This contribution addresses the question Q2.1 raised by the Special Reporter, hereby textually reported:

Question 2.1: What is the industry's experience in planning, implementation, and evaluation of, as well as compliance with cybersecurity regulations, standards, measures, or procedures?

EPUs are interested in the application of appropriate assessment tools to check their compliance to cybersecurity standards and measures. Such tools are required to meet the following features:

F1. Support to cybersecurity requirement standards, e.g. ISO/IEC 27000, NIST 800-53, NISTIR 7628, ISA/IEC 62443
F2 Allow a standard compliance analysis which is scalable with increasing Security Assurance/Maturity Levels, supporting a graded security roadmap to achieve compliance with increasing MLs/SLs
F3 Derive security controls from the architecture analysis
F4 Support the mapping between standard security requirements and solutions/measures on assets and processes
F5 Support the generation of Security Test Plans
F6 Allow scaling up the cybersecurity assessment with the number of connected generation plants and flexible loads.

For more details about assessment results, see Paper #10794 of CIGRE Session 2022.

It is expected that Regulations, Laws and Network Codes on cybersecurity implement strategies requiring compliance with

- specific standards
- appropriate Maturity/Security Levels
- appropriate technical measures
- processes and products certifications.