

# CYBER SECURITY GUIDELINE DEVELOPMENT AND INSPECTIONS

## *Experiences at the Swiss Federal Nuclear Safety Inspectorate*

B. STAUFFER  
Swiss Federal Nuclear Safety Inspectorate (ENSI)  
Brugg, Switzerland  
bernard.stauffer@ensi.ch

J. DEJOZ  
Swiss Federal Nuclear Safety Inspectorate (ENSI)  
Brugg, Switzerland

M. ANGELO  
Swiss Federal Nuclear Safety Inspectorate (ENSI)  
Brugg, Switzerland

A. LUZIO  
Swiss Federal Nuclear Safety Inspectorate (ENSI)  
Brugg, Switzerland

### **Abstract**

Like probably other nuclear regulatory authorities, Switzerland also needed several attempts in the development of its cyber security regulatory guideline for nuclear facilities. A regulatory guideline is not only important so that operators and licensees know what they have to do. In Switzerland, regulatory guidelines explicitly serve as the basis for inspections (definition of expected target states). When developing the cyber security regulatory guideline, the responsible section at the nuclear regulatory and supervisory authority, the Swiss Federal Nuclear Safety Inspectorate ENSI, drew on experience from cyber security inspections before the regulatory guideline was drawn up. It went, so to speak, the opposite way. The paper describes the way to the development of the cyber security regulatory guideline and the experience gathered in this process.

### 1. INTRODUCTION

When developing a new regulatory guideline for cyber security for nuclear facilities, particularly with regard to nuclear power plants, the question arises as to what extent the recommendations from other areas such as the finance or telecommunications sector can be used. There are already a number of known standards and recommendations available, some of which are focused on specific fields of application. The NIST series, the IEC standards or the German BSI "IT-Grundschatz" are well known. For some years now, the ISO 27000-series became accepted, however it must be first adapted to the target industry. The IAEA Nuclear Security Series guidance, in particular the Nuclear Security Series No. 17, also references the ISO 27000-series and extends these with specific recommendations for nuclear facilities.

A regulator in the nuclear field has to decide whether he wants to use one of the aforementioned standards or recommendations for his purpose or whether he wants to create his own regulatory requirements. The latter is not without its problems since a regulatory guideline must ultimately be implementable. Both options are not without problems, since a regulatory guideline must ultimately be implementable. The regulator has to deal with the available technology to make sure that his requirements that can be met with the available systems and technologies. Finally, a regulatory guideline must also fit into the legal framework of the respective country and consider the existing safety and security culture. A new regulatory guideline is an additional element in an already heavily regulated domain.

The Swiss nuclear regulatory and supervisory authority, the Swiss Federal Nuclear Safety Inspectorate ENSI, faced all of the above questions on its way to its own cyber security regulatory guideline. During its final attempt, which ultimately led to a regulatory guideline that came into force beginning 2020, the Swiss nuclear regulator focused on the suitability of the regulatory guideline as a basis for inspections. The knowledge gained

from inspections running simultaneously with the drafting of the regulatory guideline was used during the discussions about the content of the regulation. The result is now a cyber security regulatory guideline, where the requirements are both specific enough for the operators and precise enough to be directly used as target states when conducting inspections.

## 2. HISTORY OF THE DEVELOPEMENT OF THE NUCLEAR CYBER SECURITY GUIDELINE

The supervision of cyber security in nuclear power plants in Switzerland started more than 15 years ago. In 2005, the license holders submitted their first concepts to ensure cyber security in their nuclear power plants. The supervisory authority at that time used the German BSI “IT Grundschutz” as the basis. The focus was particularly on the safety related I&C systems, physical protection systems where out of scope (the nuclear security section was not part of the supervisory authority at that time). After merging the supervision of nuclear safety and nuclear security in one authority in 2008, and in consideration of the draft of the IAEA NSS No. 17 and in the light of the emerging cyber threats, it became clear to those involved that a specific regulatory guideline is needed to ensure cyber security in nuclear facilities. Finally, STUXNET in 2010 was the trigger event to create a regulatory guideline on cyber security.

The first attempt to prepare a regulatory guideline started in 2011. The know-how of the supervisory authority was on a medium level and the authority was understaffed in that domain. Another problem was the lack of clarity at that time as to whether cyber security was purely a question of nuclear security or if it should be a co-work of nuclear safety and nuclear security. From today's perspective, too many questions were unanswered that this attempt to create a regulatory guideline had a real chance of success.

The second attempt started two years later. As a first measure, additional staff was hired with experience in cyber security in the financial sector. Then various existing standards and recommendations were compared and common elements extracted. A self-assessment was carried out on some of the identified topics and sent to the operators. This self-assessment was intended to check the suitability of the planned regulations for later inspections. The result of the self-assessments showed that the planned regulations were usable from the technical point of view, but were not suitable as target states for the inspection of cyber security measures. This meant that an essential goal, namely the suitability of the planned regulations for inspections by the supervisory authority, could not be achieved. Nevertheless, a first draft of a regulatory guideline was created. However, the following examination showed that the draft regulatory guideline too much focused on the protection of information (protection against loss of data) and less on the protection of computer systems against sabotage. Ultimately, we also realized that cyber security experiences in the financial sector has only a limited value when regulating a critical infrastructure such as nuclear power plants. We needed more industry-specific know-how.

## 3. THE NEW WAY FORWARD

The third and finally successful attempt to create a regulatory guideline began in mid-2016. Based on a request of the management board, the responsible group within the nuclear regulatory authority started a series of cyber security inspections, although no cyber security regulatory guideline was yet in place. Due to the lack of own regulatory requirements, the target states of the inspections were taken from the ISO 27000-series and the IAEA NSS No. 17. At the same time, the drafting of a new regulatory guideline was started.

The first cyber security inspection was designed as a so-called focus inspection. In such focus inspections, the same inspection topics are examined in the same way in all nuclear power plants. In addition, several inspectors from different specialist sections of the authority are involved. In the present case, the experts were from the electrical engineering section, the human and organisational factors section and the nuclear security section.

Since such focus inspections do not pay attention to plant-specific technical characteristics, the inspection topics focused on the general strategic and operational elements of cyber security. The inspected topics were:

- Commitment to and management of cyber security:
  - Integration of cyber security in the management system;
  - Risk management process including cyber security risk assessment;
  - Resources for the definition, application and review of cyber security in the management system;
  - Leadership and responsibility for the management of cyber security.
- Technical and operational implementation of cyber security:

- Assets management;
- Access control;
- Network security management and security during transmission of data;
- Security measures when operating remote access/remote maintenance systems;
- Event logging and monitoring;
- Handling of information security events and incidents.

These focus inspections were a door opener in many ways. The supervisory authority obtained a structured overview of the state of cyber security in the nuclear power plants. In addition, initial experience has been gained in an area that is more multidisciplinary than many other areas. The collaboration of safety- and security-oriented experts in particular provided a lot of insights and was challenging. These focus inspections were also revealing for the operators. The experts of the nuclear power plants were not familiar with the instrument of inspection so far. And they became aware of the directions of the planned regulation in this area.

These focus inspections also helped to identify problem areas. An important one is about the target state in inspections. The authority's inspection process requires a well-defined target state and subsequently an evaluation based on the comparison of the assessed current state with the predefined target state. But if the description of the target state is kept generic, the resulting final evaluation is likely to be an average of multiple particular evaluations. The view on particular problem areas is lost, but also specific good practices are not visible anymore. This is unsatisfactory from the point of view of both the authority and the operator.

During the following cyber security inspections between 2017 and 2019, the inspection topics were narrowed down. The target states were also defined more specifically. The inspection topics were:

- Authorization and user management;
- Event logging;
- Configuration management for cyber security;
- Vulnerability management;
- Incident handling;
- Firewall management;
- Handling of service devices (e. g. laptops used for PCS and I&C configuration);
- Cyber security of physical protection systems.

Both during the preparation and the follow-up of a cyber security inspection, the draft cyber security guideline was consulted and adapted if necessary. Through this parallel work and the resulting interaction between the cyber security inspections and the development of the cyber security regulatory guideline, the content of the guideline could be improved and refined in several iterations. The understanding, which target states are useful in inspections and which are not, has helped to increase the quality of the cyber security guideline.

#### 4. FURTHER EXPERIENCES DURING DRAFTING THE CYBER SECURITY GUIDELINE

In addition to the experiences and advantages already mentioned, the know-how in the field of cyber security has been greatly expanded. Further benefit of this process was that operators could already start to analysing their cyber security program based on the draft regulatory guideline and report to the authority whether trade-offs with nuclear safety or nuclear security existed on-site.

In the nearly four years during which we completed the cyber security guideline, we had a thorough program to involve all relevant stakeholders:

- Hearings with senior management of all nuclear facilities;
- Board of the authority;
- Different national competent authorities:
  - National Cyber Security Centre;
  - Armed Forces;
  - Intelligence Service;
  - the Federal IT Steering Unit MELANI (Reporting and Analysis Centre for Information Assurance);
  - and others.

In numerous discussions it also became clear, that people with different background were using the same words, but with a different definitions or different understanding of the meaning of those words. When developing a regulatory guideline, it is important to clarify these definitions and those of related terms. To do this, it is necessary to involve the aforementioned stakeholders and to discuss the terminology precisely.

## 5. CONTENT OF THE SWISS CYBER SECURITY GUIDELINE FOR NUCLEAR FACILITIES

The final cyber security regulatory guideline sets out the requirements regarding cyber security of programmable components and related systems in the area of automated information processing and handling. That means that all IT and OT systems in nuclear facilities which could have a direct or indirect effect on nuclear safety or nuclear security fall within the scope of the cyber security regulatory guideline. This includes also data storage and transmission outside a nuclear facility, for instance data used for maintenance or system configuration.

We did not reinvent the wheel. The content of the final cyber security regulatory guidance fairly covers what has to be addressed in a cyber security regulatory guidance. This is, among others [1]:

- The administrative controls (excerpt):
  - Strategic plan on cyber security;
  - Policies and procedures;
  - Awareness programs / Interaction with “Manager in the field”.
- The organisational controls (excerpt):
  - Independency between departments who run the IT/OT and the CSO;
  - Qualification of involved personnel;
  - Competences and accountabilities of involved personnel;
  - Advisory board on cyber security.
- The technical controls (excerpt):
  - Access controls and its AAA services (authentication, authorization, accounting);
  - Rights management;
  - Cryptography;
  - Network architecture and components;
  - Needs arising from backup and recovery strategies;
  - Portable storage devices;
  - Redundancy and diversity (defence-in-depth).

Finally, the Swiss cyber security regulatory guideline is not limited to describing the known threats and how they can be countered, but sets out an ongoing process to ensure a robust cyber security system.

## 6. THE SWISS PROCESS FOR CREATING A REGULATORY GUIDELINE

The development of a regulatory guideline (same as regulatory directive) at the Swiss nuclear regulator follows a well-defined process. It has similarities with the drafting process for IAEA Nuclear Safety and Nuclear Security Series documents. There is first an initial specification of what needs to be regulated (similar to a DPP). After the subsequent drafting of the regulatory guideline, one or several external hearings can be conducted. During such hearings the operators can argue what kind of effect an intended regulation could have on their nuclear facilities. The intention is to recognize whether a regulatory requirement might have negative effects on nuclear safety or nuclear security in a nuclear facility.

After these external hearings, the draft regulatory guideline is corrected if necessary. Then the guideline undergoes an authority’s internal review. This quality assurance step ensures that different authority requirements do not contradict each other or have undesirable interactions. After this step, minor or major adjustments will again be made to the draft regulatory guideline, if necessary. This step is similar to Step 7 of the IAEA SPESS B process (Committee review).

After the authority’s internal review, a public consultation is conducted which lasts an average of four months. For classified regulatory guidelines (some of the nuclear security guidelines are classified), the circle of external stakeholders is restricted according to the need-to-know principle. Depending on the number of comments, the subsequent revision of the draft regulatory guideline is either minor or quite complex. After this

revision, a further review is carried out by an authority's internal committee (similar to Step 11 IAEA SPESS B) before a regulatory guideline is finally put in force.

As with the IAEA, the process for drafting a regulatory guideline takes a rather long time. While a revision of an existing regulatory guideline takes an average of 1.5 to 2 years, the development of a new regulatory guideline takes at least another year. This was no different when the cyber security guideline was drawn up: it took around 3.5 years to develop and review.

## 7. CONCLUSIONS

The development of the regulatory guideline on cyber security was hard work. In retrospect, the several attempts have helped to produce what we consider to be a good regulatory guideline. The supposedly lost time is compensated for by the fact that the regulatory guideline can be put in force and implemented immediately and no transitional periods are necessary for operators. The early involvement and information of the operators have also greatly increased acceptance of the regulatory guideline.

The expertise on cyber security in the industrial environment that the supervisory authority has built up during this period is recognised by other authorities and organisations and facilitates the Authority's access to specialized cyber security groups.

## REFERENCES

- [1] DEJOZ, J., "Swiss Approach to Cyber Security Regulations", Presentation at IAEA Technical Meeting on Computer Security Approaches and Applications in Nuclear Security, Berlin, 2019.