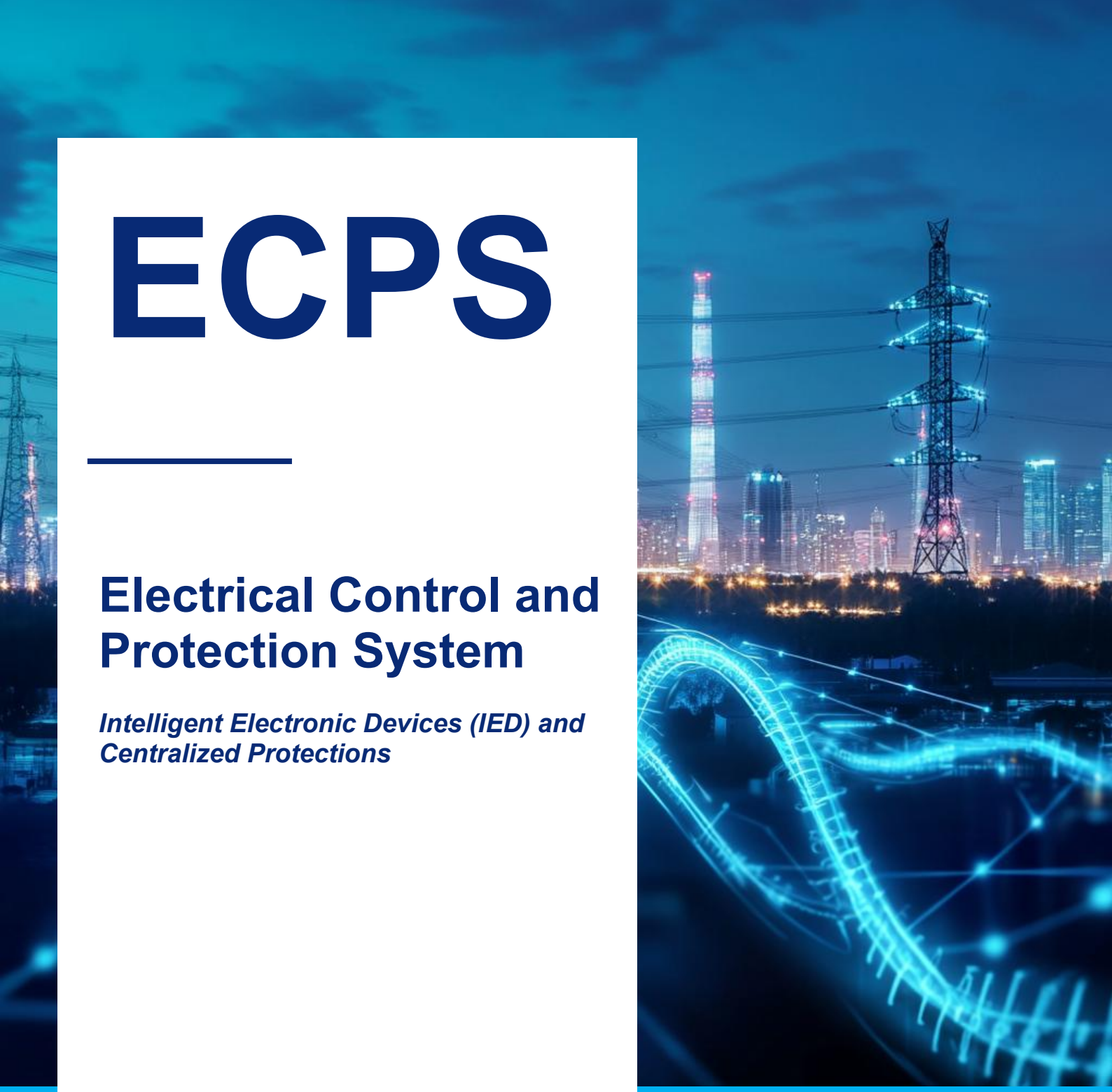


# ECPS

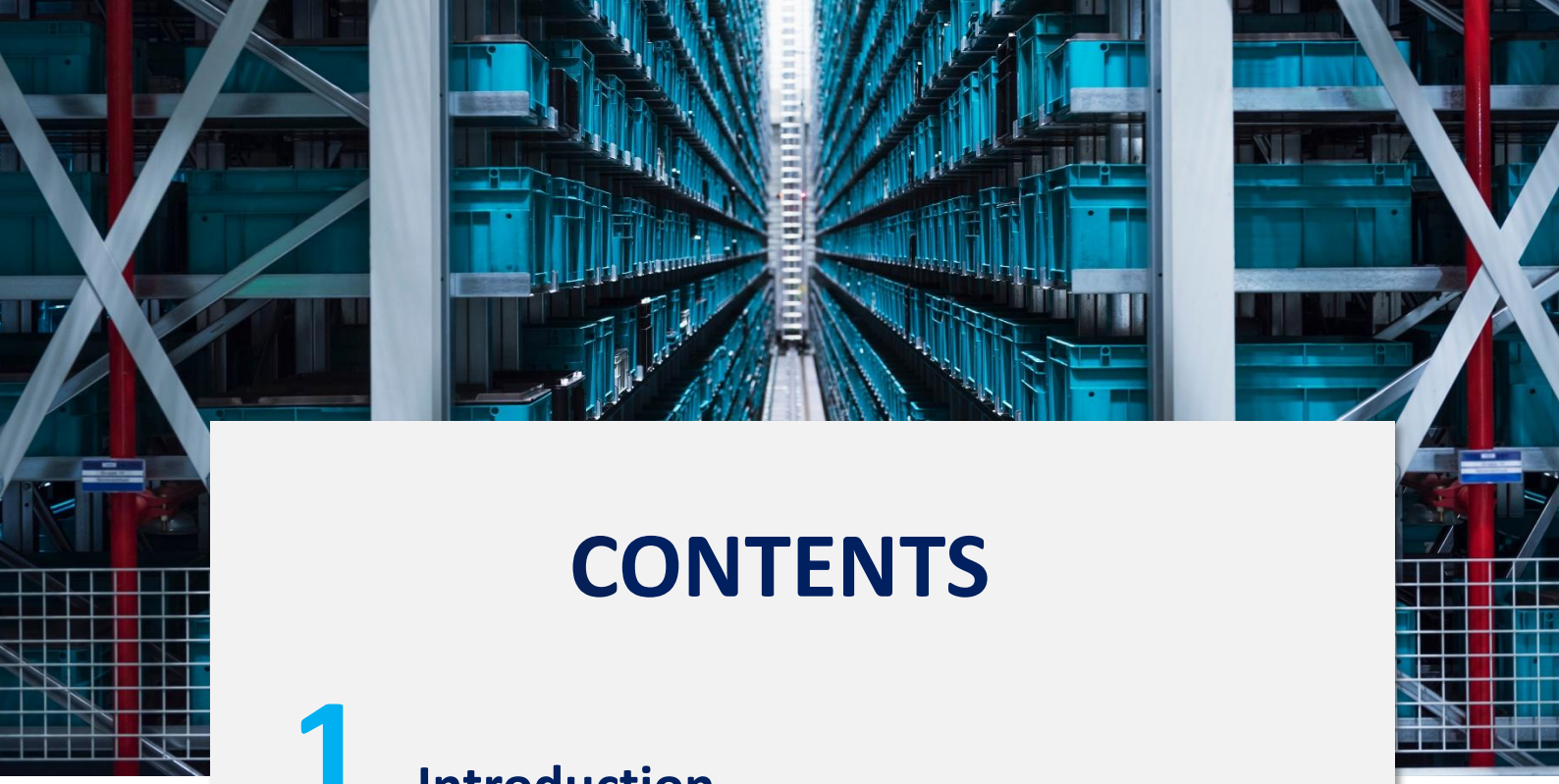
## Electrical Control and Protection System

***Intelligent Electronic Devices (IED) and Centralized Protections***

18 MARZO 2026

**EOHM Engineering Solutions**

ABB
VALUE PROVIDER



# CONTENTS

# 1 - Introduction

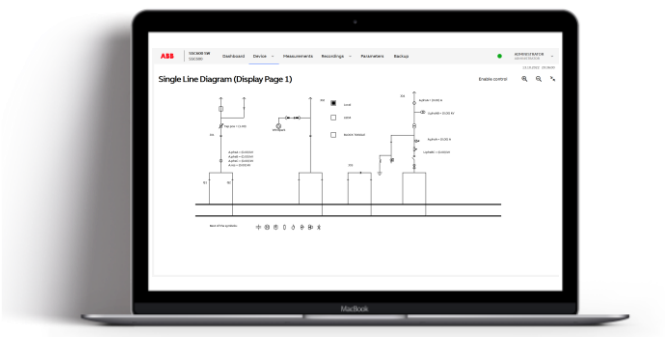
Over the last few years, accompanying the digital transformation process that encompasses practically all economic and social branches, the industry has not ceased to incorporate ‘smart’ devices not only in the process and instrumentation field, integrated in the plant control systems, but also in the electrical field.

This evolution is particularly relevant in industrial plants, power generation facilities, utilities, as well as in critical infrastructure such as data centers, where electrical reliability directly impacts operational continuity and safety.

***Electrical digitalization beyond wiring replacement: smarter control, deeper integration and centralized system management for operational resilience.***

In the electrical area, as we move into the digital age, conventional hardwired equipment is frequently moved to intelligent devices managed by communication protocols, which are known in the electric power industry as IED (Intelligent Electronics Devices).

This transference to the digitalization of electrical processes enables the register and storage of data, automatic transfers, interlocks, and trip management, monitoring and remote configuration of electrical protections, etc., replacing the traditional hardwired logic.




With the purpose of integrating all these utilities in a control system, the called Electrical Control and Protection System (ECPS) arises as a system that enables an intelligent full integration of the electrical systems and provides the following key benefits associated to this digital adaptation, among others:

**Reduction of wiring**
**Scalable system expansion**
**Programming flexibility and scalability**
**Program simulations**
**Control and Monitoring of complete system**
**Multi-protocol management**
**Remote configuration**

These benefits translate into reduced installation and lifecycle costs, higher system availability, and an architecture that can be extended or reconfigured without significant re-engineering effort.

# 2 – IED and Electrical Data Highway

## General Description

The Electrical Control and Protection System (ECPS) is based on substation automation protocols, specifically the IEC 61850 standard, which ensures interoperability in power system architectures. It enables high-speed communication between intelligent electronic devices (IEDs) with guaranteed delivery times and high availability, which allows to typically integrate in the ECPS following features:

- Electrical protection and interlocks
- Trip commands and equipment intertrip
- Fault monitoring system recorder
- Automatic transfers system (ATS)
- Emergency Diesel generator Sequences
- Dispatch communication management
- Electrical system supervision (SCADA)

*Figure 1. ABB REX615 Protection Relay*

An integrated ECPS using IEC 61850 improves reliability, standardizes communication under a single protocol, provides a unified interface for supervision, enhances data quality for operators, and centralizes communication with higher-level systems (DCS, dispatch centers, etc.).

*IEC 61850 enables integration of High, Medium, and Low Voltage IEDs into a unified protection and supervision system.*

IEDs perform protection, control, and monitoring functions, supporting SCADA data collection and replacing traditional hardwired schemes with GOOSE messaging over Ethernet networks.

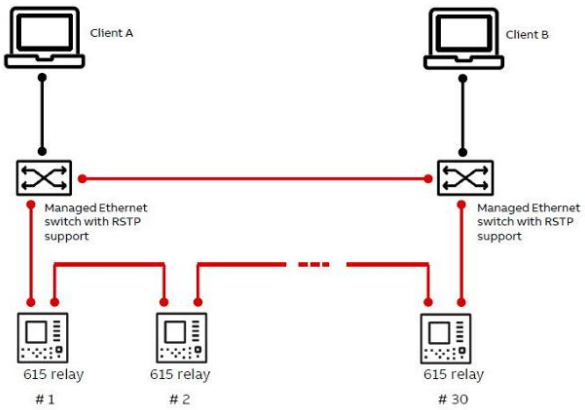



*Figure 2. Typical IEDs architecture based on IEC 61850*

## IEC 61850 Data Communication

IEC 61850 is an international standard for substation automation that ensures device interoperability. All IEDs must comply with IEC 61850, meaning configuration files are handled according to the Substation Configuration Language (SCL), including standardized data models, services, and communication. This enables system integrators to use consistent, vendor-independent data to build complete and reliable systems.

MMS (Manufacturing Message Specification) is used for communication with supervisory (Level 2) systems, while time-critical signals such as trip commands require faster communication. In IEC 61850, GOOSE (Generic Object-Oriented Substation Events) messages distribute status information as multicast messages, supporting trip signals, interlocks, and fast logic exchanges between IEDs.

The time synchronization is ensured through Network Time Protocol (NTP) or Precision Time Protocol (PTP).

# 3 – Cybersecurity

- **IEC 62351** – Data and communications security
- **IEEE 1686** – IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities
- **IEC 62443-4-2** – Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components

Building on the IEC 61850-based ECPS architecture, the increasing digitalization and integration of IEDs, communication networks, and SCADA systems expand the cyber attack surface of OT environments. As protection, control, and monitoring functions rely on standardized protocols and Ethernet networks, cybersecurity becomes essential to ensure system reliability and availability.

International standards and frameworks define cybersecurity requirements for SCADA environments and industrial control systems (ICS). IEC 62443 provides the global framework for industrial cybersecurity (IACS), covering systems, components, and processes. NIST SP 800-82 is a widely adopted OT security reference, while IEC 62351 addresses security for power system communications such as IEC 61850. In Europe, NIS2 establishes regulatory obligations for critical infrastructure operators.

**NIS 2**

**Article 21 of Directive (EU) 2022/2555** defines the minimum cybersecurity measures organizations must implement, requiring them to be appropriate and proportionate to risk, particularly considering OT systems, legacy technologies, continuous processes, and hybrid architectures in industrial environments.

**Assets & Risk**

*Identify and classify OT/ICS assets, map communication flows and assess operational risks (IEC 62443-1-2, IEC 62443-3-2, NIST SP 800-82).*

**Zones & Network**

*Implement security zones and conduits, isolate OT from IT networks and control communications between zones (IEC 62443-3-3).*

**Secure Comms**

*Apply IEC 62351 to authenticate and encrypt communications in power systems, protecting SCADA links, substations and control centers.*

**Identity & Access**

*Manage identities and privileges in OT environments. Enforce strong authentication and least privilege in accordance with IEC 62443-3-3 SR 1.1 and NIST SP 800-82.*

**Detection & Response**

*Continuously monitor OT systems for anomaly detection. Maintain ICS/SCADA-specific incident response procedures aligned with applicable frameworks (IEC 62443, NIS2, NERC CIP).*

# 4 – Electrical Control & Protection System

## System Architecture

The ECPS system architecture typically includes:

- Intelligent electronic devices (IED).
- PC based protection and control system, (gateway/system server)
- Operator station, including HMI, fault monitoring and disturbance recording.
- IEC 61850 Data communication network.

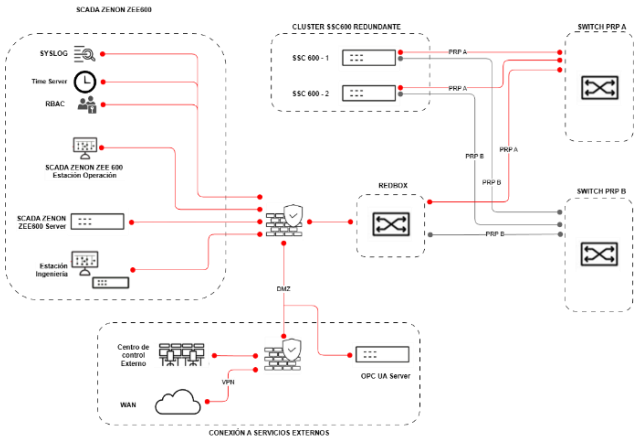



*Figure 3. Simplified sketch of system architecture*

This architecture consists of three (3) control levels and associated communications, described below.

### LEVEL 0 (L0): Hardwired I/O

Includes primary electrical equipment (switchgear, transformers, generators, breakers) and associated signals. Its function is to manage input/output data. Signals are typically hardwired to protection relays or merging units and communicated to higher levels, enabling data centralization in the ECPS.

### LEVEL 1 (L1): IEDs

Comprises protection IEDs performing data acquisition, calculations, control, and interlocking.

Additional equipment such as transformer AVR and metering panels may be included. The L1 network enables communication between IEDs and the ECPS.

IEDs typically include redundant fiber interfaces (100BaseFX) supporting HSR or PRP topologies, integrated via Redbox devices. Communication with higher levels uses IEC 61850, while GOOSE enables peer-to-peer exchange. Non-IEC 61850 devices can be integrated via Modbus TCP within a multi-protocol architecture.

### LEVEL 2 (L2): Gateway

Integrates the gateway, managing protocols, HMI interfaces, and time synchronization. The L2 network connects L1 and L2 equipment. Communication is based on IEC 61850 over TCP/IP with redundancy. This level enables bidirectional communication with the DCS and transmission of data to the Dispatch Center (L3).

### LEVEL 3 (L3): Supervision

Includes operator workstations and HMIs for control, supervision, data archiving, alarms, trending, and fault recording. It supports IED configuration, remote engineering, and maintenance. As the highest level, it integrates dispatch center supervision using standard protocols (e.g., IEC 60870-5-104).

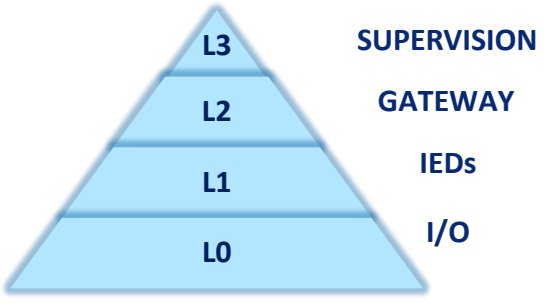



*Figure 4. Architecture Hierarchy*

## Digital Protection Relays

The communication and automation are implemented through decentralized Intelligent Electronic Devices (IEDs), specifically digital protection relays installed in protection panels and switchgear.

These relays are multifunctional, programmable, and communication-enabled, integrated at Level 1 of the ECPS architecture. They provide measurement and transmission of key electrical parameters (I, V, P, Q) using IEC 61850 over fiber optic or copper networks.

Detailed information, such as event logs, trip logs, and oscillographic fault records, is stored in the multifunction protection device and can be downloaded locally to a laptop or transmitted to higher-level systems for further analysis using fault recorder functionalities.

Apart from the electronic protection relays other intelligent equipment (IEDs) such as, remote I/O modules, merging units or bay control units (BCUs), can be integrated in the level 2.

## Data Exchange and Interlocks

IEDs combine protection, control, metering, and monitoring functions, enabling signal digitalization.

Typically, all signals from the bay or switchgear section are hardwired to the relay's I/O modules: current and voltage transformers (CTs & VTs); circuit breaker, disconnector and earthing switches status; open and closes commands, trip signals, interlock signals, etc. IEC 61850 Ethernet-based communication replaces conventional wiring for process communication and interlocking.

IEC 61850 GOOSE is used for bidirectional communication between IEDs and is equivalent to hardwired signals between devices with a high-reliability and faster speed communication that allows its use for implementing interlocking and intertrip functionalities.

Data exchange through GOOSE messaging allows to simplify operations, saving space, reducing labor time and outages, and increasing the safety of personnel.

- Power Supply and I/O
- Event and Fault Recorder
- HMI Display / Touch-screen
- Local / Remote Access
- Latched Programmable LEDs signals
- Multi-protocol / IEC 61850 based
- NTP/PTP Tyme Synchronization
- Internal Auto-Diagnostic System

# Automatic Transfer System

Under the ECPS philosophy, automatic transfer systems (ATS) for MV and LV switchgears are implemented via IEDs, ensuring reliable operation even if communication with higher-level systems is lost. ATS can operate manually, with the operator issuing open and close commands to the circuit breakers, or automatically, transferring the feeder by opening one incoming and closing the tie-breaker if a busbar loses voltage. All operations are governed by interlock schemes to prevent incorrect actions.

Automatic supply transfer is designed to prevent prolonged operation under abnormally low voltage from the primary supply and to restore busbar voltage from an alternative source after a power loss, supporting continued plant operation.

Power source transfer is normally initiated by detection of undervoltage or normal source open signal, but other detection systems could be used. Logics can be implemented in the involved protection relays and command signals between different relays are sent through GOOSES, based on IEC 61850 standard.

Automatic transfers are normally “Six-cycle fast transfer” type as per IEEE Std. 666. In the operational sequence the IED relay opens the normal source breaker, then sends a GOOSE message to close the alternative source or tie-breaker only after the normal breaker is open, preventing simultaneous connection. The alternative source then restores power to the motors, allowing them to reach rated speed within the specified time even after a brief voltage loss.

In the same way that for Automatic transfer logics, in emergency systems, logics for emergency generator sequences can be also implemented in the IEDs.

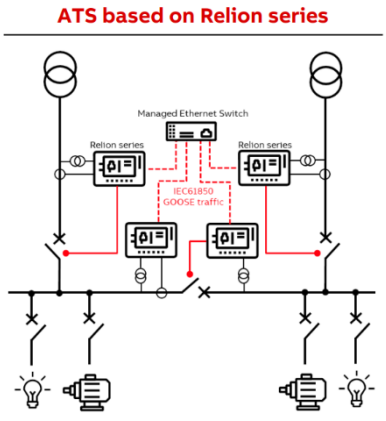



*Figure 5. ATS scheme based on Protection Relays*

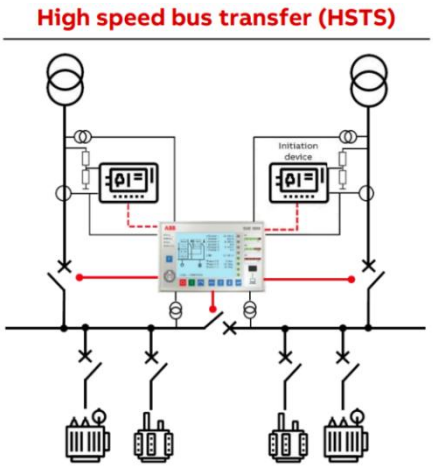



*Figure 6. ATS scheme based on Transfer Device*

An alternative to a relay-based ATS is a High-Speed Transfer System, where a dedicated piece of equipment performs the switching logic, enabling faster transfer times. This ensures process continuity and power supply quality while maintaining a safe environment for personnel and equipment. Transfer speed can be further improved by using circuit breakers with fast operating mechanisms.

| Transfer System | Average Total Transfer Duration |
|---|---|
| HSTS Time depending transfer | > 1500 ms |
| HSTS Residual Voltage transfer | 400 – 1200 ms |
| ATS based on Relays | > 400ms |
| HSTS 1st phase coincidence transfer | 250 – 400 ms |
| HSTS Fast Transfer | 30 – 100 ms |
| HSTS + VM1-T Fast operating CB | ≤ 30 ms |

**Transfer duration** = protection detection + SUE protection time + CB Opening

*Figure 7. Automatic Transfer System Alternatives*

## Fault Monitoring System

A digital fault monitoring and disturbance recorder for the electrical system can be integrated in the ECPS. The FMS centralizes in a single point the fault records of all protection relays of the electrical system of the plant.


*Figure 8. Comtrade Viewer for Fault Monitoring and Analysis*

The FMS is able to establish a communication with all the protection relays and download the fault record 'oscillos' in case of a protection trip, what is done automatically. As soon as a fault record appears in one protection relay, the FMS downloads the fault record. By this way the operator can open the "comtrade" file and with one specialized fault record software, installed in the corresponding operator workstation, analyze the fault extinction length, possible fault reasons, situation sooner and later of the fault, etc.

The fault monitoring feature, integrated into the Electrical Control & Protection System operator station, enables relay setting adjustments and access to event records and real-time measurements provided by protection relays.

This functionality is also available for other control and measurement devices. Therefore, the Fault Monitoring System (FMS) could interface with bay control units (BCUs), switches (SW), unit control systems (UCS), and other devices.

## HMI / SCADA

A PC based protection and control system is usually installed for supervision and operation of the ECPS. It includes a gateway or server, and operator station, as separated equipment, or as standalone station.

The supervision system ensures the following functions:

- Status monitoring of all IED, and measurement
- Operation of electrical system: commands for manual operation from the HMI or SCADA
- Electrical system single line diagram representation
- Alarming and sequence of events register
- Data logging and trend analysis
- Fault analysis
- Data storage
- Interface with other systems: DCS, dispatch center, etc, under the required protocol:
    - Modbus TCP/IP
    - DNP3
    - IEC103
    - IEC104
    - …etc.

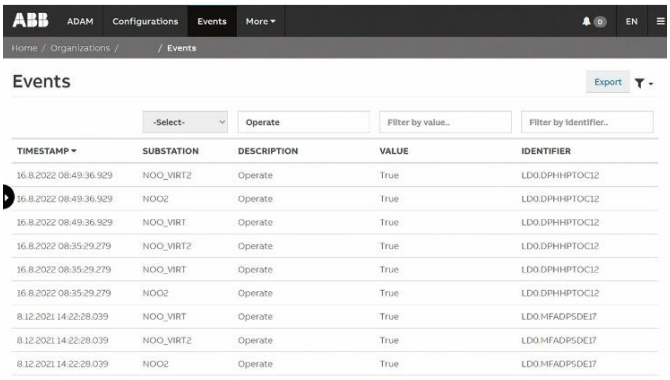



*Figure 9. SCADA Events Screen*

The operation station provides the monitoring part of the system as well as the control by sending commands to the IEDs.

## DCS Integration

While the ECPS is focused on the electrical and protections system the ICS or the Distributed Control System (DCS) of the plants oversees of the complete process and operation. Usually, both systems must exchange some information.

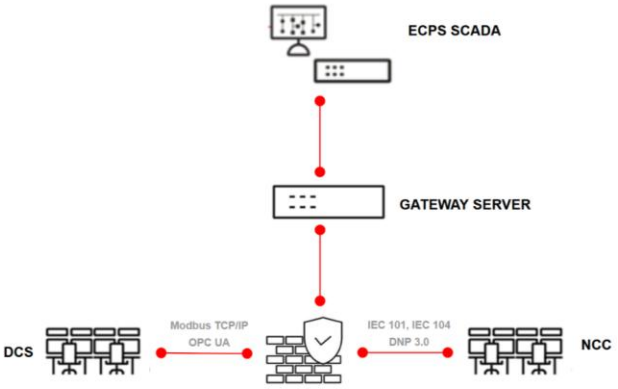



*Figure 10. Dispatch and DCS Interface*

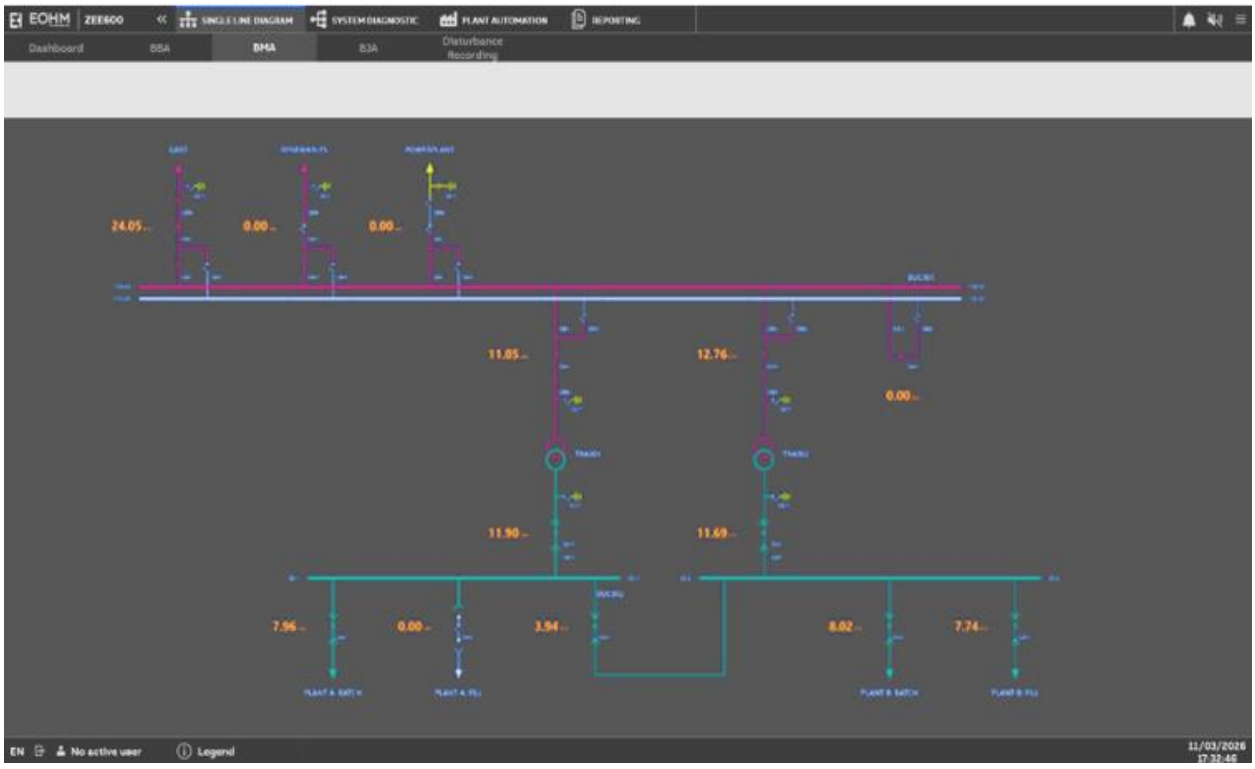
This information can be for alarm indication or for visualization in the cases where the corresponding SCADA are not located in the same control room. When required, it also enables the exchange of process signals with dispatch center through the ECPS interface.

The gateway is in charge of managing these communications with plant control system which are normally done through the protocol OPC UA or MODBUS TCP/IP.

## Dispatch Communication

The gateway/server manages communication with the supervision level and enables the exchange of signals not only with the ECPS HMI, but also between the ECPS and dispatch, as well as corporate control centers, through a dedicated communication bus based on dispatch protocol requirements (e.g., IEC 104, IEC 101, DNP3).

Data exchanged with dispatch is typically agreed with the Transmission System Operator (TSO) or other competent electrical authority and usually includes generation and HV bay information, although additional process data may also be transmitted.



# 5 – Centralized Protection

## New approach to C&P

To date, microprocessor-based relays have dominated substation protection systems. A new approach to distribution network protection and control introduces a software-driven architecture that centralizes core functionalities in a Centralized Protection & Control (CPC) device.

In this concept, protection, control, and supervision are integrated into a single device, enabling a more streamlined and intelligent architecture. By concentrating P&C functions within a CPC device, communication networks enable information exchange between components, bays, substations, and operators.

## Flexibility and system evolution

CPC provides high flexibility, allowing utilities and operators to adapt to evolving power network environments. The system can be expanded with minimal engineering effort.

This approach also extends the lifecycle of the installation, as protection schemes can be updated in line with technological developments. Maintenance is simplified, reducing downtime through easier device replacement and limited engineering effort.

## Hardware/Software Modularity

A modular software architecture allows users to build solutions tailored to specific requirements. Based on a licensing concept, additional functionalities can be integrated at any time. Continuous access to software updates enables system modification or upgrades throughout its lifecycle, maximizing asset value. Engineering is simplified, as configuration and modifications are performed on a centralized device rather than across multiple bay-level P&C devices.

## Merging Unit concept (MU)

A Merging Unit (MU), compliant with IEC 61869-13, acts as the interface between instrument transformers and protection or CPC units. It converts signals from CTs, VTs, sensors, and binary inputs into time-synchronized digital data transmitted via IEC 61850.

The MU provides sampled measurement values (typically 4 kHz for 50 Hz systems) and can handle feeder I/O signals, reporting primary equipment status and receiving trip or switching commands via the station bus.

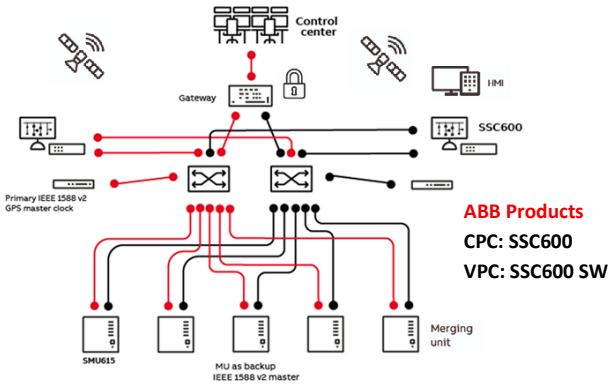



*Figure 11. Example of redundant CPC architecture*

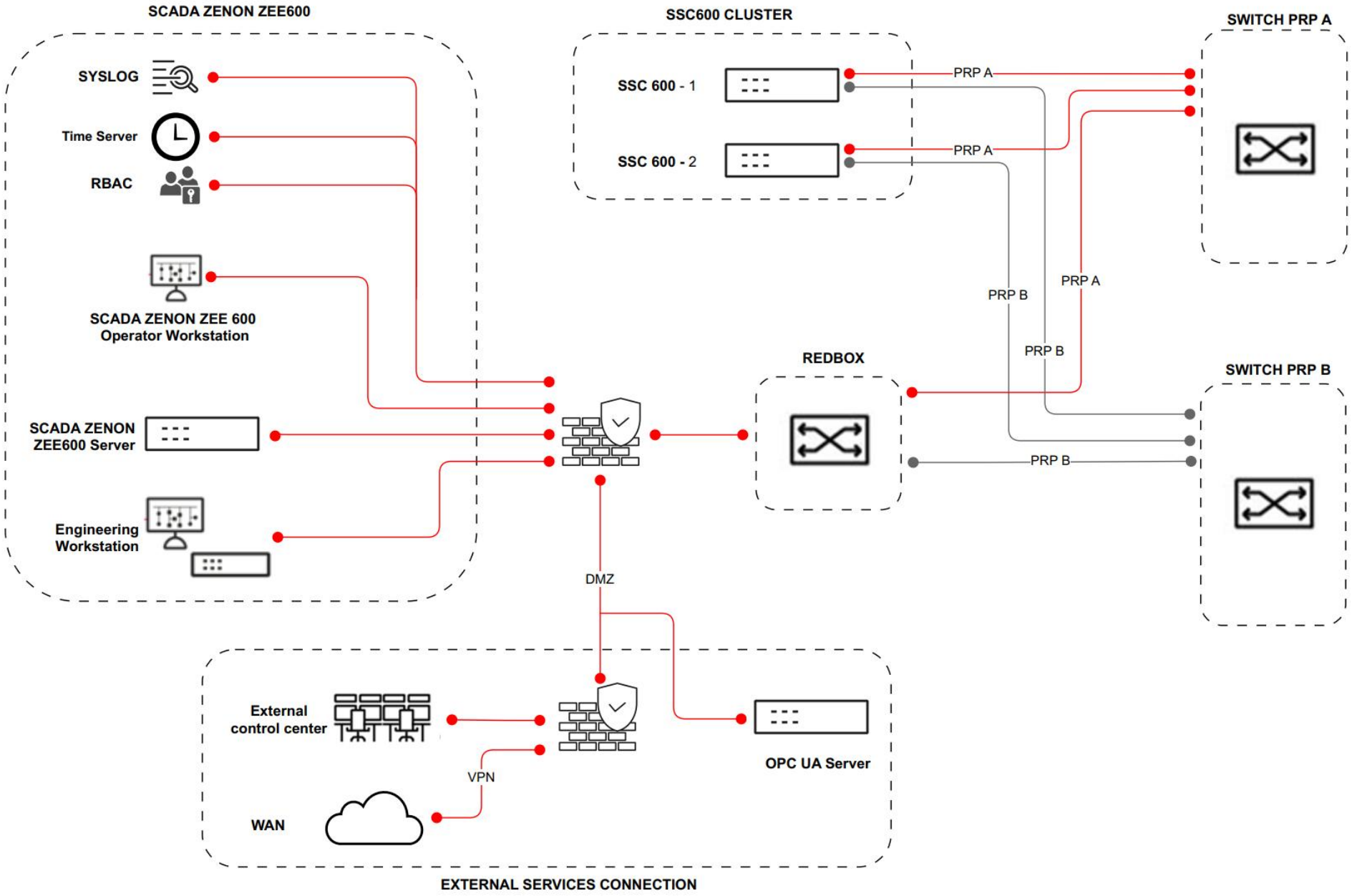
## Virtualization Technology

Virtualization, widely used in information technology (IT), is now being adopted in substation CPC systems, enabling virtualized protection and control platforms (VPC). Hardware virtualization (HWV), kernel-based, and OS-level techniques can achieve the deterministic performance and reliability required for protection and control (P&C).

Real-time performance requirements can be met using both virtual machines (VMs) and containers. HWV provides strong isolation, while OS-level containers offer lower overhead.

Virtualization enables flexible software deployment, execution, and updates within substations, simplifying maintenance and supporting multi-vendor environments.

## Typical CPC Control Architecture



# 4 – Summary and Conclusions

The **digital transformation** of industrial electrical systems is accelerating the transition from conventional hardwired solutions to intelligent, communication-based **architectures built around IEDs**. By reducing wiring complexity, the implementation of an Electrical Control and Protection System (**ECPS**) integrates protection, control, monitoring, and automation into a single platform, enhancing **flexibility, efficiency, and maintainability.** This approach enables **centralized and virtualized system**, enhancing cybersecurity posture and preparing industrial electrical systems for future operational and regulatory requirements.

1

## IED and Electrical Data Highway

### Architecture Based on IEC 61850

The ECPS is built on the IEC 61850 substation automation standard, enabling interoperable communication between Intelligent Electronic Devices (IEDs) and providing an integrated platform for protection, control, monitoring, and supervision across HV, MV, and LV systems.

## Protection & Control 2

### IED-Based Control Architecture

The system is built on a multi-level architecture in which Intelligent Electronic Devices (IEDs), communication networks, and supervisory systems interact to provide integrated protection, control, monitoring, and data exchange across the electrical installation.

3

## SCADA

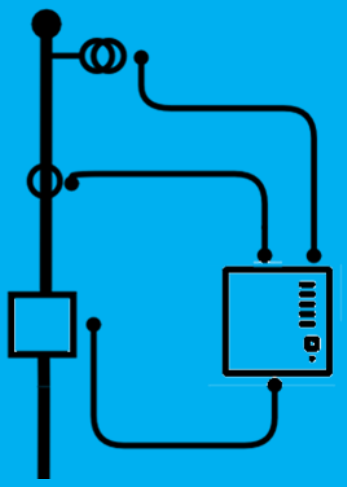
### Supervisory Control and Data Integration

Provides comprehensive monitoring, control, and analysis of the electrical system, integrating IED supervision, alarm management, fault analysis, data logging, and seamless communication with the plant DCS and external systems

## Benefits 4

### Integrated, Flexible, and Digitalized Electrical Control

Enables seamless multi-vendor supervision and decentralized logic through digitalized IED interfaces, supporting high-speed, plant-wide control while significantly reducing wiring, space, and costs.



The electrical system of a plant is more than infrastructure: it is the heart of its operation. At **EOHM**, we help industrial organizations evolve their protection, control, and supervision systems toward smarter, more integrated, and reliable digital architectures. We ensure that technology enhances stability, efficiency, and confidence in every operational decision.

**A smarter electrical system also means being safer and more resilient, ready for the future.**

**Let's build it together.**

**eohm@eohm.es**

EOHM
Everything Engineering

**www.eohm.es**



ABB
VALUE PROVIDER