Applying World-Class Manufacturing Principles as a Strategy When Modernizing Energy Control Systems

David Dolezilek
Schweitzer Engineering Laboratories, Inc.

Introduction

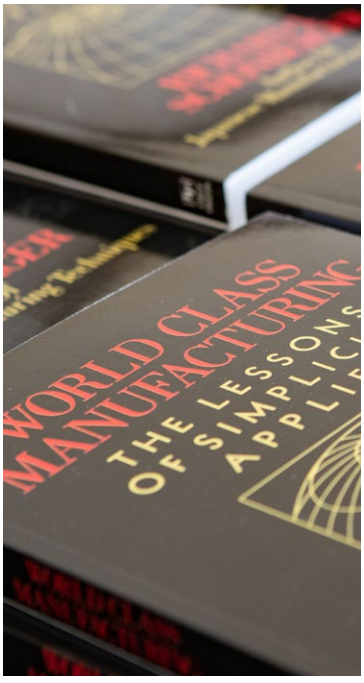
Digital transformation and energy independence are becoming key drivers for various power system investments. At the same time, the total energy consumption in the United States used to generate electricity has been steadily rising over time [1]. This trend is likely to continue, proving that electricity is the fastest and most economical method to transport and distribute energy to many consumers. A resilient energy delivery system (EDS) must be reliable, dynamic, reconfigurable, intelligent, and self-healing.

System-wide energy control system (ECS) communications is an essential component of digitization. Unfortunately, a large percentage of the power system protection devices today are electromechanical relays, which simply cannot communicate. Depending on the installed base, digital transformation updates are also likely to affect a large number of first-generation microprocessor-based relays, digital fault recorders, programmable logic controllers, and supervisory control and data acquisition (SCADA) systems.

Even though protection and control digitization based on engineering processes in communications standards like IEC 61850 will replace many discreet ancillary devices, the work cannot happen overnight. It must be carefully planned, scheduled, and executed to maintain continuous service to customers. We need to intentionally engineer the use of new technologies, new standards, and new industry practices.

The successful use of cable and communications designs in digital secondary systems (DSSs) to replace traditional substation wiring practices is one of the key obstacles to, and opportunities with, large-scale protection and control system updates. As with all engineering challenges, we must carefully manage cost, schedule, and performance of the digital transformation and the skill, knowledge, and growth of our most important asset—our employees.

For many decades, SEL has used world-class manufacturing (WCM) methods with a philosophy of continuous improvement and has helped others drive efficiencies with evidence-based return on investment (ROI). We learn, understand, and teach technical facts to avoid ambiguity and imprecision as we collaborate to create intentionally engineered mission-critical systems.



Digital changes everything

Traditional ECS production systems do not fully capitalize on the innovation potential, digital test and reconfiguration, and end-to-end capabilities afforded by new information, including information at rest, like settings and configuration; information on demand, like controls and reports; and information in motion, like power system measurements, status, and protection signals and interlocks.

To meet their needs, NamPower, with the help of their electrical consulting firm, CONCO Energy Solutions, implemented an SEL automated substation solution. This state-of-the-art solution incorporated advanced power protection, automation, and control, all based on Ethernet communications using the IEC 61850 engineering process and protocols.

A critical element in SEL's IEC 61850 communications scheme was their data modeling flexibility, which enabled a solid system design that flowed easily from concept to implementation. This simplified testing and saved time associated with implementation, test and documentation, all of which positively impacted the overall project cost.

"We are very proud. We know we've done the right thing. These are 21st century solutions, for 21st century substations."

Frank Engelbrecht
Senior Manager: Engineering Services, NamPower

EARLY UCA 2.0 STANDARDIZATION OF DIGITAL DATA FLOW

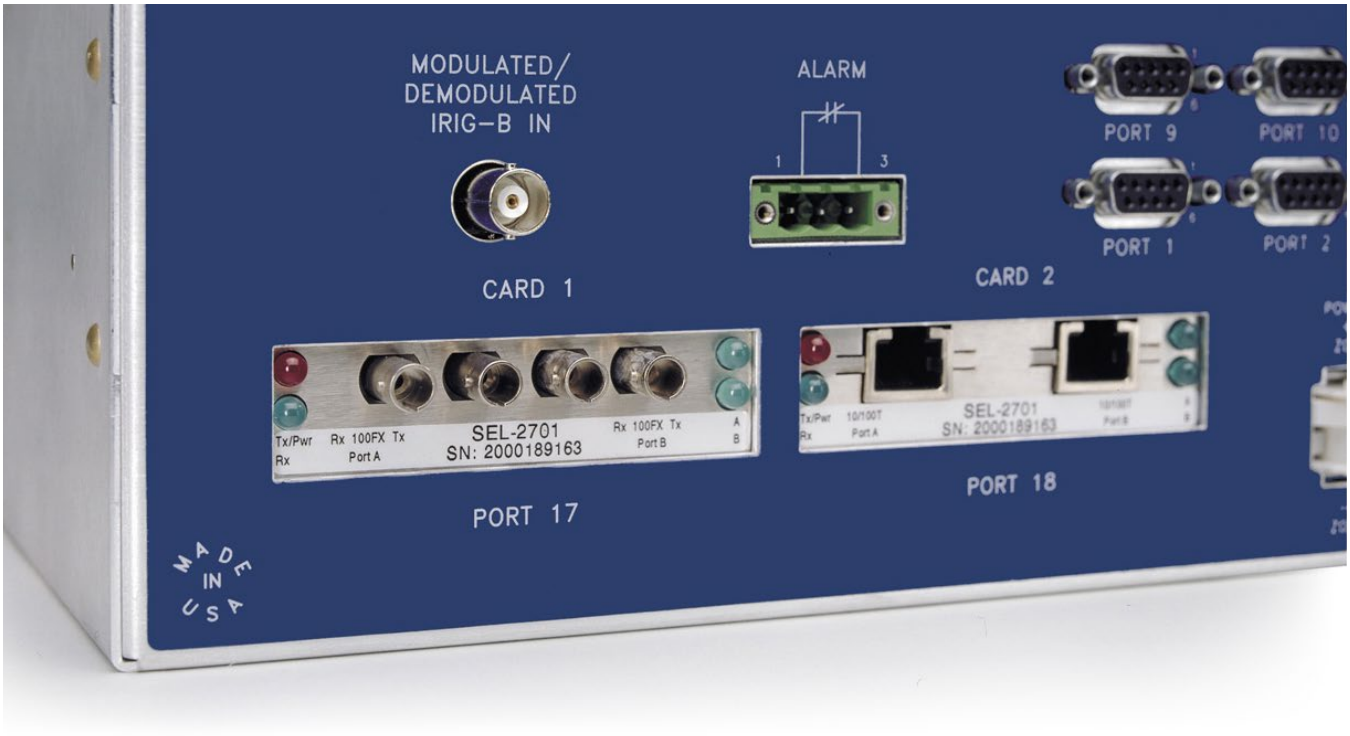
SEL's origins are intertwined with the digital transformation of protection and control (P&C) systems. After inventing numerous station bus and process bus methods in the absence of standards, in the mid-1990s SEL began to collaborate with other suppliers in North America to create the utility communications architecture (UCA) framework. Using proprietary and nonproprietary data exchange methods, UCA encouraged standardized interoperability based on a decentralized, object-oriented philosophy found among applications present in the IT industry. Using early SEL data modeling and autoconfiguration as a template, we added UCA 2.0 object modeling and self-description and UCA point names that follow a logical device model based on object-oriented techniques. Early contributors to UCA 2.0 were P&C, rather than SCADA, technology suppliers because we wanted to leverage data within purpose-built digital protection devices and the ability within IEDs to model the health and behavior of the electric power system.

This work, supported by the Electric Power Research Institute (EPRI) [2], introduced common application service models (CASM), generic object models for substation and feeder equipment (GOMSFE), and the use of manufacturing message specification (MMS) over Ethernet, which became collectively known as UCA 2.0.

In our work with UCA, we specified use of the Open Systems Interconnection (OSI) stack, and the framework defined standardized solutions at the application, presentation, session, transport, and data link layers. From the beginning, the framework allowed any appropriate protocol to operate in the application layer, which assured UCA 2.0's protocol independence. GOMSFE modeling was joined by the choice of TCP/IP at the transport layer and Ethernet at the data link layer. Because the application level is independent from the rest of the stack, the modeled data in that layer doesn't have to be concerned with any other level and simultaneously supports both standard and nonstandard, possibly proprietary, solutions. These abstract services allowed compliant IEDs to connect via any type of underlying purpose-built protocol and physical network and populate the standardized data models and unrestricted applications in the IED.

Compliant IEDs exchange both nonstandard and standardized dialogues with one another over Ethernet and other data links in support of the common data model. SEL understood that services defined by UCA 2.0 would lag supplier innovations and that for us, the goal of true interoperability was not in conflict with the goal of product enhancement. UCA 2.0 became a method to map data associated with frequent SEL innovations to the common models and to document how clients were expected to ask for them.

To make this Ethernet-based data flow a reality, SEL created the first protection-grade deny-by-default interface, the SEL-2701 Ethernet Processor, for use in relays and communications processors. SEL demonstrated interoperability in 2000, where SEL and GE exchanged GOOSE signals, and has worked to organize each interoperability demonstration over the past two decades.



UCA 2.0 becomes the IEC 61850 communications standard

In the early 2000s, to avoid competing global standards, UCA 2.0 allowed the International Electrotechnical Commission (IEC) to rebrand this work as IEC 61850 and several working groups were created to harmonize IEEE and IEC methods. UCA 2.0 remained a technical report, IEEE TR 1550, and members of UCA and IEC collaborated on the initial 10 parts of IEC 61850 to map the UCA 2.0 components, including the OSI stack, CASM, Object Orientation, GOMSFE, MMS, GOOSE, TCP/IP, and Ethernet.

Since that time, numerous versions of the ten parts of the standard have been released, numerous protocols have been added, numerous related standards have been written and referenced, numerous topologies have been developed and deployed, and numerous engineering processes have been defined. IEC 61850 continues to grow and evolve to support new data flow capabilities and increasingly sophisticated communications-assisted automation and protection.

Continuing with the same intention as UCA 2.0 before it, IEC 61850 application and data link levels are protocol-independent and IEDs perform standardized and nonstandardized tasks simultaneously. IEC 61850-compliant IEDs exchange both nonstandard and standardized dialogues with one another over Ethernet and other data links in support of the common data model.

In the past two decades, services defined by IEC 61850 have lagged product supplier innovations and certification has lagged even further. Therefore, proprietary solutions are not only allowed among IEDs from a specific supplier, but also available to other suppliers based on a license agreement written by the owner of the technology. Proprietary simply relates to ownership and in this case is nonstandard and controlled by one supplier. Though the original GOOSE was not made proprietary, other protocols are, such as the parallel redundancy protocol (PRP). Suppliers must enter and follow a license agreement with the owner to use proprietary PRP. However, once this is done, the internal methods and mechanisms to optimize it may remain confidential and private intellectual property (IP) if the company takes reasonable efforts to protect the secrecy of the information. However, this IP and other proprietary methods are often shared with the public in the spirit of improvement of the market, while others remain private to dictate performance and longevity for specific applications.

Getting digital in substations includes IEC 61850

The next generation of digital-based production systems—or DSSs—is alive and well at SEL and many forward-thinking P&C design teams. But even as we leverage the digitization of the secondary system of the ECS based on IED capabilities and resilience, the basics remain crucial.

First principles of the process level, in combination with the utility purpose and focus, should lead to an organized effort directed at analyzing features, systems, equipment, and material selections for the purpose of achieving essential functions at the lowest life cycle cost consistent with required performance, quality, reliability, and safety.

Like others, I call this orchestration, so although we all may have a different favorite music genre, and even enjoy many, ECS design must be like the orchestra—everyone on the same sheet of music, no improvisation, and practice practice practice. Intentional and methodical digitization steers priorities, synchronizes approaches among the different groups, reinforces incremental gains, and sets the targets for improvement and performance objectives of digitized stations. Although best-known methods frequently change as new innovations become available, the underlying first principles do not change. DSS harmonizes P&C with other parts of the business that can make use of the added information and detail. In this way, utilities can anticipate and monitor the value added by digitization. We may prefer rock and roll for individual projects, but a DSS strategy requires a symphony.

GETTING DIGITAL

It should be acknowledged that utilizing data collected from IEDs to realize various protection, automation, and control functions within a design is but a small part of the necessary work to digitize P&C and create a system. A data flow diagram (DFD) shows the source and destination of data, necessary datasets, preferred data link and protocol choices, and processes necessary to perform the applications as well as various restrictions and interdependencies. However, as important as the design and creation of the DFD and application of IEC 61850 engineering processes are, they are often 10–25 percent of the effort required to realize various protection, automation,

and control functions in a DSS. Even though numerous IEC 61850 logical nodes and other features are available by default, other digitization tasks include the following:

- Plan how to replace physical control handles, panel switches, meters, and timers.
- Choose relay, intelligent merging unit (IMU), or both.
- Design relay logic and variable mapping to replace standard operating procedures.
- Plan front-panel custom-commanded control buttons.
- Create front-panel one lines and LED and display values.
- Plan sequential event records.
- Design power system event reports.
- Create DFD.
- Choose station bus and process bus protocols.
- Design datasets for DNP3, MMS, GOOSE, etc.
- Select Ethernet channels.
- Collaborate with IT on IP addresses and with SCADA on IED name.
- Design system signal exchange matrix.
- Learn standard logical nodes (LNs), and interpret and display LN fields that represent aggregations (enumerations).
- Review relay data mapping to IEC 61850; consider custom LNs.
- Remap Relay Word bits and customer logic.
- Compensate for timestamps of change of state from non-SEL MUs.
- Create datasets.
- Design MMS reporting, GOOSE publication, and GOOSE subscription.
- Create GOOSE subscription quality fail strategy.
- Design Sampled Values (SV) publication and SV subscription.
- Design SV network behavior strategy and settings.
- Plan SV failure management and how to use detected communications anomalies to restrict tripping and control.
- Create Precision Time Protocol (PTP) management strategy.
- Design communications system event reports.
- Plan simulation mode management.
- Plan SV test mode management.
- Plan IEC 61850 test mode management.
- Design systemic and IED cyber-defense strategy (third-factor authentication settings).
- Plan PRP management and fault detection strategy.
- When finished, revisit front-panel design to add useful display points.

The first step, then, is to evaluate your company's state of digital maturity and readiness for DSS and consider 11 key assessment areas:

1. Strategy—Consider whether digitization is comprehensively planned and included in corporate objectives.
2. Leadership—Transformation requires a champion with an all-digital or digital-hybrid vision, compellingly and consistently communicated.
3. Design—Organizational structures should shift from siloed to cross-functional and universally support the digitization and should use RACI (responsible, accountable, consulted, and informed) to decide how to manage participation.
4. Data—Plan how to use insights from DSS data gathering and analysis to drive value, or don't collect it.
5. Technology—The scale and pace of technology adoption, including plans for IEC 61850, is a benchmark indicator of digital maturity (e.g., protection logic, automation logic, I/O mapping, SER, display points, data flow design, datasets, protocols, and fiber optics).
6. Innovation—Gauge the company's culture around the adoption of digital innovation and tools. Examples include operational technology [OT] Ethernet LAN, IEEE 802.1 STA or software-defined networking (SDN); Ethernet messaging, IEEE 802.1 VLAN/MAC/priority; PTP; and IEC 62439 Ethernet duplication or redundancy.
7. Ecosystem—Assess the extent of digital alignment with tools and processes, and replace physical tools and visible wiring with laptops, software, and invisible wires.
8. Capability—Digital transformation forges new skills, but staff will require ongoing training and development programs and new job descriptions and performance measures.
9. Process automation—Once the ECS design is complete, it can be reproduced with much less effort and even automated; however, design changes will shorten the technical life cycle and jeopardize the gains made.
10. Self-evaluation—Consider how to make design choices based on established engineering methods, including:
    a. ANSI ASTM E1699-14 Value Engineering—Improve operations, reduce costs, and substitute materials and methods that are less expensive while preserving or improving functionality, reliability, and serviceability based on performance-based specifications.
    b. IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems—Reduce the probability of the failure of systems remaining in service. Do not create a new system less reliable than one that it replaced. Differentiate between dangerous detected failures and dangerous undetected failures. Use design tools and processes to make evidence-based decisions.
    c. U.S. Department of the Army Limited Vulnerability Design (LVD)—Ensure maximum functionality and performance of the ECS by preventing or reacting to natural and man-made failure events. Protect against malicious attacks intended to interrupt the system.
        i. Identify and investigate design gaps.
        ii. Recognize vulnerabilities associated with design gaps.
        iii. Recognize risks associated with vulnerabilities.
        iv. Limit vulnerability based on cost, schedule, and performance design choices.
11. Cybersecurity—Physical and cybersecurity of the DSS, and data within it, should be designed into the ECS system at every level. Care should be taken to defend against supply chain issues and to minimize cybersecurity risks.

Your digital roadmap

Assessing your status on these 11 themes will help prepare for your work towards a mature DSS design. You will need to synchronize the deployment of skills, technologies, new processes (plus improvements to existing ones), updated analytics, key performance indicators, and serviceability of field systems.

The complexities of transitioning to DSS should not be underestimated. We have seen companies succeed in a design and fail in execution because they did not satisfy field staff. We have seen companies succeed with a design that involved all affected groups but failed because key staff left and there was no backup. We have seen companies succeed with a design that involved all groups but failed because it was impossible to confirm operation and diagnose and service the DSS. Success hinges on instilling the use of data, information, and updated technologies.

Not all IEDs are appropriate for this process. IEC 61850-4 states that the customer is responsible for ensuring that the relevant environmental and operating conditions of the system satisfy the conditions described in the technical documentation of the system and its individual products.

Apply WCM methods to your digitization design

In the end, successful digitization is the result of collaboration among the personnel divisions responsible, accountable, and affected by the new technology and the integration of the selected technologies and standards. As in WCM, the design team, led by digital champions, will need to manage the quality of the design by controlling the outcome of the process and by monitoring each step.

- Requirements—What does the company need the solution to do?
- Risks—What are the possible failure modes of the selected design?
- Identify, measure, and improve (IMI)—What internal monitoring and control is necessary to keep the design successful in service?
- Gaps—What are the gap and alignment requirements for each team member and technology to maintain success?

A powerful lesson learned from WCM is that “tolerance stack-ups” by individuals may lead to a poor design or poor system performance even after a thorough and collaborative design effort. In short, design choices found tolerable by each group may eventually aggregate and “stack up” to an intolerable level.

In hardware development, we may ask, “Do the parts that make up the assembly always go together?” In the traditional ECS example, we would analyze the performance of mechanisms, like switches, latches, actuators, and the like.

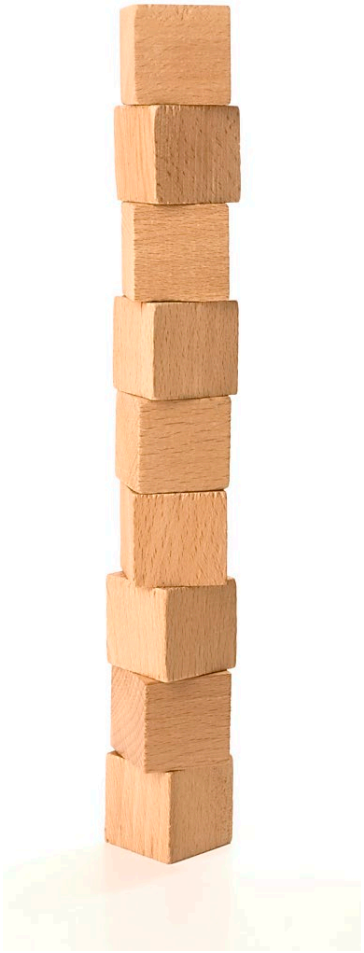
Tolerance stack-up represents the cumulative effect of part tolerances. The idea of tolerances stacking up refers to choices that individually meet their purpose, but when combined with other choices, the deviation from the design goal becomes too large.

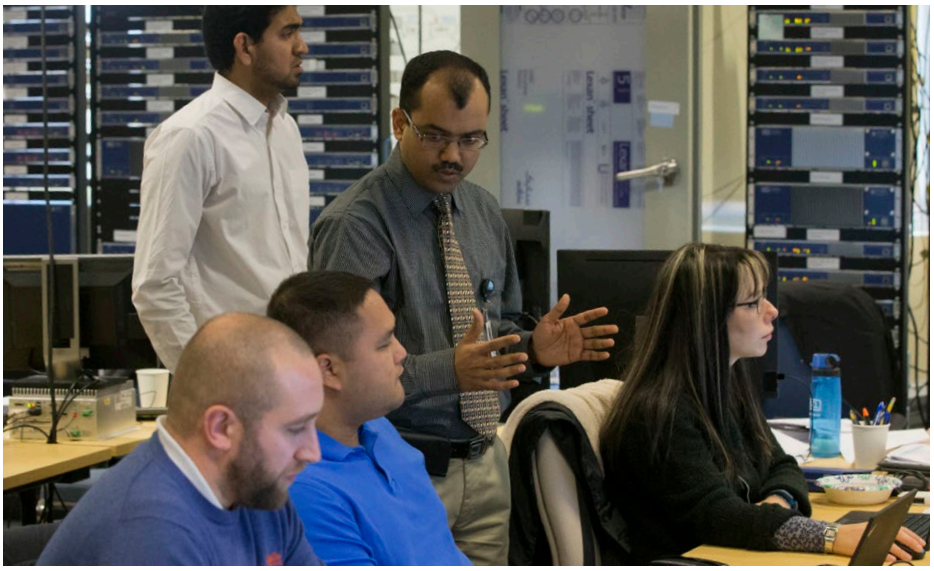
Below are some examples of individual team member choices that appear low-risk but cause design failure due to tolerance stack-up in DSS:

- Once the choice to use PTP is made, the other communications devices need to support it. Inexpensive media converters may be attractive to the fiber team to cut costs to connect IEDs to the fiber network, and their inability to participate in PTP will be invisible to the fiber-optic installation team. However, the physical delays these devices introduce will cause errors in time-synchronization algorithms, and the stack-up will result in failed IEC 61850-9-2 SV protection.

  Additionally, IT Ethernet switches may be attractive to the networking team, but they likely do not calculate and update network time inaccuracy in the PTP frames. When this field is not correctly updated in the PTP frame and not updated within the switches, the IEDs will be unaware of the stack-up of undetected time inaccuracy. Once the disparity grows large enough, the IED compensation methods will no longer work, SV-based protection will fail, and root cause will prove elusive.
- Once the choice to use private Ethernet connections is made, the fiber-optic layout and IED settings assure that access is secure and appropriate. Though an OT SDN network denies unwanted traffic and IEDs detect disturbances in data flow, IT staff often promote the use of secrecy. IT staff often accept the 24-month lifespan of secrecy mechanisms like TLS, but this will create an intolerable stack-up of field firmware changes and low mean time between removals (MTBR) in contrast to the 30-year design life of the protection system.
- Error detection is the key to rapid corrective action and service restoration to support an N-1-1 (two failures consecutively) or N-2 (two failures simultaneously) EDS. This also requires an ECS design with similar N-1 or N-1-1 availability. However, Ethernet switch and IED selection that cannot support that availability often lead IT or protection staff to choose replication of communications via IEC 62439-3 PRP message duplication. PRP may satisfy the desire to duplicate messages, but the lack of fault detection creates a predicted unavailability stack-up too large for the EDS and prohibits preventative repair before an outage. A collaborative approach often leads to selection of IEC 62439-1 Rapid Spanning Tree Protocol (RSTP) or SDN with fault detection and reconfiguration to quickly restore message delivery.

Many companies utilize a statistical method for tolerance analysis by summing tolerances as part of a worst-case analysis. The input values for a worst-case analysis are design tolerances and that worst-case analysis, also called tolerance stack-up analysis, is used to validate a design. Not all stack-up is avoidable, or destructive, but collaboration between team members will be required to understand the impact [3].





Pursue ECS design team role-based accountability

As mentioned previously, by using the RACI matrix the design team not only makes each team member's roles and responsibilities clear, as illustrated below, but also clearly shows who was accountable for making specific design choices.

ROLE	RESPONSIBILITY
Responsible	Performs the work of completing the task. Each task has at least one responsible party.
Accountable	Delegates work and performs final review and approval. An individual may be both responsible and accountable, but there is only one person accountable for each task.
Consulted	Is recruited by the other team members for review and consultation. Consulted party is an SME and/or is a user who will be affected by the design.
Informed	Is not responsible for the project but is kept informed of its progress.

RACI matrix

At its core, a RACI matrix helps set clear expectations about project roles and responsibilities. Having tasks clearly defined at the beginning of a project prohibits the conflict of having multiple people working on the same task or against one another. When using the RACI matrix, teams can encourage individuals to accept responsibility for their work and, in some cases, defer to others when they recognize a skills gap. It is a useful tool to depersonalize the process of selecting the right team members and assign roles, responsibilities, and accountability more effectively [4].

Call to action

Together, our mission is to achieve deterministic designs and proof-based certainty of performance of these systems. Although SEL offers many great inventions and innovative solutions, DSS does not require complete technical disruption, but rather a dedicated and educated workforce willing to do the mundane hard work of engineering as well as gain and retain thorough product knowledge and a deep understanding of the first principles of ECS. Digital transformation is based on science, technology, and engineering, so conclusions must be based on evidence and success will be based on use of the scientific method. In short, teams should collaborate on three activities.

1. Do everything that is known to satisfy cost, schedule, and performance while making the new design work correctly based on fault avoidance metrics in the VE process.
2. Though attempts were made to remove it, anticipate failure and design resilience and fault tolerance based on LVD processes and monitor the design process and the digital design itself to detect and remove vulnerabilities.
3. Finally, if in the end something isn't right, identify the concern, contain the problem, and collaborate on a design change when the value of its impact is larger than the cost to change based on LVD.

References

[1] U.S. Department of Energy, "GridWorks: Overview of the Electric Grid." Available: https://web.archive.org/web/20160327222928/http://sites.energetics.com/gridworks/gridworks_pdfs.zip.

[2] Electric Power Research Institute (EPRI), "Utility Communications Architecture (UCA (TM)) Version 2.0," December 1999. Available: https://www.epri.com/research/products/TP-114398.

[3] R. J. Schonberger, *World Class Manufacturing: The Lessons of Simplicity Applied*, Free Press, New York, NY, 1986.

[4] A. McDonald, A. Dolezilek, and D. Dolezilek, "Hidden in Plain Sight: Anticipating and Avoiding Hidden Failures in Communications-Assisted Protection," proceedings of the 47th Annual Western Protection Relay Conference, Spokane, WA, October 2020.

Biography

David Dolezilek is a principal engineer at Schweitzer Engineering Laboratories, Inc. (SEL) and has three decades of experience in electric power protection, automation, communication, and control. He develops and implements innovative solutions to intricate power system challenges and teaches numerous topics as adjunct faculty. David is a patented inventor and continues to research and apply first principles of mission-critical technologies. He has authored over 80 technical papers, many based on the practical use of IEC 61850 engineering processes, and has taught digital transformation of energy control systems in over 50 countries. David is a founding member of the DNP3 Technical Committee (IEEE 1815), and as a founding member of UCA2, he helped migrate that work to become the IEC 61850 Communications standard. As such, he is a founding member of both IEC 61850 Technical Committee 57 and IEC 62351 for security. He is a senior member of IEEE, the IEEE Reliability Society, and several CIGRE working groups.

SEL SCHWEITZER ENGINEERING LABORATORIES

info@selinc.com	selinc.com	LWP0036-01	20211101