

Paris Session 2022



Standards and Tools for assessing the EPU cybersecurity posture

Study Committee D2

PS2 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?

Giovanna Dondossola Italy



Compliance with Cybersecurity Standards

- EPU's are interested in the application of assessment tools to check their compliance to cybersecurity standards and measures
- Cybersecurity assessment tools with identified features
- F1. Support to cybersecurity requirement standards by national laws and regulations, e.g. ISO/IEC 27000, NIST 800-53, NISTIR 7628, ISA/IEC 62443
- F2 Allow a standard compliance analysis which is scalable with Maturity/Security Levels, supporting a graded security roadmap to achieve compliance with increasing MLs/SLs

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Compliance with Cybersecurity Measures

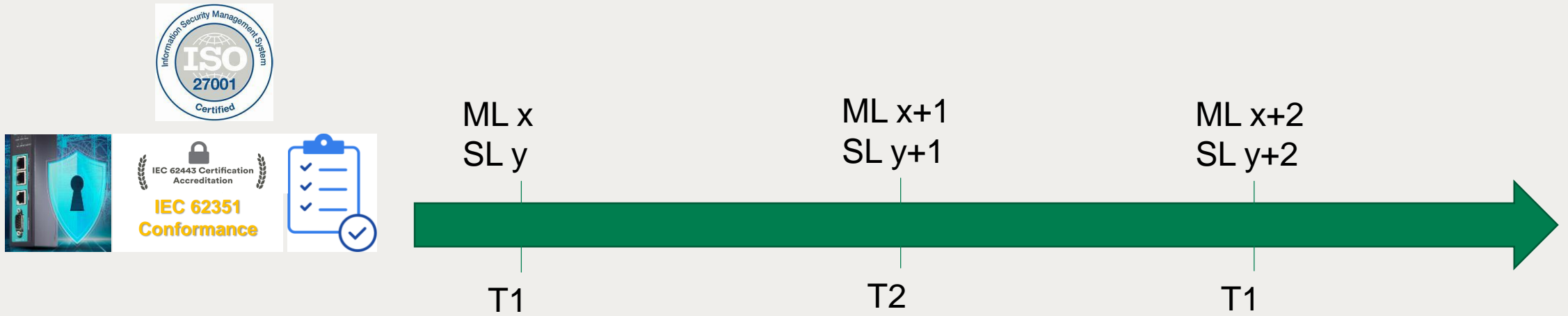
- F3 Derive security controls from the architecture analysis
- F4 Support the mapping between standard security requirements and solutions/measures on assets and processes
- F5 Support the generation of Security Test Plans
- F6 Allow scaling up the cybersecurity assessment with the number of connected generation plants and flexible loads



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

Compliance with Regulations

- The expectation is 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



Group Discussion Meeting

Thank you for your attention !