Digital Secondary Systems

Digital secondary systems—also called digital substations—use IEDs and digital communications to protect, monitor, and control a substation’s primary equipment and power lines. These systems offer many benefits in both the control house and the substation yard, including:

- Secure data concentration, event collection, system visualization, and engineering access to improve situational awareness and asset management.
- Reduced engineering cost per project through reproducible system designs that can be applied across new and existing substations.
- Improved system availability and extended maintenance intervals through self-diagnostic tests and alerts when a failure or an abnormality is detected in the secondary system.
- Replacing long runs of bulky copper wiring in the substation yard with a small number of fiber-optic cables, which carry no current and are immune to electromagnetic interference.

Digital secondary systems provide comprehensive protection, monitoring, and control functions in the substation.

Process Bus Solutions

We provide process bus systems that are engineered to meet your system requirements and operational goals.

See our process bus solutions

Our Services

We have decades of experience designing, installing, and supporting process bus systems.

Partner with us to get it done

Our Support

We strive to be not just a vendor, but a partner you can rely on.

See how we support our customers
Lower construction and maintenance costs due to reduced copper wiring and simplified field wiring, as well as fewer safety incidents and wiring-related malfunctions.

Digital Secondary System Overview

Digital secondary systems can be composed of both process bus and station bus communications. Each is a separate but overlapping and interconnected communications system designed to perform different functions in the substation.

Complete Digital Secondary System

Station Bus Communication

Process Bus Communication

1. **STATION-LEVEL DEVICES**
   Automation controllers, computers, and communications devices that provide data collection, HMI visualization, secure engineering access, and communications with SCADA.

2. **BAY-LEVEL DEVICES**
   Relays and other IEDs that receive process-level data and perform protection, monitoring, and control actions.

3. **PROCESS-LEVEL DEVICES**
   IEDs that digitize and transmit process-level data, such as voltages, currents, breaker status, alarms, and temperature. They also send breaker trip or close commands.

4. **PRIMARY EQUIPMENT**
   Power system equipment used to generate, transform, transmit, and distribute electrical power, including generators, instrument transformers, breakers, and switches.
1. **HMI**
   HMs that provide local system visualization of device statuses and alarms as well as the ability for users to issue local control commands.

2. **SUBSTATION GATEWAY**
   Automation controllers that provide protocol conversion, data concentration, and a cybersecurity access point for communicating with SCADA or other remote systems.

3. **SCADA COMMUNICATIONS**
   Automation controllers and communications devices that send data and receive control signals from Supervisory Control and Data Acquisition (SCADA) or other remote systems.

4. **ENGINEERING ACCESS**
   Local access for engineers or other personnel to configure, test, and collect data from substation IEDs.

5. **STATION BUS NETWORK**
   Communications devices, such as Ethernet switches, that secure and route communications between bay-level and station-level devices.

6. **PROTECTION AND CONTROL DEVICES**
   Relays and other IEDs that receive process-level data and coordinate protective actions and control.
commands in response to faults or other system events.

**PRECISE TIME SYNCHRONIZATION**
Time sources, such as satellite clocks, that maintain precise time with GPS signals and distribute it to IEDs using the Precision Time Protocol (PTP) or IRIG-B protocol, ensuring data synchronization.

**RELAYS IN THE YARD**
Rugged protective relays placed in outdoor cabinets near primary equipment to reduce copper wiring in the substation yard.

**PROTECTION AND CONTROL DEVICES**
Relays and other IEDs that receive process-level data and coordinate protective actions and control commands in response to faults or other system events.

**PRECISE TIME SYNCHRONIZATION**
Time sources, such as satellite clocks, that maintain precise time with GPS signals and distribute it to IEDs using the Precision Time Protocol (PTP) or IRIG-B protocol, ensuring data synchronization.

**PROCESS BUS NETWORK**
Communications devices, such as Ethernet switches, that secure and route communications between process-level and bay-level
Station Bus Systems

Station bus communications are used for substation automation schemes, SCADA communications, secure engineering access, local HMI’s, and more. Station bus systems facilitate the monitoring and control of primary and secondary systems.

Process Bus Systems

Process bus communications enable digital devices in the yard to transfer status signals and primary system measurements—like voltage, current, and breaker status—to protective devices in the control house. The devices in the yard, such as merging units, interface directly with primary equipment to measure and digitize process-level data at high speeds as well as receive and act on control signals transferred from relays.

Process bus systems can also be applied as part of a centralized protection and control (CPC) solution.

Common Elements and Structures of Process Bus Systems

Digital communications over a network or direct connections allow devices to share process-level information from primary equipment and coordinate protective actions. Networked communications must have appropriately high bandwidth, low latency, and maximum availability.
Merging units (or process interface units) convert analog signals from primary equipment to digital data, then transmit those data to protective devices over fiber-optic cable. Merging units may be standalone devices that perform A/D conversion then stream the data, or they may be intelligent merging units that perform local logic and protection. Merging units may also actuate field devices because of local decisions and perform D/A conversion of signals received in digital messages.

Protective devices analyze signals sent by the merging units and send command signals back to the merging units. Time synchronization is necessary when protection data are gathered from multiple points.

Ancillary data, such as temperature, status, and alarms, are collected by other digital devices and made available to protective devices through direct connections or a substation network.

SEL Process Bus Solutions

SEL offers process bus solutions with two different methods of exchanging control signals and sampled analog values from primary equipment:

- Sampled Values (SV)-based systems that use IEC 61850 SV, GOOSE, and Precision Time Protocol (PTP) protocols.
- Time-Domain Link (TiDL)-based systems that use the SEL T-Protocol.

These systems can be applied within the same substations and use other digital devices and protocols for ancillary data and station bus communications. Alternatively, SEL relays can also be installed directly in the yard to achieve many of the same benefits as a process bus solution, such as reduced copper cabling.

<table>
<thead>
<tr>
<th>SV-Based Process Bus</th>
<th>TiDL-Based Process Bus</th>
<th>Relays in the Yard</th>
<th>Ancillary Process Bus</th>
</tr>
</thead>
</table>
IEC 61850-9-2 SV-Based Process Bus

SEL SV-based solutions are based on the IEC 61850 standard and compatible with the IEC 61869 standard to maximize flexibility and interoperability.

Intelligent merging units with built-in protective functions digitize analog signals from primary equipment and publish them using the IEC 61850-9-2 SV protocol to subscriber IEDs, over a switched network or direct connections. Merging units and IEDs exchange information bidirectionally using GOOSE messages that convey the trip commands and other control signals, status and health of equipment, bus configuration, breaker status, and alarms. Sampled analog values are time-synchronized using PTP. Duplicate networks may be implemented using the Parallel Redundancy Protocol (PRP) to improve communications availability.

Learn More About SV-Based Process Bus Solutions

---

SEL TiDL-Based Process Bus

SEL TiDL solutions use point-to-point direct connections and the time-deterministic SEL T-Protocol to exchange both sampled analog values and control signals, creating a simplified, robust process bus solution.

SEL-TMU TiDL Merging Units perform A/D conversion and stream protection data to TiDL-enabled relays, which send control signals to SEL-TMU devices, all using the SEL T-Protocol. Because the SEL T-Protocol is time-deterministic, it doesn't require any external time sources to synchronize protection data. The system may use additional protocols for ancillary data and communication between relays.

Learn More About TiDL-Based Process Bus Solutions

---
SEL Relays in the Yard

Placing relays in the substation yard, as close to the primary equipment as possible, is a simple, low-cost way to achieve many of the core benefits of a process bus system—like eliminating long runs of copper wire—without the need for additional devices. Rugged SEL relays are designed to operate in temperatures from –40° to +85°C (–40° to +185°F) and have a decades-long track record of reliable performance in harsh substation environments. Customers all over the world have implemented SEL relays in outdoor cabinets with excellent results. Additionally, relays in the substation yard may be integrated into station bus communications and use a wide range of protocols for data collection, engineering access, and system visualization from the control house. They may also exchange protection signals and interlocks with other relays.

Learn More About Relays in the Yard Solutions

Ancillary Process Bus

Process interface units and communications technologies augment protection-related merging units by digitizing data other than the primary equipment voltage and current. Ancillary process bus solutions support other process bus designs, and they can be used for control and tripping on their own.

Ancillary process bus communications use many protocols for different data. Binary status, alarms, controls, and calculated analog values are transmitted using SEL MIRRORED BITS communications and IEC 61850 GOOSE, while SEL-2600 RTD Module messages are used for temperature data. Applications use IEC 61158 EtherCAT for a variety of data, like oscillography and synchrophasors. (EtherCAT® is a registered trademark and patented technology, licensed by Beckhoff Automation GmbH, Germany.)
Design Considerations for Process Bus Systems

Process bus implementations should minimize complexity wherever possible. To meet this goal, a design must consider interoperability, networking, time synchronization, cybersecurity, and any necessary ancillary data collection.

Interoperability

A substation may include process bus systems using a variety of protocols. The IEC 61850 standard, which defines protocols like IEC 61850-9-2 SV and GOOSE messages, helps ensure that devices from various suppliers use a common set of protocols and function together in a process bus system. SV-enabled relays also communicate with TiDL-enabled relays and other devices over station bus communications using common protocols. This flexibility allows substations to integrate process bus systems with a variety of station bus protocols, such as DNP3, FTP, Telnet, HTTP, IEC 61850 MMS, and GOOSE.

Communications

Process bus communications must satisfy rigorous privacy, security, and performance requirements. A strong cybersecurity posture is required to prevent unauthorized access to systems protecting critical infrastructure.

Because relays and merging units are in constant communication, process bus networks must have a high bandwidth and fast failover times to ensure that control commands are delivered at protection speeds. Direct connections, such as those used in TiDL systems, meet performance and security requirements for protection communications without requiring network engineering.

Networked, Ethernet-based systems meet performance requirements using methods such as VLANs to segment traffic, the SEL operational technology (OT) software-defined networking (SDN) solution to achieve fast failover times, and duplicate networks with the PRP protocol to ensure availability. While traditional PRP duplication technology may mask failures and introduce “dangerous undetectable faults,” as defined by IEC 61508, SEL PRP enhancements detect and self-alarm message failure, prompting corrective action and improving reliability.

Learn More About OT SDN

From our knowledge base:

- Using Software-Defined Networking to Build Modern, Secure, IEC 61850-Based Substation Automation Systems
- Improve Protection Communications Network Reliability Through Software-Defined Process Bus

Time Synchronization

Networked process bus systems require time-aligned protection data to generate trip and control signals that are both accurate to the nature of a fault and timely to the occurrence of a fault. Accurate time synchronization may be achieved via external satellite clocks and PTP or IRIG-B protocols.

Using deterministic, nonroutable protocols—such as the SEL T-Protocol used in TiDL systems—synchronizes the sampled analog data coming from merging units, removing the need for an external time source to distribute time to the merging unit.

From our knowledge base:

- Growing Your Time Synchronization Solutions
Cybersecurity

Cybersecurity is a vital consideration in process bus systems. However, because OT and IT systems have different purposes, the cybersecurity solutions for one may not be the most appropriate for the other.

**PRESERVE AVAILABILITY WITH PRIVACY METHODS**

Networks use privacy methods to preserve the availability of data and restrict access. Direct connections provide privacy by physically isolating communications paths, while SDN solutions provide privacy by denying all network communications that do not match a predefined set of rules. In traditional Ethernet architectures, security gateway devices deny access to outside traffic using features like a VLAN, a VPN, firewalls, virus and malware detection, password management, and user-based access permissions.

Private links between devices enable immediate detection of intentional or unintentional disturbances to data flows. Devices that detect these disturbances may issue alarms or perform automatic corrective action to maintain privacy.

SEL SDN technology is purpose-engineered to meet the cybersecurity requirements of OT applications, such as process bus networks.

**SECRECY METHODS REDUCE AVAILABILITY**

Network connections that are not engineered to maintain privacy often require coordinated secrecy methods like TLS within each device to obscure data, generally by encryption, making them unreadable to other devices and unauthorized users. This method is undesirable in secondary systems because the additional processing load and time required to encrypt and decrypt data can slow protective action. Encryption also makes data unavailable to engineers, technicians, other devices, and systems that lack the appropriate decryption capabilities.

In addition, the increased frequency of firmware updates required to stay current with secrecy technologies poses a serious obstacle for maintaining system availability, requires that devices be updated simultaneously, and introduces new supply chain and personnel vulnerabilities. Unintended consequences that affect protection reliability include device down time during firmware upgrades to address security vulnerabilities and a lack of communications among devices until they are all upgraded to the same firmware version.

**From our knowledge base:**

- Do IT Cryptographic Security Controls Work for Energy Systems?
- Defense-in-Depth Security for Industrial Control Systems

**Ancillary Data**

Protection, control, and monitoring devices collect and digitize data such as temperature, status, alarms, and more to supplement the digitized current and voltage data provided by merging units.

Most SEL protection, control, and monitoring devices support traditional CT/PT and digital message inputs, and many SEL devices also support low-energy analog (LEA) and Rogowski coil inputs. These devices can publish this information via digital messages to other IEDs as needed.

**SEL Engineering Services**
Digital secondary system implementations can be as simple or sophisticated as an application demands, but many important factors must be considered in designing the system.

Partner with SEL Engineering Services to create a turnkey solution that addresses the needs of your system and puts you in control. SEL application engineers provide thorough training in all products applied in a solution, ensuring that you are able to achieve your operational goals once a system is in place.

<table>
<thead>
<tr>
<th>NERC PRC COMPLIANCE SERVICES</th>
<th>CYBERSECURITY NERC CIP COMPLIANCE SERVICES</th>
<th>CYBERSECURITY CYBERSECURITY SERVICES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partner with SEL to meet NERC PRC standards and streamline compliance processes.</td>
<td>Partner with SEL to meet NERC CIP cybersecurity standards and streamline compliance processes.</td>
<td>Partner with SEL to design, implement, or audit the cybersecurity framework for your application.</td>
</tr>
</tbody>
</table>

**Our Support**

We've collaborated closely with our customers since the company was founded over 40 years ago—a major reason why we're North America’s most trusted provider of protective relays and ranked #1 by international utilities in price, service, and support.

**The Industry’s Best Warranty**

SEL devices are designed for a working life of at least 20 years, and every SEL-manufactured device comes with a ten-year warranty—the best in the electric power industry. If it fails under warranty, repair and replacement are free. We always do all that we can to repair any returned product, whether it meets our warranty or not.

**RUGGED AND RELIABLE—GUARANTEED**

SEL products are designed and manufactured for the world’s most challenging environments, exceeding all industry standards for temperature, shock, and electric stress. An optional conformal coating for circuit boards adds an extra level of protection against contaminants in extreme environments.

Our products have a mean time between failures (MTBF) of more than 700 years, based on observed field performance. This means that if you have 700 SEL products installed in your systems, you can expect to have less than one device fail per year for any reason, whether it’s a defect or an external factor such as overvoltage, overcurrent, wildlife damage, or environmental exposure.
Every device we manufacture comes with free lifetime technical support. SEL support teams are stationed in regional offices around the world and staffed with application engineers who are experts in our products and in power system applications.

No matter how often you need to call or how long your SEL products have been in service, our customer service and technical support professionals are ready to help.

SECURITY BULLETINS AND UPDATES
We notify product owners of updates and security patches for the full life of the product. Software and firmware updates are distributed directly to our customers via secure file transfer, and their authenticity and integrity are verifiable through digital signatures and cryptographic hashes.

More About Security Notifications

SECURITY BULLETINS AND UPDATES
We thoroughly review and test the code in our products, which allows us greater control over their quality, security, and functionality. Customers are notified of updates and security patches for the full life of every SEL product.

CYBER ATTACK MITIGATION
We freely provide a broad set of cybersecurity best practices that you and your team can begin using immediately to improve the security of your systems and mitigate the risk of a damaging cyber attack. And if you need to meet regulatory requirements or need expert help implementing cybersecurity solutions, SEL Cyber Services professionals are ready to partner with you to get it done.

CYBERSECURITY SERVICES AND SUPPORT
From system assessment and baselining to cyber-defense solution development and ongoing system management, our full suite of security services can help strengthen your defenses and streamline the demands of maintenance and compliance. Cyber services support contracts can include incident response, audits, system hardening, patch/update management, and more, depending on your anticipated needs.

Contact SEL Cyber Services

SEL meets your workforce training and continuing-education needs through seminars, conference and tradeshow presentations, and SEL University courses.
SELU courses and many of our seminars provide Professional Development Hours (PDHs) for maintaining Professional Engineering (P.E.) licenses. Courses and seminars can be delivered in various formats, including self-paced online learning, virtual classrooms, live and recorded webinars, and in person.

We can also work with you to develop training that is customized to the specific needs of your workforce.

**TRAINING AND EDUCATION OFFERINGS**

- SEL University Courses
- Conferences and Tradeshows
- Seminars and Webinars

**DIGITAL SECONDARY SYSTEMS EDUCATIONAL RESOURCES**

- CBT 101: Introduction to SEL Relays
- eCOM 202: Introduction to IEC 61850

Questions? Contact Us!

If you have any questions about SEL products, services, solutions, or support, please contact us. Our service and support professionals are ready to provide the answers you need.

Contact us →

Unbeatable Support

SEL support teams are stationed in regional offices around the world and staffed with application engineers who are experts in our products and in power system applications.

Technical support for SEL-manufactured devices is always free. No matter how often you need to call or how long your SEL products have been in service, you’ll reach an SEL expert who can provide the service and support you need.

Our cybersecurity team is always ready with the information and resources needed to keep your OT networks and critical systems secure and working effectively. Cyber services support contracts can include incident response, audits, system hardening, and more, depending on your anticipated needs.