.e., the operators are supposed to act on the information they provide. On the system level algorithms are likely to be defined by system vendors and will be connected to main actuators of the systems. The tasks for the I&C applications are

supposed to be implemented by both automatic and manual solutions. For the component level protection, it is likely that simple algorithms are suggested to ensure that they will move to safe states in case of malfunctions. Valves and pumps are typically in this category, which may make it necessary to ensure that both plant and system protection in certain conditions should be allowed to override component protections.

The safety philosophy is embedded in the safety classification, which is a shorthand indication of the safety importance of specific structures, systems, and components. The classification instrument for a plant should according to regulatory requirements be available early in a plant construction project. The safety classification gives according to the principle of a graded approach to nuclear safety a connection between V&V methods and efforts to be used selected systems.

5.2 Applications design

Applications design has to do with applying specific I&C platforms for selected I&C architecture. It relies therefore on functions provided in the platform. Some platforms have a restricted set of functions specifically intended to be used for safety and safety related systems, because they have gone through more extensive testing when they were developed. To what extent this gives an opportunity to argue that specific design errors have been removed from these functions is something to be considered in negotiations with the regulatory bodies, but they may prove to ease their acceptability.

The platforms have typically many support systems that are intended to make application design easier. The availability of such support systems may also prove to be a dividing argument in the selection between two otherwise similar platforms. It may even be possible to automate some parts of the application design and to enable rapid testing of proposed design alternatives (Rigger et al. 2020). Ideally design support should be well integrated with relevant databases from which important information could be collected and crosschecked. This would imply necessary connections between the databases and flexibility in building searches for various questions that may arise. Applications can as a start be based on simple database systems that keep track of plant signals and internal variables of the I&C system. The handling of requirements, configuration and documentation should also be implemented in support systems. The use of 3D modelling of buildings is another important application that in addition to design of plant piping can be used for design of cabling and power supplies for the I&C. The design of procedures to be used in operations and maintenance can build on this information to be utilised together with simulations of the whole plant to analyse responses to selected disturbances and emergencies.

An important issue in design is to be able to simulate plant responses with various I&C alternatives. In practice this implies a large range of models with a varying fidelity (Hu et al. 2018) depending on the intent of the simulation. For example, in the verification of accident behaviour it is important that the thermohydraulic behaviour is simulated correctly, which means the rest of the plant may be described with less details. Similarly, a full scope simulation of the plant and the control room would be required when the task is to validate control room design (OECD/NEA, 2019).

In support of developing and maintaining the safety case of the plant, there are several packages that can provide support to specific chapters. Help could for example be obtained by keeping accurate track of dependencies (locations, systems, power supplies, etc.) between components and signals (Benard et al. 2008). Another example are the accident codes and the packages for thermohydraulic load flow calculation, which can be used to assess the acceptability of safety measures in disturbance and emergency situations. Important are also the PSA packages with which the resulting core damage probability of various combinations of hidden faults, component failures and erroneous operator actions can be calculated to assess the need for improved protections. These packages may also be adapted to provide a display of a real time risk profiles during operation to support assessments of plant state. Virtual reality (VR) tools based on 3d modelling of the plant can in turn interfaced to radiation calculation software provide efficient training facilities for maintenance actions in spaces with increased radiation levels.

Much has been written on software development, which is more directed to the development of I&C platforms than to specific I&C applications. For example, Asplund (2015) considers software design for the transportation domain and points to the need for integrated support systems that can automate crucial task of the design process. The availability of information from the platform design and maintenance can provide important information for assessing platform suitability for safety automation in the nuclear domain.

5.3 Operations support

Operations support can be divided into three distinct but overlapping areas. The first may be called operative and is considered with normal day-to-day activities. Activities in this area are considered with an overview of the previous week and planning for the coming week. In the plans availability of necessary resources is checked and more detailed guidance for various activities are produced. The second area may be called tactical and is concerned with the planning from the recent start-up to the next refuelling shutdown. For this planning the main challenge is to keep the shutdowns as short as possible. Many detailed plans, which imply that contracts are written with vendors, consultants, and maintenance companies for actual work to be executed. The third area may be called strategic has an outlook that stretches over several refuelling periods to evaluate needs for complicated inspection and maintenance actions, plant changes and other possible actions that are needed for ensuring the plant to be operated for its projected lifetime. Due to the exceptionally long operational life, there is a challenge simply to keep them all operating and to ensure data integrity.

One important issue is to transfer all design support systems also to be used during plant operation, because they will be needed when plant or I&C modifications are made. For a new plant it is likely that there are design deficiencies that the plant owner would like to correct detected problems. Then it is important that modifications do not introduce new problems because of changes made. In the light of present understanding it is likely that major I&C modernisations will be necessary after some twenty years. If specifications and other information from the original design is available in computer readable form, it makes the modernisation easier.

Considering present operational NPPs their level of automation has a large span. Comparing the level of automation as seen in conventional industry, with the level of automation in typical NPPs operated today, they represent older technologies. When problems of obtaining spares have occurred modernisations of the I&C can be forced. Sometimes however, there have also been new support systems introduced, such as the safety display systems after the TMI accident. These systems were however, mainly motivated as corrections of earlier deficiencies in the control rooms of their time (cf. Bainbridge, 1983).

Looking at the four operating reactors in Finland, they have a rather high level of automation (Parasuraman, Sheridan, 2000). They have sequence automatics that support states changes, which include checks that certain conditions are fulfilled before the sequence is moved from one step to the next. Safety automation can initiate automatic actions on multiple objects when certain conditions are detected. The information systems at the Finnish plants have been modernised and have at each round been improved regarding monitoring and analysing functions. For the two new Finnish reactors presently being built the selected level of automation is roughly similar as compared with the four older reactors. Sheridan (2000) is voicing support for additional automation presumed that it is developed with conscient understanding of operator needs.

The nuclear domain relies on a combination of corrective and predictive maintenance. The cost of outages implies a focus on predictive parts of maintenance activities. This implies closely monitoring states of major components for an early detection of emanating failures. In the design phase this principle suggests the inclusion of additional sensors for condition monitoring and control. Correspondingly in the operational phase reliability models can be used to optimise test and maintenance intervals.

For the large, but also for smaller components, we may in the future assume that they will have their own local intelligence for condition monitoring and control, which in the response to various degrading mechanisms can give estimates for remaining time of undisturbed operation. It seems clear that with such projections systems for maintenance support will grow considerably in the future. An object for development is also the maintenance instructions, which can be built on an extensive use of pictures. I also think that this general

principle can be applied in the software of the I&C systems. If this principle is applied for platforms, it could ensure that their dependability is increasing with the years they are utilised in actual plants.

5.4 Artificial intelligence

Artificial intelligence (AI) is back on many research agendas after a quite life for nearly thirty years. It is therefore interesting to look how the technology might influence the nuclear domain. One thing is certain, the design processes for industrial systems will be influenced. Computers are already now used for predicting probable paths for state excursions when major components fail. The nuclear domain uses full scope simulators for the training of operators. Document and configuration management systems are applied for newer plants but have not for older plants reached a penetration one may wish. The AI technology can open large possibilities for support functions during operation, but hard requirements for V&V assessments (Common position, 2018) of used algorithms may make it impossible to use them for safety or safety related systems. Automated language analysis has already reached a level, where it would be possible to analyse instructions to achieve better consistency in use of language and concepts.

Requirements management would be another low hanging fruit, especially if AI could be used to implement functions to analyse relationships between requirements and to build a database on how they have been responded to. Systems of procedures and instructions would also be interesting in the operation of the plants. Madni and Sievers (2018) foresee the introduction model-based systems engineering (MBSE) as a major innovation for industrial domains and I agree with them that nuclear is one. The analysis of events has already advance to the level of research application, due to algorithms able to analyse written text (Morrow, 2014).

I see the licensing process as another interesting application for AI, especially due to the need to integrate both qualitative and quantitative data (Hybertson et al. 2018). Among the ideas is also an application (Moura et al. 2017) of the so called self-organising maps (SOM) for accident analysis. For future research application one may even suggest the development of operator models that can be connected to databases of instructions, which could operate a full scope simulator version of the plant. By running such system of systems (SoS) models, one could perhaps identify previously unknown transients that may challenge plant safety. Santosh et al. (2009) propose to use an AI-based system to support operators in diagnosing a loss of coolant (LOCA) events in nuclear power plants. I think these proposals are sound, but one may ask if a regulator would accept such solutions and perhaps even give the plant credit for them.

6 Towards the future

Nuclear I&C depends on future development of the nuclear domain. For people familiar with the nuclear it may feel strange that opposition against nuclear power plants still is strong, despite the need for a global transfer of energy supplies away from fossil sources. Western democracies, with some notable exceptions, seem to have decided to disregard the nuclear opportunity by phasing out their nuclear fleet and shutting down older plants without planning for replacements. Newcomers in the world are forced to rely on a diminishing number of plant alternatives due to the disappearance earlier nuclear vendors. There is a rising interest in small and medium sized reactors (SMR), but before this technology can make a difference, massive investments in research and development seem to be needed.

A new and interesting field of research connected to SoS is addressing command and control for networked systems (Eisenberg et al. 2018). The authors suggest an approach for polycentric control that include models of physical, information, social and cognitive domains. I&C design has a tradition of processes that were used in the analogue age. Whether or not they still are useful for digital systems can be doubted. My own feeling is that it may be appropriate at least to look on new approaches such as the one proposed by Fiorineschi et al. (2016). To what extent industrial initiatives such as the *Industry 4.0* (Tay et al. 2018) will develop, is also interesting to see.

6.1 Models of and in systems engineering

Two types of models are used in systems engineering, one set of models help in understanding how different parts of the design process link together and move forward in time. The other type of models is specific for well defined design tasks that help the designers to manoeuvre between conflicting requirements and to optimise selected designs according to sometimes conflicting criteria. Kannengiesser and Gero (2015) discuss the first type of models by presenting typical task structures for design projects and they build models of functional-behaviour-structure (FBS) that can be of help for discussing variations in the structure of design projects. Flach et al. 2017 point to the need for combining design and cognitive sciences to be able to find a balance between product and human centric thinking. They bring forward the concept of affordance, which can help to find a balance by admitting that there exist implicit costs that cannot be afforded by acting only on one type of demands. Gran (2002) proposes the use of Bayesian belief nets to establish confidence in finalised products, but my feeling is that this method would be better placed to establish confidence in the design process as such.

Safety culture has since the Chernobyl accidents become a catch phrase in the whole nuclear domain. One may ask if the concept could be used for tasks done in a design project. With an analogy one could say that it is a different task to design a safe car, as compared to drive a car safely. This distinction was however not recognised at one point in time, when I was involved in an IAEA mission to South Africa to evaluate the safety culture of a design organisation (SCART, 2006). The method suggested for that mission was not adapted to the business and tasks of design organisations. If such a mission would be undertaken today, they should be based on an understanding of how design contributes to operational safety. A first iteration of applicable views and methods for a considering safety culture in design organisations may be found in the report (Macchi et al. 2013).

6.2 Dependable I&C systems

Not to get lost in all the -ilities that are suggested for software one may perhaps start to speak about dependable I&C and what that could mean (Conrard et al. 2005). The problems of complexity with software-based solutions were identified early (Leveson, Harvey, 1983) and unfortunately the problems these authors bring forward have not yet found satisfactory solutions. Many methods to ensure dependability of software have been suggested, but the best methods seem still to be a combination of early testing of concepts together with a considerate quality controls of the design process as defined in a management system. Dependable software packaged into a versatile I&C platform would in my mind be the solution to aim for.

Another problem is connected to the C^3 issues (cf. Appendix) because systems of requirements cannot be complete. Furthermore, it is not possible to say if a piece of software will reach a specific state or not. without running it, which in most cases is practically impossible. A possibility to introduce fault management in the software is not always practical, because it will increase system complexity and make it necessary to consider the possibility of these provisions may fail. In addition, the use of models in engineering processes, implies that there is always a possibility that used models are not correct representations of reality. This means that I&C design must live with possibilities for errors and failures. Despite these difficulties there is in my mind possibilities to establish both structural and empirical evidence for dependability. Structural evidence can be collected from the design process, where it is proved that good design principles have been followed. Empirical evidence can correspondingly be collected from comprehensive testing of both single modules and the gradually increasing entities that are formed in integrating the modules. Specific assurance of software safety can finally be collected during FAT and SAT by integrating suitable online test modules in the I&C system.

Present large nuclear power plants were designed for base loads in the transmission networks to which they are connected. This situation has changed today with increasing amounts of sun- and wind-based power plants in the transmission grids. Future power plants have therefore to be able to react flexibly to changes in supply and demand. This would place requirements on load following for future nuclear power plants to be reflected in the I&C design (IAEA, 2018B).

I have so far not touched on the difference between safety and security (Kriaa et al. 2015; Iaiani et al. 2021), which certainly are important for I&C systems. In its simplest form one may say that safety involves fighting nature, but security is the task of protecting against intelligent villains. Other models have therefore to be used for security because the essence of the problem is game theoretic. A simple approach to the problem is a two-by-two matrix, where two players (protector, villain) can invest resources either to protect against or to execute an attack. Considering expected costs and benefits of successful attacks both the protector and the villain have their own break evens. The protector should make successful attacks more expensive than the cost the villain is willing to spend. Similarly, the villain will attack, if the expenses to mount an attack are less than the gains of a successful attack.

One specific concern in the nuclear domain is to ensure that there is a pool of knowledgeable and experienced engineers for the lifetime of the plants. This means that educational and research institutions must be supported for futures longer than typical quarterly economics of the business world. In Finland we have universities active in the nuclear domain both in Helsinki and Lappeenranta. We also have continuing research programmes in the domain of nuclear safety that have been active from the early 1970ies (Hämäläinen, Suolanen, 2018; Wahlström, 2020). The present programme continues to the year 2022 and has subprojects related to I&C.

6.3 Societal responses to risk

Views on risks in the society has developed over the last fifty years and many things have changed. I had the privilege to work two years at the International Institute of Applied Systems Analysis (IIASA) in Austria from 1989 to 1991 and I have been following academic discussions in the area since then. The perhaps most important change of views is coupled to the work of Ulrich Beck (1992), which was published in German already in 1986. The Journal of Risk Research was running a special issue (Burgess et al. 2018) on the influence of Beck on societal considerations of risks, which among other things pointed out the fact that many risks today actually are introduced by human and organisational actors in major industries. I remember from my time at IIASA that the theses brought forward by Beck and others were not, perhaps wrongly, held in high esteem by my nuclear colleagues at that time.

This general theme has been taken up by other researchers. For example, Michael Power has in two books analysed general trends in responding to risks by setting up risk management systems in organisations that operate risk prone processes (Hutter, Power, 2005; Power, 2007). Some researchers see the situation in a need of new approaches (Pasman et al. 2013) and others are concerned with the bureaucratisation of risks (Dekker, 2014). A Finnish study (Ylönen, Litmanen, 2015) points to the fact that lessons learned are continuously evaluated by the nuclear industry to select what to react on and what to disregard for the time being. It is not astonishing that different people have different views on what is important and what is not. The development more generally caused researchers to consider the effectivity of actual safety activities. Rae et al. (2018) for example has pointed out that there may be “safety activities” that have no or even negative influence on real safety.

Resilience is a concept brought forward about fifteen years ago (Hollnagel et al. 2006) and other researchers have responded (Linkov et al. 2013). The idea being that risk analysis and safety engineering should not only look at errors and failures, but also on successes where the systems were able to resume their functions after adverse events. Uday and Marais (2015) point out the need to see resilience in a system of systems approach, which itself carries many challenges (Harvey, Stanton, 2014). The concept of resilience has found support especially when societal risks have been investigated (Patriarca et al. 2018; Bergström, 2018). However, I do not, as many supporters do, see resilience engineering as something entirely new and different from classical methods, because even looking at successes you must know what to protect against. As Kontogiannis (1997) explains, designers and operators have to adopt recovery centred approaches, which at least in some respects relies on cognitive capacity of persons who face new dangerous situations.

More generally regarding these issues, I have a strong feeling that the nuclear industry has too much disregarded societal aspects of nuclear safety. Just considering the three major accidents, TMI, Chernobyl and Fukushima, criticism may be expressed. The TMI accident illustrated major flaws connected to human and organisational factors (HOF) that were known but not corrected before the accident. Chernobyl demonstrated major flaws that were attributed to a deficient safety culture, which at that time was not considered as a specific issue to consider. However, many of the studies after the TMI accident pointed at least in principle to issues that should have made Soviet regulators to reconsider their own oversight of the nuclear domain. The comment I heard from Soviet colleagues at that time was "TMI was an accident possible only in a capitalistic country". If this statement is accepted, then Chernobyl was an accident possible only in a communist country. The Fukushima accident was in my view caused by a violation of the single failure criterion. It was caused by a large earthquake and the tsunami it caused, which prevented residual heat removal. Sweden in a similar situation in 1992, when doubts were raised regarding the single failure criterion, it was decided to shut down all plants that were affected until the deficiency was corrected (Teperi et al. 2019).

Increasing complexity of the I&C systems introduces a need for deep knowledge and insights that may not be available by regulatory bodies. It may therefore be necessary for regulators to increasingly rely on consultants for making assessments. Another solution could be if the nuclear domain would create systems of accreditation and certification to be established on a global scale. This would enable organisations working globally to accredited to do certified assessments in selected fields of I&C design (Heck et al. 2010; Dodd, Habli, 2012). Regardless of the solution selected, I feel that the most practical solution for nuclear regulatory systems is to create and maintain them on an international scale. This would imply that normative versions of the systems of requirements would be written in English, which still leaves needs for interpretations due to their formulation in natural language.

6.4 A future of nuclear

Today the uncertainties connected to new nuclear power plants is a problem. Without new plants to be built, the likelihood is small that the problems with I&C outlined in this paper will be addressed and solved. There is a possibility however, that a generation of small and medium sized reactors (SMR) are considered attractive enough to be built. They would in any case need major investments in international cooperation to establish necessary knowledge bases and licensing requirements to move forward. If the nuclear domain instead proceeds along a business-as-usual path, the nuclear contribution to world energy may stay around the present 10% with new plants replacing only those shut down finally. In this case it may even be decided that I&C modernisations are too expensive if plants are supposed to fulfil new regulatory requirements.

Present problems are also connected to the need for adaptations a global market with long chains of suppliers (Ruuska et al. 2011). I&C platforms for process industries are available, but there may be problems with their acceptability in the nuclear domain. It would still be necessary to manage long chains of linked contracts (Esterman et al. 2020), to use best available technologies (BAT) from a global market. The question is if financiers are willing to invest in R&D as well as in pilot plants to be built. Even if this could be ensured there is still a need for sites where these plants can get public support.

If the nuclear domain would be able to take part in activities to combat climate change, there is a need to move forward and to think big (Flyvbjerg, 2014), because development will otherwise be too slow and/ or too expensive for single actors. From a Finnish point of view, we have two large nuclear power plant in the pipeline. I do not think we could get support for a third plant of this type. However, if there would be SMRs on the market, one may perhaps be more optimistic, especially if they were designed for production of heat and/or hydrogen. Finland is a cold county and not very densely populated, which places demands on heat production wintertime and transportation during the whole year.

If we look at possibilities for new builds, the projected costs will be one of the deciding factors (Lovering et al. 2016; OECD/NEA, 2020). Important is also the type of project foreseen because a series of first-of-a-kind-engineering projects (FOAKE) (Patterson, Clarkson, 2015), cannot utilise the organisational learning that is

needed to make projects profitable. Perhaps the capability for organisational learning is one of the crucial things for the nuclear domain (Argote et al. 2020). My own impression is that the nuclear domain has stumbled seriously several times in developing the technology for civilian use.

7 Conclusions

Systems thinking is concerned with the need to at the same time consider both entirety and details. I have in this article taken a broad view on nuclear I&C, where issues have been left mostly as simple mentioning. If they in the future could be given more attention and become research agendas for in depth investigations, it may be possible to move forward. Sheard (2018) gives in her article impressions of how systems engineering has developed over a period of fifteen years and influenced software engineering. With concrete projects a similar development in nuclear I&C might perhaps have been possible. The almost total stand still on the market of nuclear power plants after 1990, forced however plant vendors to restructure their operations from two earlier decades when an average of 16,6 new plants each year were taken into operation

Large plants seem still to be possible to build by engineers in South Korea, but even France seems to have lost some of their abilities in building large plants, which examples of Flamanville and Olkiluoto illustrate. The Russians seem to have support from their national research and funding sources, but they still seem to have difficulties to adapt to standards that are applied in large international projects. The skills that were found in the Soviet Union for the Loviisa plant forty-five years ago seem not to have been maintained.

At the end of my paper, I will try to summarise conclusions that I have collected after my retirement. It is based on reading academic literature in systems thinking. I think our young engineers would be well positioned to take care of details, if we old-timers are able to point out what is wrong with present systems. What kind of changes are needed in the systems, which is composed of not only, nuclear operators, vendors, universities and regulatory bodies, but also of the entire socio-technical system of financing, politicians, media and common people? If the nuclear is seen as a problem and not as a solution, there is no possibilities to move forwards. I have selected the following three bullets, where I think additional understanding would be needed:

- Large development projects need a broad cooperation both nationally and internationally, where one example could be needs for finding commitment for a transfer away from fossil energy sources for electricity production.
- Possibilities to achieve better cost and timetable estimates for projects in the nuclear domain, i.e., both newbuilds and modernisations of existing plants, should be investigated. Interesting would also to provide reasons for problems that have been experienced.
- Possibilities through systems engineering develop project methods and tools for the creation of dependable I&C solutions should be investigated. Efforts should be divided between design and development of versatile I&C platforms and the development of computer-based support systems suitable for the nuclear domain.

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 program. The only way to do it, is to run the program and see if it was reached or not. Again, this is 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 counterpart can be proved. I interpret this in such a way that a system of requirements is either incomplete or inconsistent.

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 its I&C systems together with failure modes. If specialised I&C is added to compensate for failures of the rest of the I&C, this will cause an ever-increasing complexity and therefore there will be failure modes that cannot be controlled.

Disclaimer: This paper was written by an old-timer, who has more than fifty years of personal experience from the two domains of nuclear and I&C. Being old has disadvantages, but also advantages. Now I can say what I couldn't say earlier in my career and I have collected anecdotes with which I can illustrate some follies that I have seen during the years.

References

Samuel André, Fredrik Elgh, Joel Johansson, Roland Stolt (2017). The design platform – a coherent platform description of heterogeneous design assets for suppliers of highly customised systems, Journal of Engineering Design, 28:10-12, 599-626.

Linda Argote, Sunkee Lee, Jisoo Park (2020) Organizational Learning Processes and Outcomes: Major Findings and Future Research Directions. Management Science, doi.org/10.1287/mnsc.2020.3693.

Fredrik Asplund (2015). The future of software tool chain safety qualification, Safety Science, 74, 37–43.

T. Aven, M. Ylönen (2016). Safety regulations: Implications of the new risk perspectives, Reliability Engineering and System Safety, 149, 164–171.

Terje Aven, Marja Ylönen (2019). The strong power of standards in the safety and risk fields: A threat to proper developments of these fields? Reliability Engineering and System Safety, 189, 279–286.

Liseanne Bainbridge (1983). Ironies of Automation, Automatica, 19: 6, 775-779.

Jan Bosch (2016). Speed, data, and ecosystems; the future of software engineering, IEEE Software, 82-88.

Beck, U. (1992). Risk Society: Towards a New Modernity. London: Sage.

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.

Johan Bergström (2018). An archaeology of societal resilience, Safety Science, 110, 31–38

Jason Bickford, Douglas L. Van Bossuyt, Paul Beery, Anthony Pollman (2020). Operationalizing digital twins through model-based systems engineering methods, Systems Engineering, 23:724–750.

H.-W. Bock, S. Richter (1998). Ensuring long-term availability of Teleperm XS, IAEA XA9949623.

Jérémy Bonvoisin, Friedrich Halstenberg, Tom Buchert, Rainer Stark (2016). A systematic literature review on modular product design, Journal of Engineering Design, 27:7, 488-514.

Richard Buchanan (2008). Introduction: Design and Organizational Change, Design Issues: Volume 24, Number 1, Winter.

Adam Burgess, Jamie Wardman & Gabe Mythen (2018). Considering risk: placing the work of Ulrich Beck in context, Journal of Risk Research, 21:1, 1-5.

Bradley Camburn, Vimal Viswanathan, Julie Linsey, David Anderson, Daniel Jensen, Richard Crawford, Kevin Otto, KristinWood (2017). Design prototyping methods: state of the art in strategies, techniques, and guidelines, Des. Sci., 3, 1-33.

Benjamin T. Ciavola, John K. Gershenson (2016). Affordance theory for engineering design, Res Eng Design, 27:251–263.

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

Blaise Conrard, Jean-Marc Thiriet, Michel Robert (2005). Distributed system design based on dependability evaluation: a case study on a pilot thermal process, Reliability Engineering and System Safety, 88, 109–119.

Nigel Cross, Anita Clayburn Cross (1998). Expertise in Engineering Design, Research in Engineering Design, 10:141-149.

J. S. Busby (1998). Effective Practices in Design Transfer, Research in Engineering Design,10:178-188.

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

J. C. F. de Winter, D. Dodou (2014). Why the Fitts list has persisted throughout the history of function allocation, Cogn Tech Work, 16:1–11.

Francesco Di Maio, Ajit Rai, Enrico Zio (2016). A dynamic probabilistic safety margin characterization approach in support of Integrated Deterministic and Probabilistic Safety Analysis, Reliability Engineering and System Safety, 145, 9–18.

Ian Dodd, Ibrahim Habli (2012). Safety certification of airborne software: An empirical study, Reliability Engineering and System Safety 98, 7–23.

Sidney W.A. Dekker (2014). The bureaucratization of safety, Safety Science, 70, 348–357.

Claudia M. Eckert, David C. Wynn, Jakob F. Maier, Albert Albers, Nikola Bursac, Hilario L. Xin Chen, P. John Clarkson, Kilian Gericke, Bartosz Gladysz, Daniel Shapiro (2017). On the integration of product and process models in engineering design, Design Science, vol. 3, 1-41, DOI: 10.1017/dsj.2017.2.

Boris Eisenbart, Kilian Gericke, Lucienne T. M. Blessing (2017). Taking a look at the utilisation of function models in interdisciplinary design: insights from ten engineering companies, Res Eng Design, 28:299–331.

Daniel A. Eisenberg, David L. Alderson, Maksim Kitsak, Alexander Ganin, Igor Linkov (2018). Network Foundation for Command and Control (C2) Systems: Literature Review, IEEE Access, 6, 68782-68794.

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.

EPRI (2008). Generic requirements specification for qualifying a commercially available PLC for safety-related applications in nuclear power plants, TR-107330.

EPRI (2009). Effects of Digital Instrumentation and Control Defense-in-Depth and Diversity on Risk in Nuclear Power Plants, 1019183.

EPRI (2014). Effects of Digital Instrumentation and Control Defense-in-Depth and Diversity on Risk in Nuclear Power Plants, 3002002953.

EPRI (2016). Advanced Nuclear Technology: New Nuclear Power Plant Information Turnover Guide (Revision 1), Report 3002007425.

Marcos Esterman, Shridhar Palekar, Francis Conway, Joseph Ehmann, Venus Limcharoen (2020) Toward robust concurrent product development across the supply chain: a risk assessment framework, Journal of Engineering Design, 31:3, 150-177.

Elie Fadier, Cecilia De la Garza (2006). Safety design: Towards a new philosophy, Safety Science, 44, 55–73.

Jeanne Ferrante, Karl J. Ottenstein, Joe D. Warren (1987). The Program Dependence Graph and Its Use in Optimization, ACM Transactions on Programming Languages and Systems, 9: 3, 319-349.

Lorenzo Fiorineschi, Federico Rotini, Paolo Rissone (2016). A new conceptual design approach for overcoming the flaws of functional decomposition and morphology, Journal of Engineering Design, 27:7, 438-468.

John M. Flach, Pieter Jan Stappers, Fred A. Voorhorst (2017). Beyond Affordances: Closing the Generalization Gap Between Design and Cognitive Science, DesignIssues: Volume 33, No.1.

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

Jared Fortune, Ricardo Valerdi (2013). A Framework for Reusing Systems Engineering Products, Systems Engineering, 16;3, 304-312.

Floris Goerlandt, Nima Khakzad, Genserik Reniers (2017). Validity and validation of safety-related quantitative risk analysis: A review, Safety Science, 99, 127–139.

Wolfgang A. Halang, Janusz Zalewski (2003). Programming languages for use in safety-related applications, Annual Reviews in Control, 27, 39–45.

Maggie Hamill, Katerina Goseva-Popstojanova (2015). Exploring fault types, detection activities, and failure severity in an evolving safety-critical software system, Software Qual J, 23:229–265.

Bahram Hamraz, Nicholas H. M. Caldwell, P. John Clarkson (2013). A Holistic Categorization Framework for Literature on Engineering Change Management, Systems Engineering Vol. 16, No. 4.

Xin Han, Rong Li, Jian Wang, Guofu Ding & Shengfeng Qin (2020). A systematic literature review of product platform design under uncertainty, Journal of Engineering Design, 31:5, 266-296.

Catherine Harvey, Neville A. Stanton (2014). Safety in System-of-Systems: Ten key challenges, Safety Science, 70, 358–366.

Laura Hay, Alex H. B. Duy, Chris McTeague, Laura M. Pidgeon, Tijana Vuletic, Madeleine Grealy (2017). Towards a shared ontology: A generic classification of cognitive processes in conceptual design, Des. Sci., 3, 1-42.

Petra Heck, Martijn Klabbers, Marko van Eekelen (2010). A software product certification model, Software Qual J, 18:37–55.

Peter Heisig, Nicholas H.M. Caldwell, P. John Clarkson (2014). Core information categories for engineering design – contrasting empirical studies with a review of integrated models, Journal of Engineering Design, 25:1–3, 88–124.

Babak Heydari, Mohsen Mosleh, Kia Dalili From (2016). Modular to Distributed Open Architectures: A Unified Decision Framework, Systems Engineering, 19:3, 252-266.

Hollnagel, E., Woods, D.D., Leveson, N., 2006. Resilience Engineering; Concepts and Precepts. Ashgate.

Andrew Hopkins (2015). The cost–benefit hurdle for safety case regulation, Safety Science, 77, 95–101.

Imre Horváth (2004). A treatise on order in engineering design research, Research in Engineering Design, 15: 155–181.

Bridget Hutter, Michael Power (eds, 2005). Organisational encounters with risk, Cambridge University Press.

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, 2016A. Design of Electrical Power Systems for Nuclear Power Plants, Specific Safety Guide, SSG-34.

IAEA, 2016B. Design of Instrumentation and Control Systems for Nuclear Power Plants, Specific Safety Guide, SSG-39.

IAEA (2018A). Approaches for overall instrumentation and control architectures of nuclear power plants, NP-T-2.11.

IAEA (2018B)Non-baseload Operation in Nuclear Power Plants: Load Following and Frequency Control Modes of Flexible Operation, IAEA Nuclear Energy Series, NP-T-3.23.

IAEA (2019). Human Factors Engineering in the Design of Nuclear Power Plants, Specific Safety Guide, SSG-51,

IAEA (2020). Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial Digital Instrumentation and Control Equipment for Use in Nuclear Power Plant Applications, NR-T-3.31.

Matteo Iaiani, Alessandro Tugnoli, Sarah Bonvicini, Valerio Cozzani (2021). Major accidents triggered by malicious manipulations of the control system in process facilities, Safety Science, 134, 105043.

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

David B. Kaber (2018A). Issues in Human–Automation Interaction Modeling: Presumptive Aspects of Frameworks of Types and Levels of Automation, Journal of Cognitive Engineering and Decision Making, Vol.12, No.1, pp. 7–24.

David B. Kaber (2018B). Reflections on Commentaries on “Issues in Human–Automation Interaction Modeling”, Journal of Cognitive Engineering and Decision Making, Vol.12, No.1, pp. 86–93.

Udo Kannengiesser, John S. Gero (2015). Is designing independent of domain? Comparing models of engineering, software and service design, Res Eng Design, 26:253–275.

Kinnersley S, Roelen A. (2007). The contribution of design to accidents. Safety Science, 45: 31–60.

Tom Kontogiannis (1997). A framework for the analysis of cognitive reliability in complex systems: a recovery centred approach, Reliability Engineering and System Safety, 58, 233-248.

Siwar Kriaa, Ludovic Pietre-Cambacedes, Marc Bouissou, Yoran Halgand (2015). A survey of approaches combining safety and security for industrial control systems, Reliability Engineering and System Safety, 139, 156–178.

Klaus Krippendorff (2011). Principles of Design and a Trajectory of Artificiality, J Prod Innov Manag, 28, 411–418.

Kamila Kunrath, Philip Cash & Maaike Kleinsmann (2020A) Social- and selfperception of designers' professional identity, Journal of Engineering Design, 31:2, 100-126.

Kamila Kunrath, Philip Cash & Maaike Kleinsmann (2020B) Designers' professional identity: personal attributes and design skills, Journal of Engineering Design, 31:6, 297-330.

Jussi Lahtinen, Tuomas Kuismin, Keijo Heljanko (2015). Verifying large modular systems using iterative abstraction refinement, Reliability Engineering and System Safety, 139, 120–130.

Sang Hun Lee, Hee Eun Kim, Kwang Seop Son, Sung Min Shin, Seung Jun Lee, Hyun Gook Kang (2015). Reliability modeling of safety-critical network communication in a digitalized nuclear power plant, Reliability Engineering and System Safety, 144, 285–295.

Nancy G. Leveson, Peter R. Harvey (1983). Analyzing Software Safety, IEEE Transactions on Software Engineering, SE-9, 5, 569-579.

Igor Linkov, Daniel A. Eisenberg, Matthew E. Bates, Derek Chang, Matteo Convertino, Julia H. Allen, Stephen E. Flynn, Thomas P. Seager (2013). Measurable Resilience for Actionable Policy, Environmental Science & Technology, 47, 10108−10110.

Giorgio Locatelli, Mauro Mancini, Erika Romano (2014). Engineering to improve the governance in complex project environments, International Journal of Project Management, 32, 1395–1410.

Peter E.D. Love, Robert Lopez, David J. Edwards, Yang M. Goh (2012). Error begat error: Design error analysis and prevention in social infrastructure projects, Accident Analysis and Prevention, 48, 100– 110.

Junpeng Lv, Hai Hu, Kai-Yuan Cai, and Tsong Yueh Chen (2014).Adaptive and Random Partition Software Testing, IEEE Transactions on Systems, Man, And Cybernetics: Systems, 44:12.

Luigi Macchi, Elina Pietikäinen, Marja Liinasuo, Paula Savioja, Teemu Reiman, Mikael Wahlström, Ulf Kahlbom, Carl Rollenhagen (2013). Safety culture in design, NKS-278, Nordic nuclear safety research.

Madni AM, Sievers M. (2018). Modelbased 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.

Stephanie L. Morrow, G. Kenneth Koves, Valerie E. Barnes (2014). Exploring the relationship between safety culture and safety performance in U.S. nuclear power operations, Safety Science, 69, 37–47.

G. Motet (2009). Risks of faults intrinsic to software languages: Trade-off between design performance and application safety, Safety Science, 47, 873–883.

Raphael Moura, Michael Beer, Edoardo Patelli, John Lewis (2017). Learning from major accidents: Graphical representation and analysis of multi-attribute events to enhance risk communication, Safety Science, 99, 58–70.

Mika V. Mäntylä, Juha Itkonen, Joonas Iivonen (2012) Who tested my software? Testing as an organizationally cross-cutting activity, Software Qual J, 20:145–172.

Niklas Möller, Sven Ove Hansson, Jan-Erik Holmberg, Carl Rollenhagen (2018). Handbook of Safety Principles, First Edition. Edited by, John Wiley & Sons, Inc.

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

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

Mark O'Halloran, Jon G. Hall, Lucia Rapanotti (2017). Safety engineering with COTS components, Reliability Engineering and System Safety, 160, 54–66.

Giota Paparistodimou, Alex Duffy, Robert Ian Whitfield, Philip Knight, Malcolm Robb (2020) A network science-based assessment methodology for robust modular system architectures during early conceptual design, Journal of Engineering Design, 31:4, 179-218.

Raja Parasuraman, Thomas B. Sheridan (2000). A Model for Types and Levels of Human Interaction with Automation, IEEE Transactions on Systems, Man, And Cybernetics—Part A: Systems and Humans, Vol. 30, No. 3, May.

H.J. Pasman, B. Knegtering, W.J. Rogers (2013). A holistic approach to control process safety risks: Possible ways forward, Reliability Engineering and System Safety, 117, 21–29.

Alberto Pasquini, Simone Pozzi, Luca Save (2011) A critical view of severity classification in risk assessment methods, Reliability Engineering and System Safety, 96, 53–63.

Riccardo Patriarca, Johan Bergström, Giulio Di Gravio, Francesco Costantino (2018). Resilience engineering: Current status of the research and future challenges, Safety Science, 102, 79–100

Patterson, S., and Clarkson, G. (2015). First of a kind engineering in digital I&C projects. NPIC and HMIT 2015, Charlotte NC.

Payam Pirzadeh, Helen Lingard, Nick Blismas (2020). Effective communication in the context of safe design decision making, Safety Science, 131, 104913.

Michael Power (2007). Organized uncertainty; designing a world of risk management, Oxford University Press.

A. J. Rae , D. J. Provan , D. E. Weber and S. W. A. Dekker (2018). Safety clutter: the accumulation and persistence of 'safety' work that does not contribute to operational safety, Policy and Practice in Health and Safety, 16:2, 194–211.

Raz AK, Kenley CR, DeLaurentis DA (2018). System architecting and design space characterization, System Engineering, 21:227–242.

Jens Rasmussen (1985). The role of hierarchical knowledge representation in decision making and system management, IEEE Transactions on Systems, Man, and Cybernetics, SMC-15, NO. 2, 234-243.

Eugen Rigger, Thomas Vosgien, Kristina Shea & Tino Stankovic (2020). A top-down method for the derivation of metrics for the assessment of design automation potential, Journal of Engineering Design, 31:2, 69-99.

Emilie M. Roth, Amy R. Pritchett (2018). Preface to the Special Issue on Advancing Models of Human–Automation Interaction, Journal of Cognitive Engineering and Decision Making, Vol.12, No.1, pp. 3–6.

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 Manage. 29, 647–660.

Neeraj Sangal, Ev Jordan, Vineet Sinha, Daniel Jackson (2005). Using Dependency Models to Manage Complex Software Architecture, OOPSLA'05, October 16–20, 2005, San Diego, California, USA.

T.V. Santosh, A. Srivastava, V.V.S. Sanyasi Rao, A.K. Ghosh, H.S. Kushwaha (2009). Diagnostic system for identification of accident scenarios in nuclear power plants using artificial neural networks, Reliability Engineering an dSystem Safety, 94, 759–762.

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

T. B. Sheridan (2000). Function allocation: algorithm, alchemy or apostasy? Int. J. Human-Computer Studies, 52, 203-216.

Kostas Stylidis, Casper Wickman & Rikard Söderberg (2020) Perceived quality of products: a framework and attributes ranking method, Journal of Engineering Design, 31:1, 37-67.

S.I. Tay, T.C. Lee, N.A. A. Hamid, A.N.A. Ahmad (2018). An Overview of Industry 4.0: Definition, Components, and Government Initiatives, Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 14-Special Issue.

Taylor JR. (2007A). Statistics of design errors in the process industries. Safety Science, 45, 61–73.

J. Robert Taylor (2007B). Understanding and combating design error in process plant design, Safety Science, 45, 75–105.

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.

Anna-Maria Teperi, Nadezhda Gotcheva (Eds. 2020). Human Factors in the Nuclear Industry; A Systemic Approach to Safety, Elsevier.

Payuna Uday, Karen Marais (2015). Designing Resilient Systems-of-Systems: A Survey of Metrics, Methods, and Challenges, Systems Engineering, Vol. 18, No. 5.

Darian Unger & Steven Eppinger (2011). Improving product development process design: a method for managing information flows, risks, and iterations, Journal of Engineering Design, 22:10, 689-699.

Wahlström Björn, Lahti Jaakko, Timonen Juhani (1979). Interactive programs, software reliability and other problems related to man and software interface,IFAC SoCoCo, Prague.

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 (1994). Models, modelling and modellers; an application to risk analysis, European Journal of Operations Research (EJOR), Vol.75, Issue 2.

Björn Wahlström, Jari Kettunen, Teemu Reiman,Bernhard Wilpert, Hans Maimer, Juliane Jung,Sue Cox, Bethan Jones, Rosario Sola, José M.Prieto, Rosario Martinez Arias & Carl Rollenhagen (2005). LearnSafe: Learning organisations for nuclear safety, VTT Tiedotteita – Research Notes 2287.

Wahlström, B., 2007. Reflections on regulatory oversight of nuclear power plants. Int. J. Nucl. Law 1 (4), 344–377.

Wahlström, B., 2015. Differences between analogue and digital I&C, NPIC & HMIT 2015, Charlotte NC.

Björn Wahlström (2018). Safety Automation, in Handbook of Safety Principles, First Edition. Edited by Niklas Möller, Sven Ove Hansson, Jan-Erik Holmberg, and Carl Rollenhagen, John Wiley & Sons, Inc.

Björn Wahlström (2020). Human factors in nuclear power; reflections on 50 years of development in Finland, in Teperi, Gotcheva (2020). Human Factors in the Nuclear Industry; A Systemic Approach to Safety.

David D. Woods (2018). The theory of graceful extensibility: basic rules that govern adaptive systems, Environment Systems and Decisions, 38, 433–457.

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

Marja Ylönen, Tapio Litmanen (2015). Signaled and Silenced Aspects of Nuclear Safety: A Critical Evaluation of International Nuclear Safety Thinking, Risk, Hazards & Crisis in Public Policy, 6: 1.

Wei Zhang, Hong Mei, Haiyan Zhao (2006). Feature-driven requirement dependency analysis and high-level software design, Requirements Eng (2006) 11: 205–220. DOI 10.1007/s00766-006-0033-x