Contribution ID: **448** Type: **Paper**

# Cyber Security guideline development and inspections - experiences with the ”opposite” approach

During inspections, one compares the actual state with a nominal state. This nominal state may be based on national laws, regulatory requirements or guidelines, or international standards. However, in the area of cyber security for nuclear facilities, one often finds itself in a dilemma: missing laws or guidelines. The adaptation of laws is a protracted process, and international standards are not sufficiently precise to use it as a clearly defined nominal state in inspections.

Regarding regulatory guidelines, we observed that many countries are having trouble creating such for nuclear facilities. And after the guidelines were put into force, we observed that they are difficult to apply or are not suitable for inspections.

We had the same problems. Over the years, we started with the drafting of a cyber security guideline, but we didn't succeed. It changed in 2016 when we started to conduct inspections on cyber security in the nuclear power plants without having a cyber security guideline nor specific legal provision. To make matters worse, neither the supervisory authority nor the nuclear facili-ties had any experience with inspections in cyber security. However, assessment of cyber securi-ty in the NPPs was already done before, but without the use of the inspections.

The first inspection, which was carried out in all nuclear power plants, was a so-called "focus inspection", which was carried out together with the colleagues from electrical engineering and human and organizational factors. As a basis (nominal state) a selection of recommendations from the ISO 27001 and the IAEA NSS 17 were used. All major aspects of cyber security (e. g. policies, protection measures, incident response and mitigation) were examined, however on a rather generic level. The results were inconclusive. On the one hand, this focus inspection al-lowed us to get a good overview of the cyber security measures at the nuclear power plants. On the other hand, nominal states based on an ISO standard or IAEA guidance are rather difficult to apply. Since the recommendations in these international standards (and this also applies to the NSS 17) have some scope of interpretation, they are easily met. But in nuclear facilities, we usu-ally expect higher standards.

In the following years we carried out further inspections in the nuclear power plants. During this process, the topics to be inspected were narrowed, but we went deeper into the topics. With in-creasing experience, the nominal state could be better defined, which contributed to the credibil-ity of the evaluations. In addition, we learned what exactly we have to specify in a regulatory guideline.

In 2017, we restarted the drafting of a cyber security guideline for nuclear facilities. It now be-came apparent that the experiences from the inspections allowed us to formulate the require-ments in the guideline clear and precise. The applicability of the requirements for the licenssee and the usability as a nominal state for inspections are in our opinion much better.

In short, with learning by doing, we first gained experience with cyber security inspections, which proved to be very helpful during the guideline development. We are convinced that this (unintentionally planned) approach has helped us to create a better cyber security guideline and saved us a subsequent revision of it. It should also be noted that the licensees have gained dur-ing this time a certain degree of confidence and are now in a better position to understand the requirements in the new guideline.

And last but not least: with this experience, along with the expert review during an IPPAS mis-sion, we have been able to increase our professional credibility both vis-à-vis the licensees and other state institutions

## Gender

Male

## State

Switzerland

**Authors:** Mr STAUFFER, Bernard (Swiss Federal Nuclear Safety Inspectorate ENSI); Mr DEJOZ, Jorge (Swiss Federal Nuclear Safety Inspectorate ENSI); Mr MANCO, Angelo (Swiss Federal Nuclear Safety Inspectorate ENSI); Mr LUZIO, Andrea (Swiss Federal Nuclear Safety Inspectorate ENSI)

**Presenter:** Mr STAUFFER, Bernard (Swiss Federal Nuclear Safety Inspectorate ENSI)

**Track Classification:** CC: Information and computer security considerations for nuclear security