The Development of the New Idea Safety Guide for Design of Instrumentation and Control Systems for Nuclear Power Plants

Gary Johnson

Independent Consultant
Livermore, California
kg6un@alumni.calpoly.edu

Alexander Duchac

International Atomic Energy Agency
Vienna, Austria
a.duchac@iaea.org

Abstract

The International Atomic Energy Agency (IAEA) is a United Nations organization that was formed to "accelerate and enlarge the contribution of nuclear energy to peace, health and prosperity throughout the world." The IAEA prepares Safety Standards in accordance with the IAEA. These Standards are not binding on Member States, but may be adopted by them. The Safety Standards are, however, binding for the IAEA's own activities (safety reviews, technical cooperation missions, training activities), on the IAEA, and on Member States. IAEA Safety Standards are organized into three levels: Safety Fundamentals, Safety Requirements, and Safety Guides. It is necessary to take the measures recommended. Currently nearly 120 safety guides are in effect. The article gives an extensive review of existing documents.

Key Words: Instrumentation and control, safety, nuclear power plants, standards

Background

The International Atomic Energy Agency (IAEA) is a United Nations organizations that was formed to, "accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world [1]." As of February 2016, one hundred and sixty eight nations were members of the IAEA.

The IAEA prepares Safety Standards in accordance with the IAEA Statute which mandates that the IAEA "establishes or adopts… [in consultation with…] standards of safety for the protection of health and minimization of danger to life and property, and provides for the application of these standards." These Standards are not binding on Member States but may be adopted by them. The Safety Standards are, however, binding for the IAEA's own activities (safety reviews, technical cooperation missions, training activities), on Member States in relations to operations assisted by the IAEA, and on Member States wishing to enter into project agreements with the IAEA.

As illustrated in figure 1, IAEA Safety Standards are organized into three levels: Safety Fundamentals, Safety Requirements, and Safety Guides. The Safety Fundamentals are given in one document that establishes the fundamental safety objective and principles of protection and safety for nuclear facilities and activities. Safety Requirements establish an integrated and consistent set

the requirements that must be met to ensure the protection of people and the environment, both now and in the future. At this moment these documents describe member state consensus for the implementation of the Safety Fundamentals in fourteen topic areas. Safety Guides provide recommendations and guidance on how to comply with the Safety Requirements. Safety Guides present international good practices to help users striving to achieve high levels of safety. The guides represent member state consensus that it is necessary to take the measures recommended, or equivalent alternative measures. Currently nearly 120 safety guides are in effect.

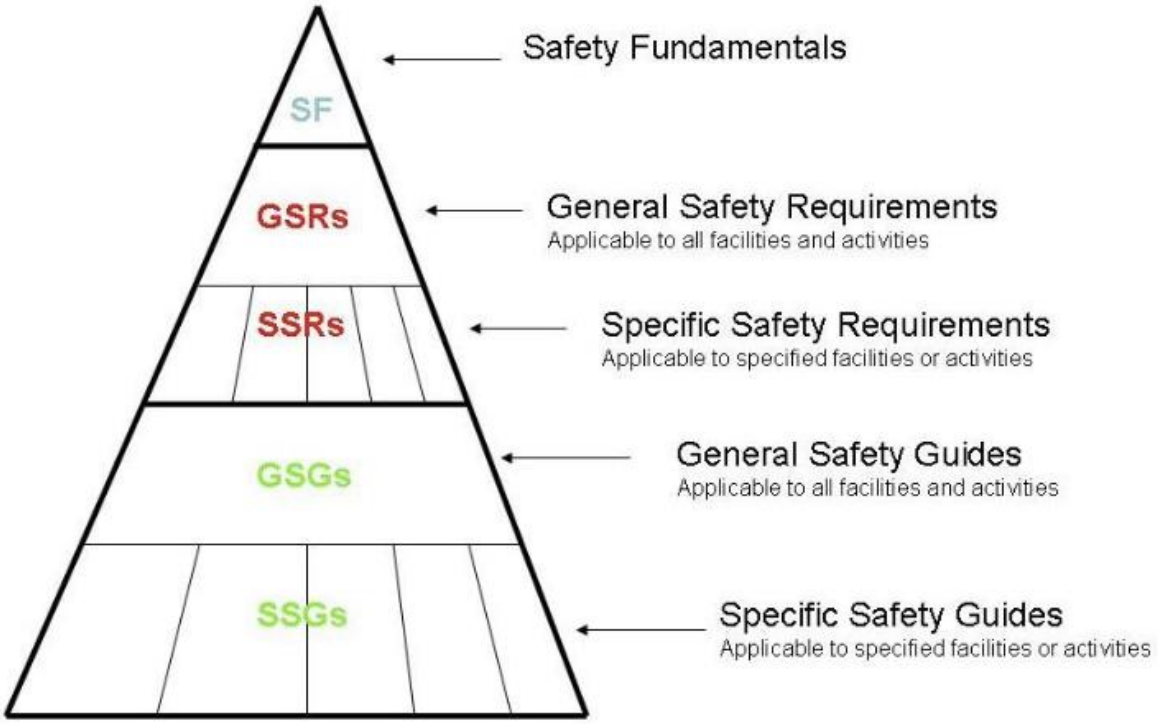

Figure 1. The hierarchy of IAEA Safety Standards[2]

In 2009 the IAEA undertook work to update and replace two existing safety guides that dealt with Instrumentation and Control for Nuclear Power Plants. These guides were:

NS-G-1.3 [2] which provided recommendations regarding the implementation of IAEA requirements for Instrumentation and Control (I&C) Systems, and
NS-G-1.1 [3], which provided detailed guidance on the development of software for I&C systems important to safety.

In 2009 NS-G-1.1 was nine years old and NS-G-1.3 seven. Since the publication of these two standards there had been many developments in the I&C domain. These developments involved both technical advances and advances in the criteria provided by non-governmental standards development organizations.

IAEA published a new I&C standard, SSG-39 [4], in 2016 to replace NS-G-1.3 and NS-G-1.1.

[2] From: Long Term Structure of The IAEA Safety Standards and Current Status (2016).
Electronic version available at: https://www-ns.iaea.org/committees/files/CSS/205/status.pdf

Merger of the Two Safety Guides

In updating these, I&C safety guides one important question was should NS-G-1.1 and NS-G-1.3 each be updated or should the two standards be merged into one standard. Ultimately a number of considerations led to the decision to merge the documents. Some of the main reasons for the merger were:

Safety is a systems issue and it was felt that the segregation of guidance for I&C systems into two documents, one dealing with hardware and systems, and the other dealing with software, complicated discussion of the interactions of these topics.

Since the development of NS-G-1.1 many of the topics it covered had been addressed by standards prepared by international standards development organizations (SDO's), i.e., the International Electrotechnical Commission (IEC) and the Institute for Electrical and Electronic Engineers (IEEE). It was felt better not to duplicate the work of these bodies.

The SDOs were also rapidly expanding digital systems guidance to address new topics such as the use of field programmable gate arrays, the acceptance of industrial digital devices, and data communications. It would have been difficult for IAEA to revise a document such as NS-G-1.1 at a pace that could match the growing list of topics to be addressed.

Consequently it was decided that the IAEA guidance in the software area should focus on the elemental and basically static guidance for real-time software for nuclear power plants important to safety. Nevertheless, many points were carried over from NS-G-1.1. A concerted effort was made to extract fundamental recommendations into a specific software section in SSG-39. Also, much of the lifecycle guidance in NS-G-1.1 was recast as guidance for both software and hardware development in SSG-39.

Relationship to Non-Governmental Standards

Non-governmental standards such as those produced by IEC and IEEE respond to one of two basic sets of requirements those of the U.S. Nuclear Regulatory Commission, and those given in the IAEA Safety Requirements. Most countries have taken one of these sets of requirements as the starting point for developing their own regulations.

IAEA safety standards should not unnecessarily conflict with national requirements (otherwise the member states would not endorse them). By extension the IAEA standards should not unnecessarily conflict with the existing standards that support the two main sets of requirements as this could force unnecessary changes to existing standards. To avoid such conflicts it was necessary to conduct a deep technical review that involved representation from a broad range of experts from the international community. Section 6 discusses this review.

Overview of the Safety Guide

As with NS-G-1.3 and NS-G-1.1, SSG-39 gives guidance meant to ensure the suitability and reliability of nuclear power plant I&C systems. The document mainly provides recommendations for systems important to safety. A fundamental assumption behind the safety guide is that commercial industry is already highly proficient at developing I&C systems, but they may not be fully aware of specific methods that are employed to ensure that I&C systems provide the levels of safety and reliability required by the nuclear industry.

One view of the safety guide is that it describes a consensus set of design practices intended to ensure the reliability of I&C systems. The guide addresses reliability, not just in terms of failure rates and fault tolerant architecture, but from the fundamental requirement that I&C systems must have characteristics that ensure that safety functions can be performed with the necessary reliability. The main subjects covered and the motivation for discussing these subjects are described below.

The management system for I&C design

Management systems focus on all phases of the I&C development lifecycle to ensure that safety requirements (including reliability) are included in the design and continue to support their function during the entire life of the I&C system. Two fundamental mechanisms may contribute to system reliability: 1) component failures and 2) errors that result in failure of system functions even when all components are working normally. Design, operational, or maintenance errors can affect system reliability even if no component failures occur.

Design basis for I&C systems

The development of high reliability systems depends upon the availability of correct and complete design requirements that identify the overall I&C systems and each individual I&C system's necessary capability, functionality, and reliability. This section provides a guide to identifying such features.

I&C architecture

This section provides criteria that should be considered when developing I&C architectures. I&C architecture identifies the I&C functions that will be provided to support normal operations and the response to accidents. At the overall plant level the I&C architecture defines the systems that will be provided to support normal operations, control of abnormal operations, and response to accidents. At this level the architecture defines features needed to maintain independence between the I&C systems that support normal operations and the systems that:

Are intended to respond to abnormal plant operation including conditions:
Are intended to initiate mechanical systems that prevent fuel damage in the event serious failures in plant equipment
Are meant to control the consequence of common cause failures in the systems that respond to serious failures in plant equipment.

In all cases the failures considered include component failure, design errors, operational errors, and maintenance errors.

At the individual system level architecture describes the features to be provided to limit propagation of individual failures within the individual systems.

Safety classification

Economic and staffing limitations necessitate that the highest level of resources be provided for the development of I&C systems having the greatest safety importance. This section discusses the grouping of I&C safety functions and associated systems according to their importance to safety and the assignment of design requirements for each class.

Recommendations for I&C system design

This section describes methods that may be used to achieve the functional and reliability requirements established by the I&C design basis, architectural requirements, and safety classification. There are two sections dealing with this topic: one deals with generic recommendations that apply to all systems and the other deals with recommendations for specific types of systems. These two sections give guidance for reliability design to cope with single failures

as well as other features to ensure reliability is not jeopardized by conditions that may occur during the systems' lifetime. For example, as a result of exposure to harsh environments, unauthorized operation, measurement drift, and ageing.

Considerations relating to the human-machine interface

This section deals with characteristics that the human-machine interface should have to help operators make reliable operational decisions and to avoid making operational errors.

Software

Software does not fail, but software systems may be more prone to design errors than hardware. This section elaborates on the management system recommendations to present techniques and features intended to improve software reliability.

Correlation with other international instrumentation and control standards for nuclear power plants

Safety guides give only high level recommendations that are meant to ensure the functionality and reliability of I&C systems in nuclear power plants. Standards development organizations such as IEC and IEEE provide much more detailed recommendations that support the ideas in SSG-39. For that reason the guide has an annex that identifies the IEC and IEEE standards that have a strong relationship to each section of the safety guide. Some IEC and IEEE standards deal with even more detailed ideas that do not correlate directly to the safety guide. It is believed that the standards listed in the annex are sufficient to lead users to the more detailed recommendations.

Main Technical Differences From the Previous Safety Guides

In the 1990's the nuclear power plant I&C community adopted the concept of formal development lifecycles as a fundamental approach to ensure and demonstrate the quality of software development. The principles for the development of software lifecycles were described in documents such as IAEA NS-G-1.1, reports developed by various regulatory organizations, and international standards such as IEC 60880 [5] and IEEE 7-4.3.2 [6]. Since that time both the nuclear industry and other process industries have recognized that formal development lifecycles should play the same role for hardware systems as well, as evidenced by the development of IEC 61508 [7] for commercial products, and IEC 61513 [8] for nuclear power plant systems. To reflect these developments SSG-39 includes a full section describing the fundamental characteristics expected in the development of hardware systems and components, and both the hardware and software development for digital systems.

SSG-39 takes into account the continuing development of computer applications and the evolution of the methods necessary for their safe, secure and practical use. The document identifies two very important interfaces with I&C design: Human Factors Engineering and Cyber Security. When designing the I&C systems, it is necessary to coordinate with these two engineering domains and to integrate human factors engineering inputs and computer security inputs into I&C life cycles.

SSG-39 references the IAEA computer security guide, NSS-17 [9] and provides criteria for avoiding negative safety effects from computer security features. The intent of SSG-39 is to identify major interfaces with the computer security activities, and to give recommendations on I&C design features that affect these activities, e.g. interaction with cybersecurity programs in the overall I&C process planning, graded approach to security in the I&C system design, impact assessment for mal-operation of critical digital assets, incident response and periodic vulnerability assessment in individual system lifecycle phases. More detailed information on computer security is provided in NSS-17.

SSG-39 accounts for developments in human factors engineering and provides considerations on the interactions of I&C design with human factor engineering programs. The document contains specific clauses that identify major interfaces with the human factors activities, and gives recommendations on I&C design features that affect these topics, e.g. the human-machine interface in the design of the main and supplementary control rooms. Guidance is also given for user displays and controls.

Although SSG-39 covers certain aspects of human factors as they relate to I&C, it does not provide comprehensive guidance on this domain. The development of human factors engineering requirements and the verification and validation of human factors engineering activities are normally performed as part of a human factors engineering program. Currently, IAEA is developing a new dedicated Safety Guide on Human Factors Engineering (the working draft is numbered as DS492) that provides a set of specific recommendations on how to deal with human factor engineering in the design and operation of nuclear power plants. This standard will address:

- Considerations specific to human factors engineering, including the human machine interface(s) for achieving compliance with the requirements established in SSR 2/1, Rev.1 [10];
- Competences needed for integrating human factors engineering into the design of nuclear facilities throughout the plant lifecycle for achieving compliance with the requirements established in GSR-Part 2 [11] (Leadership and management for safety; published in 2016 as a revision of GS-R-3);
- The human factors engineering process to be considered in achieving human machine interface design across plant states.

Digital systems consist of both software and hardware. A certain amount of guidance on digital system hardware and hardware systems that needed to be recognized at a high level. Criteria that existed in NS-G-1.1 and other criteria developed after the publication of that standard were included in SSG-39 to cover topics that mainly involved system performance requirements, communications systems, and cyber security considerations.

When NS-G-1.1 was written most digital systems were being developed using general purpose microprocessors or programmable logic controllers. Since that time the industry has witnessed the use of other kinds of digital platforms such as systems programed using hardware description languages (e.g., field programmable gate arrays) and industrial digital devices having limited functionality, The selection and use of such devices raise issues that are different from the older technologies. Thus a discussion of high level principles for such systems were given.

SSG-39 is closely related to IAEA Safety Guide SSG-34 [12], Design of Electrical Power Systems for Nuclear Power Plants, which provides recommendations for power supply, cable systems, protection against electromagnetic interference, equipment and signal grounds, and other topics that are necessary for the satisfactory operation of I&C systems. With regard to I&C systems, SSG-34 gives recommendations on power supplies to ensure that requirements on their safety class, reliability provisions, qualification, isolation, testability, maintainability and indication of removal from service that are consistent with the reliability requirements of the I&C systems they serve. Wherever possible SSG-34 and SSG-39 give identical criteria for such topics.

Special recommendations are given to address electromagnetic interference, because power supplies can provide a transmission path for electromagnetic interference that might originate outside the I&C systems or might arise from other I&C systems that are connected directly or indirectly to the same power supply. Particular consideration is also given to ensuring the long term availability of the electrical systems that are necessary for the operation and monitoring of safety systems.

Coordination With Other Organizations

The development of SSG-39 was coordinated with three other international organizations concerned with standards for nuclear power plant I&C: The OECD/NEA Multi-national Design Evaluation Program (MDEP) Digital I&C Working Group (DI&CWG), the IEC Subcommittee for Instrumentation, Control, and Electrical Systems of Nuclear Facilities (IEC SC45A), and the IEEE Nuclear Power Engineering Committee (NPEC).

MDEP is a multinational initiative taken by national safety authorities to develop innovative approaches to leverage the resources and knowledge of the national regulatory authorities who will be tasked with the review of new reactor power plant designs. Within MDEP the DI&CWG works to document common positions in the DI&C safety systems design areas and harmonize and converge national codes, standards and regulatory requirements and practices in the area of digital I&C.

During the development of SSG-39 the DI&CWG was working actively in the areas of the treatment of common cause failure, qualification of software tools, verification and validation, communications independence, selection and configuration of hardware description language programmed devices, simplicity in design, selection and use of industrial digital devices, interaction between safety and cyber security, and safety criteria for I&C architecture. IAEA staff actively participated in the DI&CWG work and strove to achieve consistency between SSG-39 recommendations and the common positions of the DI&CWG regulators. The continued cross discussion between IAEA and MDEP resulted in the development of consistent approaches between the documents published by the two organizations.

The experts participating in the development of SSG-39 included members of the SC45A and NPEC standards development committees who had deep and broad understanding of each group's standards. Their participation was vital to avoiding unnecessary conflicts between SSG-39 and the two non-governmental standards organizations. The participants also took back to their organizations new ideas that may be incorporated into the SDO documents in the future. Furthermore, IAEA staff continually participated in SC45A and NPEC meetings to keep them informed of the status of the SSG-39 draft and the key technical issues under discussion.

Development and REview process

The core team that drafted the standard was made up of about 15 experts from Canada, Czech Republic, France, Korea, Russia, the United Kingdom, and the United States. The number 15 includes several people who could not participate in all meetings so the typical drafting meeting involved less than 10 participants.

Several drafting meetings were needed for the group to develop a draft that was considered to be sufficiently mature for industry wide review. This draft was sent directly to more than 100 known experts in twenty-two countries. The experts were offered the opportunity to make comments and were asked to share the draft with other experts who may also wish to comment. In addition IEC SC45A and IEEE NPEC were specifically asked to review the draft to identify any conflicts with their standards. In addition to these personal contacts the draft was distributed and comments were solicited from all IAEA member states via the announcement of a technical meeting to review the draft.

More than eleven hundred comments were received from thirty individuals or organizations representing about twenty nations or international institutions. The IAEA staff grouped the

comments and developed proposed dispositions. These proposed dispositions and residual comments were discussed at a technical meeting hosted by Electricity de France in Lyon during the week of 12 December 2011. Thirty experts from seventeen nations or international organizations attended. A large number of the comment dispositions were rapidly accepted but several hundred still needed to be discussed. Thanks to the hard work and determination of the experts and the excellent meeting arrangements the review was completed with only a small number of comments identified as needing further discussion. Of course, being in Lyon, the meeting was also a gastronomic success.

Establishment of the new IAEA safety standard required a comprehensive step-by-step preparation and review process which contains 14 steps and involves different review committees. In case of SSG-39, the main review committees were the Nuclear Safety Standard Committee (NUSSC), the Nuclear Security Guidance Group (NSGC) and Commission of Safety Standard (CSS). Each draft safety guide is reviewed internally before its submission to the review committee.
The first review of Draft G by the 34th NUSSC meeting during 19-21 November 2012 was unsuccessful; the draft was rejected due to prevailing disagreement among NUSSC representatives on the three topics such as reliability determination for digital systems, assessment of common cause vulnerabilities in safety systems, and criteria for implementation of diverse actuation systems. A compromise solution was found during an extraordinary consultancy meeting that was held in February 2013. It was decided to move these three topics into an informative Annex.

The review of a revised draft by the 35th NUSSC meeting was successful and the safety guide was sent to member states for their comments. After 8 months, which is a period given to member states to review draft safety guide, the IAEA received 386 comments from which 159 comments were accepted. The comment resolution was not easy, because several "critical" comments related to the effects of automatic control system failures ignited a new discussion among three influential NUSSC members. After several iteration cycles a common position was found and a new draft was provided to the 37th NUSSC meeting in June 2014, which eventually endorsed this draft for the final step – CSS endorsement.

As mentioned in section 4, the safety guide references the IAEA computer security guide, NSS-17 and provides criteria for avoiding negative safety effects from computer security features. With this regard the draft safety guide was also reviewed in a NSGC meeting in June 2014. Although it looked initially as an easy review, it turned to be a difficult step to obtain an approval by NSGC. The main reason for a long and heavy discussion in the group was that the NSGC group did not like quite many clauses on security interface arguing that sufficient security guidance is provided in the IAEA security series publications. It was explained that provisions for ensuring the security of digital safety systems need to be included in different stages of I&C design and the NSGC eventually endorsed this draft.

SSG-39 was established as the new safety guide by the 36th CSS meeting in November 2014; however at that time several IAEA requirements documents were under revision to address the lessons learned from the accidents at Fukushima Daiichi. It was decided not to release SSG-39 until after these requirements documents were approved. In the end this delayed publication by one and a half years and resulted in: bringing the terminology "Technical Support Centre" in line with that agreed for revision of SSR 2/1, and revised sections on accident monitoring and communications facilities which addressed the fundamental points concerning accident monitoring from IAEA publication NP-T-3.16 [13] on Accident Monitoring Systems for Nuclear Power Plants. After these changes were made, the document was finally published in May 2016

Conclusion

SSG-39 provides recommendations on the design of I&C systems to meet the requirements established in IAEA Safety Design Requirements SSR-2/1 (Rev. 1). It provides guidance on the overall I&C architecture and on the I&C systems important to safety to ensure safe operation of the plant in all plant states. SSG-39 integrates two very important interfaces with I&C design such as Human factors engineering and Cyber Security. Special attention was given to reduce duplication of guidance that is already in industry standards of IEC and IEEE to avoid confusion and result in unnecessary conflicts.

The preparation of SSG-39 took 8 years and involved considerable engineering and editorial work to produce drafts, reviews by member states and review committees, resolutions of numerous comments and final editorial work to publish it as a safety standard series publication in May 2016. The SSG-39 is a consensus document; some topics related to design of digital systems in safety applications, although important, were moved into and informative Annex, because consensus on those topics among several members states could not have been accomplished. Nevertheless, the SSG-39 provides a solid engineering basis to be considered when designing or reviewing various aspects of I&C systems.

References

[1] IAEA Statute, https://www.iaea.org/about/about-statute (1989)

[2] IAEA, Safety Guide No. NS-G-1.3, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, IAEA (2002)

[3] IAEA, Safety Guide No. NS-G-1.1, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, IAEA (2000)

[4] IAEA, Specific Safety Guide No. SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA (2016)

[5] IEC 60880, Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions, IEC (2006)

[6] IEEE 7-4.3.2, IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations, IEEE (2016)

[7] IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, IEC (2010)

[8] IEC 61513, Nuclear power plants – Instrumentation and control systems important to safety – General requirements for systems, IEC (2011)

[9] IAEA Nuclear Security Series No. 17, Computer Security at Nuclear Facilities, IAEA (2011)

[10] IAEA, Specific Safety Requirements No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design, IAEA (2016)

[11] IAEA, General Safety Requirements No. GSR Part 2, Leadership and Management for Safety, IAEA (2016)

[12] IAEA, Specific Safety Guide No. SSG-34, Design of Electrical Power Systems for Nuclear Power Plants, IAEA (2016)

[13] IAEA Nuclear Energy Series No. NP-T-3.16, Accident Monitoring Systems for Nuclear Power Plants, IAEA (2015)