

CIGRE Study committee D2

PROPOSAL FOR THE CREATION OF A NEW WORKING GROUP

WG D2.71

NAME OF THE CONVENOR

Alan Soares (UNITED STATES OF AMERICA)

TITLE

Software Assurance and Lifecycle Quality for Digital Power Systems

THE WG APPLIES TO DISTRIBUTION NETWORKS: YES

ENERGY TRANSITION

3 / Digitalization

POTENTIAL BENEFIT OF WG WORK

2 / potential interest from a wide range of stakeholders

3 / likely to contribute to new or revised industry standards

4 / state-of-the-art or innovative solutions or directions

5 / Guide or survey on techniques, or updates on past work or brochures

6 / work likely to contribute to improve safety

STRATEGIC DIRECTION

1 / The electrical power system of the future reinforcing the End-to-End nature of CIGRE: respond to speed of changes in the industry by preparing and disseminating state-of-the-art technological advances

2 / Making the best use of the existing systems

SUSTAINABLE DEVELOPMENT GOAL

9 / Industry, innovation and infrastructure

BACKGROUND :

The digitalization of electric power systems is increasing the dependence of critical operational functions on software and firmware embedded in primary and secondary equipment, protection, automation and control systems, substations, **telecommunications networks**, SCADA/EMS/DMS platforms, engineering systems, **cybersecurity infrastructure** and other operational environments. These software- and firmware-dependent functions increasingly rely on components originating from multiple OEMs and third-party suppliers, including proprietary software, firmware, operating systems, libraries, open-source components, communication stacks, configuration data, cybersecurity components and other software dependencies.

A particular challenge for the electric power sector is the mismatch between the long operational lifecycle of power-system assets and the comparatively rapid evolution of software, firmware and supporting digital platforms. Assets may remain in service for decades, while software components, operating systems, libraries, telecommunications platforms and cybersecurity technologies may undergo frequent updates, substitutions or obsolescence. Changes to individual components can therefore affect interoperability, deterministic behaviour, timing performance, communications availability, reliability, cybersecurity, and the integrity of the end-to-end operational function.

These challenges are further amplified by the high availability requirements, restricted maintenance windows, legacy-system dependencies, multi-vendor integration and strong interdependencies between **operational technology, telecommunications and cybersecurity systems** commonly found in power-system environments. Utilities may also have limited or no visibility of source code and must therefore establish appropriate assurance through supplier evidence, software and firmware provenance and authenticity controls, Software Development Lifecycle (SDLC) and Secure Software Development Lifecycle (SSDLC) maturity assessment, behavioural and black-box testing, verification and validation, integration and regression testing, and

lifecycle governance.

Emerging software-defined environments, including **Virtualized Protection, Automation and Control (VPAC)** and virtual IEDs, further increase these assurance dependencies by decoupling critical operational functions from dedicated physical hardware and introducing additional dependencies on operating systems, virtualization platforms, **telecommunications services, cybersecurity controls, time synchronization, network services** and shared computing infrastructure.

PURPOSE / OBJECTIVE / BENEFIT OF THIS WORK :

- To establish an internationally applicable framework for software and firmware assurance from the perspective of utilities as asset owners, system integrators and operators.

- To define risk-based assurance practices linking the criticality of software- or firmware-dependent functions to the evidence, testing, supplier controls and lifecycle activities required.

To provide guidance for assessing OEM software development lifecycle (SDLC) and secure software development lifecycle (SSDLC) maturity, including requirements, development, verification, vulnerability management and release practices, as well as software/firmware provenance and authenticity, supply-chain assurance, behavioural testing, and change impact/requalification.

- To aid in strengthening resilience and lowering risk for vital infrastructure, while addressing the shortage of skilled professionals.

SCOPE :

The WG will cover:

1. Software and Firmware Criticality and Assurance Levels:

- Develop a practical methodology for classifying software- and firmware-dependent functions according to their operational criticality, potential impact on protection, control, availability, safety and system reliability. Define corresponding assurance levels and link each level to proportionate requirements for evidence, verification, validation, testing, traceability, supplier assurance and lifecycle controls.

2. Provenance, Authenticity and Supply-Chain Assurance:

- Assess practices for establishing and maintaining software and firmware provenance, integrity and authenticity throughout their lifecycle, including supplier and OEM traceability, third-party and open-source dependencies, software and firmware inventories, Software Bill of Materials (SBOM), where applicable, trusted delivery mechanisms, component substitution, dependency transparency, end-of-support considerations and continuity risks associated with long-life power-system assets.

3. OEM Software Lifecycle Maturity, Secure Development and Supplier Assurance:

- Define criteria by which utilities can assess the maturity and adequacy of OEM Software Development Lifecycle (SDLC) processes and the integration of Secure Software Development Lifecycle (SSDLC) practices. This should include requirements management, secure architecture and design, configuration management, development and coding practices, verification and validation, vulnerability and defect management, regression and security testing, release and change management, patch and remediation processes, supplier quality controls, traceability and long-term lifecycle support.

4. Black-Box, Behavioural, Verification and Validation Testing:

- Investigate assurance methods applicable where source-code visibility is limited or unavailable, including black-box functional and behavioural testing, abnormal-condition testing, robustness and fault-response assessment, interoperability testing, performance and timing validation, Factory Acceptance Testing (FAT), Site Acceptance Testing (SAT), regression testing, simulation, Software-in-the-Loop (SIL), Hardware-in-the-Loop (HIL) and other appropriate verification and validation techniques. The work should consider how the required depth of testing may vary according to software criticality and operational risk.

5. Change Impact Assurance, Configuration Management and Requalification:

- Develop a risk-based approach for determining the extent of retesting, revalidation and requalification required following changes to software, firmware, operating systems, libraries, communication stacks, configurations, virtualization platforms, hardware dependencies or interfacing components. Consider configuration baselines, dependency mapping, version compatibility, release integrity, change traceability, rollback capability, recovery procedures and preservation of validated known-good configurations.

6. Multi-Vendor and Software-Defined Power-System Environments:

- Address system-level assurance in environments comprising multiple OEMs, suppliers and system integrators, including interoperability, shared dependencies, interface responsibilities and accountability for integrated-system assurance. Virtualized Protection, Automation and Control (VPAC), virtual IEDs and other software-defined power-system environments should be considered as important application cases for evaluating assurance where critical functions depend on multiple independently evolving software, firmware, computing, communication and infrastructure layers.

7. Operational Assurance, Quality Metrics and Maturity Assessment:

- Investigate practices for maintaining software and firmware assurance throughout operational life, including defect and problem management, field-failure analysis, supplier feedback, release stability, configuration compliance, change failure, recurring defects, vulnerability and remediation performance, obsolescence exposure and lifecycle-support risk. Identify practical software-assurance metrics and key performance indicators (KPIs), and consider the development of a **Software Assurance Maturity Framework for Power Utilities** to support

benchmarking, gap assessment and continuous improvement.

8. Relationship With Existing Work

- The WG will build upon and complement relevant CIGRE activities addressing digitalisation, asset lifecycle management, testing, version management, obsolescence and software-dependent power-system functions. Particular consideration will be given to the following existing Working Groups:
- **JWG A3/D2.52 - Application of Digital Twin in Switchgear**, particularly regarding software-dependent equipment, digital representations and lifecycle information associated with switchgear.
- **JWG A3/B3/D2/IEEE PES.54 - Global Database for Circuit Breaker Testing Data**, particularly regarding digital data, testing evidence, traceability and the use of equipment lifecycle information.
- **WG B4.104 - HVDC Digital Twin**, particularly regarding software-intensive HVDC control and protection environments, digital models and lifecycle assurance.
- **WG B5.63 - Protection, Automation and Control System Asset Management**, particularly regarding lifecycle and asset-management practices for software- and firmware-dependent PAC systems.
- **WG B5.75 - Documentation and Version Handling Related to Protection, Automation and Control Functions**, particularly regarding configuration, documentation, revision and version management.
- **WG B5.81 - Obsolescence Management for Protection, Automation and Control Systems**, particularly regarding software and firmware obsolescence, lifecycle support and technology evolution.
- **The proposed WG will complement these activities by focusing specifically on software and firmware assurance across the lifecycle, including SDLC/SSDLC maturity, provenance and authenticity, supplier assurance, behavioural and black-box testing, change-impact assessment, regression testing, requalification and operational assurance.**

DELIVERABLES AND EVENTS

Deliverables Types

Annual progress and activity report to Study Committee

Future connections

Technical Brochure and Executive Summary in Electra

Tutorial

Webinar

Time schedule

Q1	2027	Recruit members
Q2	2027	Develop work plan
Q2	2029	Draft TB for Study Committee review
Q3	2030	Final TB

APPROVAL BY TECHNICAL COUNCIL CHAIRMAN:

Rannveig S. J. Loken

October 23rd, 2026



cigre.org

e-cigre.org

cse.cigre.org

session.cigre.org

