European Commission

JRC TECHNICAL REPORTS

Operating experience with digital I&C systems at nuclear power plants

A summary report from the European Clearinghouse

Miguel Peinador

2019

Joint Research Centre

EUR 29618 EN

This publication is a Science for Policy report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication.

Contact information
Name: Miguel PEINADOR VEIRA
Address: Westerduinweg 3, PO Box, 1755 ZG Petten – The Netherlands
Email: Miguel.PEINADOR-VEIRA@ec.europa.eu
Tel.: +31 (0)224 56 5176

EU Science Hub
https://ec.europa.eu/jrc

JRC114977

EUR 29618 EN

PDF ISBN 978-92-79-98751-9 ISSN 1831-9424 doi:10.2760/10611

Luxembourg: Publications Office of the European Union, 2019

How to cite this report: M. Peinador, *Operating experience with digital I&C systems at nuclear power plants. A summary report from European Clearinghouse*, EUR 29618 EN, Publications Office of the European Union, Luxemburg, 2019, ISBN 978-92-79-98751-9, doi:10.2760/10611, JRC114977.

Contents

Abstract

This study presents the results of a review of available recent international operating experience reported by nuclear power plants regarding digital I&C systems. Event reports retrieved from IAEA and US NRC databases are characterised and used to derive insights and lessons learned.

Foreword

The European Network on Operating Experience Feedback (OEF) for Nuclear Power Plants, hereafter referred to as European Clearinghouse on OEF, was established in 2008 by group of European Nuclear Safety Regulators and institutions for promoting collaboration on OEF, dissemination of the lessons learned from NPP operating experience and understanding the role of operating experience feedback systems in safe and economic operation of existing, as well as new build NPPs and promotion of advanced event assessment approaches and methods.

Currently eighteen European nuclear safety regulatory authorities (Finland, Hungary, The Netherlands, Lithuania, Romania, Slovenia, Switzerland, Belgium, Bulgaria, Czech Republic, France, Germany, Slovak Republic, Sweden, Spain, UK, Ukraine and Poland) and three European Technical Support Organizations (TSOs, from Belgium, France and Germany) are represented.

The main objectives of the European Clearinghouse on OEF are to:

— Contribute to the improvement of the OEF in European NPPs through strengthening and sharing the competences in OEF, as well as improving communication and co-operation inside the CH network and with the international OEF community. Specifically cooperation between licensees, regulatory authorities and TSOs in order to collect, communicate and evaluate information on reactor operating events and systematically and consistently apply the lessons learned in all the members' countries;

— Establish European best practice for assessing NPP operating events, through the use of state-of-the art methods, computer aided assessment tools and information gathered from various national and international sources, e.g. EU national regulatory authorities' event reporting systems and the International Reporting System for Operating Experience jointly operated by the IAEA and OECD-NEA;

— Provide staff to coordinate the OEF activities of the European Clearinghouse and maintain effective communication between experts from European regulatory authorities and their TSOs involved in OEF analyses; and

— Support the long-term EU policy needs on OEF by harnessing JRC and European TSO research competencies on the methods and techniques of nuclear events evaluation.

The office of the European Clearinghouse is operated by the Joint Research Centre of the European Commission. The European Clearinghouse regularly carries out in-depth analyses of events related to a particular topic (the so-called "topical studies") in order to identify main recurring causes, contributing factors and to disseminate the lessons learned aiming at reducing the recurrence of similar events in the future.

Acknowledgements

The author would like to thank A. Ballesteros, G. Manna, Z. Simic and M. Strucic for their feedback and contributions to this report.

1 Introduction

A topical study on events related to NPP's digital instrumentation and control systems was published by the EU Clearinghouse in 2013 [1]. Given the fast developments in this domain and the interest of the international nuclear safety community, as expressed by the OECD / NEA Working Group on Operating Experience, the Clearinghouse office was instructed to review the events reported in the years after the publication of the study. This note presents the results of such an update.

In general, digital I&C systems are characterised by using a sequential sampling of input data, as compared to the continuous flow of data of analogue technologies. Digital I&C equipment takes up much less physical volume than their analogue counterparts and require much less cabling. Some of the main advantages of digital systems are that they are less susceptible to measurement drift, they allow for more flexibility in the configuration of operation parameters and they provide enhanced self-diagnostics and monitoring capabilities. On the other hand, digital systems are typically more difficult to be verified and validated, and software may introduce common cause failure modes potentially defeating the defence in depth provisions of the plant design. Furthermore, digital systems require the staff of the plant to develop new skills, often very different from those required for the analogue components.

The **purpose** of this report is to review the events reported by the NPPs around the world to highlight the problems which have been actually encountered in recent years, to derive the lessons learned and the corrective actions than can be implemented to prevent recurrence; and, eventually, to formulate the recommendations for regulatory bodies and policy makers that could help to ensure a safe adoption of the digital technology by the nuclear industry.

2 Regulatory context

The introduction of software and computer based equipment in the nuclear industry, and particularly the challenges associated to the licensing aspects, has attracted the attention of national regulatory bodies as well as of international organisations, such as the European Commission, the IAEA and the OECD/NEA.

In the period 1995-2000, a task force of experts from European nuclear safety institutes sponsored by the European Commission was given the mandate of ”reaching a consensus among its members on a number of software licensing issues which have important practical aspects”, leading to the publication of a common position in 2000 [2], which was subsequently updated. Later, at the request of WENRA, a new report was published in 2007 based on the previous work, and revised up to its latest version in 2018 [3]. This latest version represents a common position endorsed by the regulatory bodies or technical support organisations from the group of participating countries, including Belgium, Finland, Germany, Spain, Sweden and the UK (in Europe) as well as Canada, China and South Korea. Furthermore, the US NRC participated to some extent to this effort, providing input and publishing one version of the report under the NUREG/IA series.

The common position [3] reviews a number of important licensing issues, comparing different licensing approaches and establishing where possible a consensus on requirements and recommended practices.

The IAEA's specific safety requirements SSR-2/1 [4] contain a number of requirements on instrumentation and control systems (req. #59 through #67), one of which (req. #63) addresses specifically the use of computer based equipment in systems important to safety. Furthermore, the IAEA provides guidance in complying with these requirements through the specific safety guide SSG-39 [5], currently in its 2016 version. This guide covers both analogue and digital I&C systems including software, with some sections specifically dedicated to the latter.

In addition to the safety requirements and associated guidance, the IAEA has also published various technical reports covering digital I&C themes. One of them [6] reviews different challenges faced by the nuclear industry in the transition from analogue to digital technologies, providing an excellent overview of the regulatory concerns linked to it.

More specifically, this IAEA report discusses the following 17 issues: (1) self-diagnostics (as compared to surveillance testing); (2) independent verification and validation; (3) management of the functional requirements specification; (4) configuration management; (5) common cause failures (particularly software CCFs); (6) use of smart devices (sensors and actuators including software-based technologies); (7) safety classification (lack of internationally harmonised approaches); (8) computer security; (9) harmonisation of standards; (10) online condition monitoring; (11) environmental qualification (particularly electromagnetic interference effects); (12) impact of hardware description language programmable devices (application specific integrated circuits, complex programmable logic devices and field programmable gate arrays); (13) digital communications (how to prevent that data exchange between redundant channels or safety and non-safety systems defeats the defence-in-depth approach); (14) safety classification of soft controls; (15) formal methods of software development; (16) use of wireless technology; and (17) the treatment of digital I&C in probabilistic safety assessments.

For its part, the OECD/NEA has recently established a working group on digital I&C (WGDIC), which builds on the previous work developed by the MDEP Digital Instrumentation and Controls Working Group (DICWG) from 2008 to 2017. The participating countries (Canada, China, Finland, France, India, Japan, South Korea, Russia, South Africa, the U.A.E., the UK and the US) reached during this

period a total of 13 common positions covering various topics, which are publicly available[1].

[1] http://www.oecd-nea.org/nsd/cnra/wgdic.html

3 Scope

3.1 Digital I&C systems

Only events related to digital I&C systems have been reviewed for this study. Although there is no universally accepted definition of a sharp line separating digital from analogue systems (as often I&C systems contain both digital and analogue components combined), as far as this study is concerned, an I&C system has been considered as digital if it is computer based or if it is mainly composed of components programmed with hardware description languages. Furthermore, any event where software has a role to play has also been included in the scope of the study.

3.2 Operating experience databases

Two major databases were used in order to obtain information about events related to digital I&C systems: IAEA IRS and the US NRC LERs. A brief description of each of them follows.

Table 1. List of operating experience databases reviewed

Database	Access	Advantages	Limitations
IAEA/OECD IRS	Restricted	• Worldwide coverage. • Events of interest for the international community	Inconsistencies in reporting criteria across different countries.
U.S. NRC LERs	Open	Complete and consistent source for all US NPPs.	Limited searching capabilities.

3.2.1 IAEA / OECD IRS database

The International Reporting System for Operating Experience (IRS) is jointly operated by the International Atomic Energy Agency (IAEA) and the Nuclear Energy Agency (NEA) of the Organization for Economic Cooperation and Development (OECD). The IRS is established as a simple and efficient system to exchange important lessons learned from operating experience gained in nuclear power plants of the IAEA and NEA Member States.

The fundamental objective of the IRS is to contribute to improve the worldwide safe operation of commercial nuclear power plants (NPPs). The IRS is collecting detailed information on both technical and human factors related to events of safety significance.

The IRS database contains about 4,000 event reports with detailed descriptions and analyses of the event's causes that may be relevant to other plants.

The database is accessible to authorised users through a web-based interface, created to facilitate data input and online access to reports. The IRS contains a well-defined and detailed classification system for events, with a set of codes. Events are searched by user-defined criteria composed of free keywords and characterisation codes, among other possible criteria available to the user.

3.2.2 US NRC LERs database

The US commercial nuclear reactor licensees are required to report certain type of events according to the US Nuclear Regulatory Commission (NRC) regulation 10CFR50.73. These reports are called "Licensee event report" (LER) and they are available to the public on the NRC's website. More than 50,000 reports are currently available starting from 1980.

The LER database is searchable using a variety of criteria, including name, dates, reactor type and vendor or free text search in the title, abstract and full report. However, LERs are stored without detailed characterisation (i.e.: failed system or component, type of event effects, related human factors, etc.).

3.3 Time period

Both databases have been searched for events dated from January 2013. The search was carried out in September 2018. It must be noted that events occurred in late 2017 or in 2018 might not yet be included in the databases at the time of the search, particularly in the IRS case.

4 Search criteria and screening

IRS events where the «FAILED/AFFECTED SYSTEM» data field contained at least one of the following codes were retrieved from the database:

3.I Instrumentation and control systems
3.I.2 Digital I&C systems
3.IA Plant/process computer (including main and auxiliary components)
3.IB Fire detection
3.IC Environment monitoring
3.ID Turbine generator instrumentation and control
3.IE Plant & process monitoring (including the main and remote/supplementary control room equipment and various remote control functions)
3.IF In-core and ex-core neutron monitoring (including BWR reactor stability monitoring)
3.IG Leak monitoring (reactor coolant boundary, containment and auxiliary buildings)
3.IH Radiation monitoring
3.IH.1 Plant radiation monitoring
3.IH.2 Personnel monitoring (dosimetry & contamination detection)
3.IK Reactor power control (e.g.: control rods & boration/dilution systems)
3.IL Recirculation flow control (BWR)
3.IM Feedwater control
3.IN Reactor protection
3.IP Engineered safety features actuation (including emergency systems actuation)
3.IQ Non-nuclear instrumentation
3.IR Meteorological instrumentation
3.IS Seismic instrumentation
3.IT Vibration monitoring

Furthermore, IRS events where the «FAILED/AFFECTED COMPONENT» contained at least one of the following codes were added to the list of potentially relevant events:

4.4 Computers
4.4.1 Computer hardware
4.4.2 Computer software

Finally, the IRS database was searched for all events containing the words «digital» or «software» in their abstracts.

Regarding the US LER database, as the search using codes is not possible for the relevant data fields (system/component affected), events containing the words «digital» or «software» in their titles or abstracts were retrieved.

5 Review of the events

After consolidation (some events were reported to both databases), the search of both databases led to a list of 82 events (52 from IRS, 29 from LER and 1 event reported to both databases). All these reports were reviewed to screen out those which could not be considered within the scope of the study, as described in section 2.1. The final result of the process after the screening is the list of 25 event reports presented in Appendix 8.1.

5.1 Characterisation of the events

In order to provide a quick insight into the 25 events selected for in-depth analysis, the following tables present their classification according to the digital I&C system affected (using the IRS coding system) and according to the digital I&C system life cycle phase (requirement specification, design, verification & validation, implementation / integration / installation, operation / maintenance and modifications). For the sake of consistency with the previous topical study, similar categories were used (only categories with at least one event are included in the table).

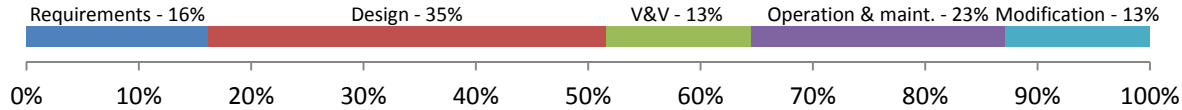
Table 2. Distribution of events per digital I&C system affected

Digital I&C system	IRS	LER	Observations
Turbine generator instrumentation and control	3	5	
Plant/process computer	5	-	
Feedwater control	1	4	
Leak monitoring	-	1	
Engineered safety features actuation	1	1	
Other	3	1	Mostly related to digital control of auxiliary systems other than TG and FW
Total	*13*	*12*	

As shown by the table, a large proportion of the events reported concern non-safety systems, notably the digital electro-hydraulic control systems of the turbine generator and the digital control of feedwater systems. Although not required to reach the safe shutdown of the reactor, the correct operation of these balance-of-plant systems is critical from the point of view of the plant availability. For this reason, they are usually designed according to very demanding quality and reliability requirements, meaning that lessons derived from these events are in principle useful as well for safety systems.

In the case of the reports related to plant and process computers, three of them affected the overall plant digital control system (plants recently commissioned, with a high degree of digitisation of I&C systems, including safety functions) while the other two impacted the operation of more conventional auxiliary computers, not directly linked to real time plant process.

Figure 1. Distribution of events per life cycle phase



The categories used for the distribution of the events per life cycle phase of the digital system were the same as in the previous study: requirements specification, design, verification and validation (V&V), operation & maintenance and modifications phase. The phase «implementation, integration, and installation», which had been used for the

topical study, has been merged here with the V&V phase, the reason being the difficulties in making the difference between the two from the information provided in the event reports.

As shown by Figure 1, events reported span across the entire life cycle, with the design phase taking approximately 1/3 of the events and the other 2/3 evenly shared by the other phases.

5.2 Insights from the review of events

Following the outlined methodology, and further to the characterisation of the event reports according to the system affected or the life cycle phase involved, the events were also compared to the digital I&C technical challenges as presented in the technical report from the IAEA.

Three particular topics turned out to be reflected in a significant number of events and deserve to be highlighted here: the use of smart devices (5 reports), the configuration management (4 reports) and digital communications (3 reports). The following subsections outline these events and the common themes underlying them.

5.2.1 Use of smart devices

The term «smart device» is commonly used to refer to sensors and actuators containing computer based technology, usually microprocessors with firmware or embedded software. In addition to the traditional sensing/acting functions, smart devices perform also calculations and provide communication functions.

Smart devices have displaced the traditional analogue sensors and actuators from the market, and the latter are increasingly difficult to obtain. However, the qualification of smart devices for a particular application in a nuclear power plant may require independent access to the source code of the embedded software from the vendor. As the nuclear industry is small compared to the size of the market served by smart devices vendors, the lack of incentives of the latter to disclose proprietary information makes difficult for the licensee to ensure adequate verification and validation. Sometimes it is difficult for the licensee even to identify that embedded software is present in equipment supplied as a package.

An additional challenge is that, because they are very flexible supporting different configurations, smart devices may be used for many different applications across the plant. This fact introduces two new issues:

— The common cause failure mode of the software embedded in the same smart device model may now affect a large number of components/systems

— For the sake of flexibility, a smart device model may contain many software functions that are not actually needed for a given application. These inactive functions could interfere however with the required ones, if the device is not configured properly, or if the software contains an error.

One of the event reports describes the case where a licensee discovered in 2014 that a certain type of relay used in the automatic start of the emergency diesel generators contained embedded software (a microprocessor controlled the coils of the relays). These relays had been installed a few years earlier, and therefore, the common cause failure mode of the embedded software had not been taken into account. This event is an example of inadequate qualification of a smart device for a safety-related application (malfunction of the relays would have disabled the automatic start of the emergency diesel generators).

The other four events related to this topic concern only non-safety related applications.

In the first one, the smart device involved was the automatic voltage regulator used for the control of the main generator. The root cause of the event was that this component

had not been sufficiently validated by site personnel. More specifically, an independent failure analysis of the new equipment by the licensee had not been possible because the proprietary information required was not readily available, and the simulator provided by the vendor was not able to replicate actual conditions of the plant. The failure resulted in a generator trip followed by a reactor scram.

In the second event, an unnecessary turbine trip (followed by a reactor trip) was caused by the failure of a power supply module on a circuit board in the digital electro-hydraulic turbine control system. However the trip would have never progressed if unnecessary trip logic associated with turbine overspeed monitoring had not been present in the turbine control system.

In another case, when operators of a BWR were preparing to transition from motor-driven feedwater pump to turbine-driven feedwater pump as part of the plant power ascension after an outage (the reactor was already in mode 1 at 18% of full power), the feedwater flow started to fluctuate, leading to reactor vessel water level swings of growing amplitude, and the operators proceeded with a manual reactor scram. Software errors in the digital feedwater module were the immediate cause of the event. The root cause was that the software embedded in the digital feedwater control contained parameters that were not identified, evaluated and mitigated in the corresponding engineering change package. As a corrective action, the plant has given mandate that any engineering judgements and unverified assumptions encapsulated within vendor provided software be clearly identified and independently validated prior to modification completion.

The last event involved the loss of the Instrument Air system, later leading to a manual reactor trip and a safety injection signal. The plant had one electric-driven compressor operating normally, with two additional diesel-driven compressors available in standby. During a routine round, an operator inadvertently pushed the load/unload button in the operating compressor digital control display (he was trying to get the screen to a different mode, and direct sunlight made difficult to see it). The standby compressors started but did not load. The reason was that a cooling fan permissive in the PLC coding (not required in standby mode) left the compressors in a non-responsive state. The vendor supplied compressor software had not been subject to a detailed technical review by plant staff.

5.2.2 Configuration management

Configuration management is a quality assurance issue applicable to all components, and not specifically to digital I&C systems. However, in the case of digital I&C systems, the number of software and hardware items, as well as the number of associated documents supporting those items, is particularly high. Furthermore, software is typically subject to a very high number of modifications before and after commissioning, which makes the topic particularly relevant in this case.

A weak or superficial configuration management process is often the underlying cause of many difficulties found during software modifications or digital I&C upgrades.

Four events can be linked to configuration management problems. Two of them involved the digital control of the turbogenerator and the other two caused malfunctions on the feedwater system. In all cases, modifications in these systems were not properly documented, or the impact on the plant behaviour was not properly understood. No safety system was affected in these cases, and the consequences were limited to a reactor trip.

5.2.3 Digital communications

Digital I&C systems provide the ability to exchange large amounts of data between different systems. Contrary to analogue point to point connections, digital communication technology typically uses networks, with a single connection passing multiple signals.

This creates new failure modes where faults may propagate through connected systems, or the failure of the connection itself can cause multiple faults in different systems.

There are many valid reasons for safety systems to share data with non safety systems, or for different safety channels to share data between themselves. Therefore the design needs to carefully prevent the possible propagation of failures through communication networks to ensure real independence between redundant channels and between safety and non safety systems.

Two very similar events were reported in 2014 by reactors featuring modern digital platforms for the control of safety systems. In both cases the operator stations and large screens at main control room of the computer information and control system went suddenly blank and control was manually transferred to the backup panel for about half an hour (the time to reboot the central data processing server). In one case the reactor was operating at full power, in the other case it was at hot shutdown. Both events were attributed to excessive CPU load created by synchronisation of large data sets from an auxiliary server used to process historical data.

Another example of issues with digital communications was experienced by a plant which had commissioned a new digital electrohydraulic control system for the main turbine in 2010. This is not a safety system; however it had been designed to prevent single failures from causing turbine trips, because of availability considerations. The system was thoroughly tested during its commissioning, including the capability of the standby CPU to take over from the online CPU in case of failure of the latter. Even so, after one year of normal system operation, the standby unit was unable to take over from the operating one after some intermittent communication losses between the two CPUs, leading to a turbine trip. The original vendor improved the system's architecture to solve the issue, however several years later a single failure in a communication hub progressed immediately to a turbine and reactor trips. The CPU in operation had not recognised the failure in the hub, so the automatic switchover to the redundant CPU (not affected by the communications hub failure) never took place, thus defeating the redundancy of both channels.

6 Lessons learned

The following lessons can be derived from the review of recent operating experience with digital I&C systems in power reactors.

Box 1. Review of embedded software.
Assumptions and engineering judgments used to develop software embedded in digital I&C components should be clearly identified, and then verified by staff familiar with plant design and operation, independently from the component vendor.

It has been observed that sometimes the licensees rely excessively on the expertise from vendors of digital I&C components to understand and review the software embedded in such components (digital relays, PLCs, microprocessors ...). Often, the information required for an independent verification is proprietary and is not readily available to plant staff. As software developers might not be fully familiar with plant process parameters and behaviour, there is a risk that a misunderstanding about the actual values taken by a plant parameter under certain circumstances will result in a software error. In most cases, these errors will be detected during the component V&V, but if the error is associated to very specific and infrequent plant configurations, it could slip through the V&V process. The verification of the embedded software by staff familiar with the plant processes should include function blocks, mathematical calculations and modelled plant behaviour.

Whenever this verification has been overlooked, the failure of the digital I&C component has led to a wide variety of effects on plant operation, as these components are more and more widely used across nuclear plants. Typical examples include feedwater flow perturbations (leading to reactor trips), spurious activation of generator protections or the loss of instrument air. In one case, embedded software had been used for digital relays being part of the diesel generator control system, without the licensee being aware of it.

Box 2. Common cause failures in software.
When digital I&C systems are required to be single failure proof, the actual fulfilment of this requirement should be carefully reviewed, verified and validated.

Operating experience shows that some digital I&C systems designed to be resistant to single failures contain hidden, unanalysed failure modes challenging the independence of redundant chains. This has been experienced particularly in the case of systems including network communication components.

Digital systems resistant to single failures often feature two independent processing units, each receiving input from different sources. One of the units is online while the other is in standby to take over if the operating unit fails. However some cases have been reported where the switchover failed because the original fault was not recognised as such by the operating processor.

Box 3. Interactions between safety and auxiliary functions of software.
The design of safety related digital I&C systems containing software should be such that auxiliary functions performed by the system do not interfere with the safety function.

The practice of reusing software modules previously developed for other applications is commonly used by software developers. This poses a risk of introducing unnecessary functionalities that, under certain circumstances, might lead to software errors. Similar risks appear when the same hardware (like a server) is used to run safety related applications together with other secondary tasks.

Plants equipped with fully digital plant control systems experienced disruptions on its computer operator stations because the main server was overloaded with data

synchronisation requested by an auxiliary server used for historical data processing and filing. The hardware performance of the main server was insufficient to handle the data load and was shutdown.

Box 4. Optical fibre technology.
Installation and maintenance of optical fibre technology should be done according to detailed specific procedures and after following adequate training.

Optical fibre connectors are susceptible to failure caused by dirt and other failure modes linked to the inadequate layout of the optical fibre cables.

In one case, the presence of dirt at an optical fibre connector disturbed the exchange of data between a module located at the switchyard and the main control room, generating a spurious load rejection signal that resulted in turbine and reactor trip. A modification of the system to make it resistant to single failures was planned, but not yet implemented.

Box 5. Impact of software modifications on procedures.
The modifications of digital I&C systems' operational procedures following software modifications should be validated.

Sometimes the modifications in the software of digital systems may appear to be minor, not requiring validation of the updated procedures. However subtle interactions between different parameters may lead to unexpected results.

In one NPP with two reactor units, a modification in the digital electrohydraulic control of the turbine had been carried out in one of the units, in order to improve the regulation of the reactor pressure during start-up using the main steam bypass valves. The corresponding operational procedure was updated and validated. However, when the same modification was implemented one year later in the other reactor unit, it was judged that the procedure update did not require a validation. Due to some minor operational differences between the two reactor units, in this case the procedure was incorrect, suddenly leading to the bypass valves to the fully open position and causing a reactor trip.

Box 6. Ergonomics of digital systems human-machine interfaces.
Special attention should be paid to ergonomic considerations of displays and touch screens used to control equipment important for safety.

The widespread use of digital displays, LCD screens, touch screens etc. in many different locations across the NPPs gives more and more importance to the ergonomics of these human-machine interfaces. Although rarely the root cause of a serious event on its own, the lack of contrast or sharpness in digital displays can increase the probability of operator error.

A case was reported where the operators inadvertently opened one of the main steam dump valves to the atmosphere while they were introducing commands through a local touch screen panel in the framework of a test procedure. A contributing factor to this human error was that it was difficult to distinguish the different colours used in the display to highlight the various menu options available, and that the room lighting created disturbing glares on the display.

7 Conclusions

The safety significance of the events reported by nuclear power plants worldwide in relation to digital I&C systems during the past five or six years is very low. It can be argued that computer-based systems are used mostly in non safety applications, thus explaining why the events reported did not compromise the safety of the plants. However the number of plants which have upgraded their I&C systems to fully digital platforms, together with the new builds now entering commercial operation (with digital safety systems as part of their original design) is gradually increasing. In these cases, systems like the reactor protection or emergency core cooling rely on computers. Particularly in the case of modernisation projects of existing plants, one could expect a high chance of experiencing safety significant events, if only because of the complexities of the modifications involved. However this does not seem to be the case, at least for the moment.

In the case of events related to the safety / security interface, again their number and safety relevance are very limited. However, it must be recognised that events having any aspect related to security are very unlikely to be reported to the databases used for this study, therefore making impossible any conclusion regarding the trend of this type of events.

Beyond the discussion on the safety significance of the events, the experience accumulated with the operation of non safety systems such as the electro-hydraulic control of the main turbine or the main feedwater control can offer valuable lessons for the design, operation and regulatory oversight of safety systems. This study has identified some of them, based on the review of 25 relevant events reported since 2013.

A recurrent theme underlying many of the events reviewed is that software developers on one hand and engineering staff familiar with the plant design and operation on the other hand not always find easy to understand each other and not always have access to the same information (with access to proprietary code being cited as an issue in some cases). This may lead the licensees to rely excessively on vendors for software verification and validation, particularly when software is embedded in isolated components. When this weakness is added to the inherent "sneaky" character of many software failure modes and to the complexities of software validation in a real operation environment, the chances for software defects to pass through all quality assurance barriers may be significant. The strict adherence to software development guidance remains one of the most important among these barriers.

- Vendors and licensees should ensure full and independent verification and validation of software embedded in safety-related components.
- Inspectors working for nuclear safety authorities should give high priority in their oversight tasks to make sure that licensees have robust policies in place to identify embedded software in safety-related applications, and that this software is subject to appropriate V&V processes.

Furthermore, nuclear safety authorities' management should periodically verify that current regulations correctly address the observed operating experience, as summarised, among many other sources, by this study.

Finally, it has been observed that most if not all lessons learned formulated in this report could be linked to topics widely discussed in the literature (albeit perhaps described in different words), and particularly to the previous topical study published in 2012. As is often the case, this review of operating experience did not bring new issues to the attention of the industry and safety authorities; however, it confirms the need to better use the available feedback, and appropriately manage the gained knowledge to avoid the recurrence of issues already known to the industry.

References

[1] Seménas, R., Kaijanen, M., *Nuclear power plants digital I&C systems-related events (topical operating experience report),* Joint Research Centre, European Commission, 2013.

[2] *Common position of European nuclear regulators for the licensing of safety critical software for nuclear reactors*, EUR 19265, European Commission's Advisory Experts Group, The Nuclear Regulators' Working Group, Task Force on Safety Critical Software, Directorate General for the Environment, European Commission, 2000.

[3] *Common position of international nuclear regulators and authorised technical support organisations,* Task Force on Safety Critical Software, Bel V – BfE – CNSC – CSN – ISTec – KAERI – KINS – NSC – ONR – SSM – STUK, 2018.

[4] *Safety of nuclear power plants: design,* IAEA Safety standards series No. SSR-2/1, IAEA, Vienna, 2016.

[5] *Design of instrumentation and control systems for nuclear power plants,* IAEA Safety standards series No. SSG-39, IAEA, Vienna, 2016.

[6] *Technical challenges in the application and licensing of digital instrumentation and control systems in nuclear power plants,* IAEA Nuclear energy series No. NP-T-1.13, IAEA, Vienna, 2015.

List of abbreviations and definitions

CH	European Clearinghouse
CPU	Central Processing Unit
I&C	Instrumentation and Control
IRS	International Reporting System or operating experience
JRC	Joint Research Centre
LCD	Liquid Crystal Display
LER	Licensee Event Report
MDEP	Multinational Design Evaluation Program
NEA	Nuclear Energy Agency
NPP	Nuclear Power Plant
NRC	US Nuclear Regulatory Commission
OECD	Organisation for Economic Co-operation and Development
OEF	Operating Experience Feedback
PLC	Programmable Logic Controller
TSO	Technical Support Organisation
V&V	Verification and Validation
WENRA	Western European Nuclear Regulators Association

Annexes

Annex 1: List of events

Source	Year	Title
NRC	2013	Software errors in new digital feedwater control system result in manual reactor scram due to approaching high reactor pressure vessel water level setpoint.
NRC	2013	Manual reactor scram due to loss of reactor feedwater pumps.
NRC	2013	Reactor trip due to generator trip during main generator reactive power testing.
IAEA/OECD	2013	Escalated malfunction risk in the safety classified relays.
NRC	2014	Condition prohibited by technical specifications due to an instrument tunnel sump level indication transmitter incompatible with the containment environment.
NRC	2014	Reactor scram during automatic voltage regulator channel transfer.
IAEA/OECD	2014	KIC operator station shortly unavailability.
IAEA/OECD	2014	The operator station of computer information and control system (KIC) is unavailable temporarily.
IAEA/OECD	2014	Operating experience regarding complications from a loss of instrument air.
IAEA/OECD	2014	Computer virus found on various plant laptops and media.
IAEA/OECD	2014	Unit scram on loss of power to one out of two operating RCPs due to short circuit in the 500 kV outdoor switchgear caused by human errors.
IAEA/OECD	2014	Short time unavailability of computer information and control system (KIC) operator station.
IAEA/OECD	2014	Reactor scram due to loss of signal status from 400 kV line to digital electrohydraulic control.
NRC	2015	Manual auxiliary feedwater system actuation.

Source	Year	Title
NRC	2015	Turbine driven auxiliary feedwater pump in a condition prohibited by technical specifications due to a design issue.
NRC	2015	Valid automatic actuation of the reactor protection system due to main steam bypass valves opening.
NRC	2015	Automatic reactor trip results from a turbine trip initiated from the digital electro-hydraulic control system.
NRC	2015	Reactor scram due to digital protective relay system lockout.
IAEA/OECD	2015	Improper flow accelerated corrosion model results in 4-inch steam line failure and manual reactor trip.
IAEA/OECD	2015	Reactor scram due to main turbine trip.
IAEA/OECD	2016	Violation of instruction requirements resulting in computer infection by virus.
IAEA/OECD	2016	Level fluctuation of steam generator caused by sudden close of feedwater flow control valve.
IAEA/OECD	2017	Personnel erroneous actions that led to opening the steam dump valve to the atmosphere.
NRC	2018	Manual unit trip on low steam generator level following trip of a turbine feedwater pump due to a design issue.
NRC	2018	Automatic reactor scram due to an unanticipated electro-hydraulic control logic condition.

Source: IAEA/OECD and NRC.

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

- at the following standard number: +32 22999696, or

- by electronic mail via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications
You can download or order free and priced EU publications from EU Bookshop at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

KJ-NA-29618-EN-N

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub

ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

doi:10.2760/10611

ISBN 978-92-79-98751-9