

**Protection and Control System Impacts from The Digital World**  
**presented to**  
**2015 Western Protective Relay Conference**  
**Spokane, Washington**

Steven Kunsman  
ABB Raleigh, NC, USA  
[steven.a.kunsman@us.abb.com](mailto:steven.a.kunsman@us.abb.com)

Stefan Meier  
ABB Switzerland, Switzerland  
[stefan.meier@ch.abb.com](mailto:stefan.meier@ch.abb.com)

Roger Hedding  
ABB Raleigh, NC, USA  
[roger.hedding@us.abb.com](mailto:roger.hedding@us.abb.com)

**Introduction**

Gone are the days of the simple electro-mechanical relay without firmware and communication interfaces. The fact exists that protection and control systems have changed significantly in the past decade and will continue to change with technology advancements. The digital world has impacted the protection system from the introduction of microprocessor based relays in the 1980s to protection relays with communication interfaces in the 1990s. Today's advanced digital protective relays utilize high speed communication to replace copper wires for inter-bay control, safety interlocking and even breaker trip and closing. Modern sensor technology also allows for the digitization and analog acquisition in the switchyard replacing hazardous inductive CT and PT circuits with process bus communications.

The Digital World has brought many benefits but also introduces challenges. This paper will focus on the impact of the protection and control system as a result of microprocessor relay introduction in the 1990s. It will discuss key issues the protection and control engineer has encountered in the past and will face with the deployment of the advanced protective relay. Key areas discussed will be performance and benefits including the digitization and transfer function of Nonconventional Instrument Transformers, security threats and best practices for the protection system, fleet management in the age of NERC PRC/CIP regulations and performance consideration to achieve high availability of the protection and control system. As well the paper will address some protection issues such as; since fiber optic current sensor systems have no iron, and no CT saturation, the differential relay need not have multiple slopes to account for CT performance, just a minimum pick up thus increasing the sensitivity several fold.

The educational benefits to understanding these impacts is paramount in the adoption and embracing of modern monitoring and control systems. Understanding the requirements to improve the performance of the substation automation protection and control systems is the goal to create the informed decision maker embracing these advancements in new technology which from a reliability perspective can greatly improve the overall power system performance.

## 1 Background

After the introduction of microprocessor based relays in the 1980s, the change to protection relays with communication interfaces in the 1990s had relatively little impact on the protection systems as such, but enabled integration of protection devices into substation automation protection and control systems.

Although the introduction of IEC 61850 standard opened-up opportunities for improved integration of protection and control relays of different vendors into automation systems, it had very little or no impact on the protection functions itself. Only now by extending the application of the same standard to the process level for data exchange between the primary system and the protection and control IEDs (intelligent electronic devices), it starts to play a mission critical role in the power system protection. The Digital Substation solution's key technologies (relays, advanced substation automation and modern instrument transformers) are the advantages where IEC 61850/Ethernet are positioned as technology enablers and not obstacles.

## 2 Induction disc to Microprocessors

First multifunction microprocessor relays were developed in the early 1980s. One was based on the Washington State University Master's Degree Thesis by Ravi Iyer. He joined Brown Boveri Corporation under the mentorship of Stanley Zocholl to design the distribution protection unit becoming the first multifunction microprocessor relay in 1984. This relay performed three phase and ground instantaneous and time overcurrent protection, multi-shot circuit breaker reclosing and integrated per phase metering in a single device that was slightly larger than two single phase electromechanical overcurrent relays. The innovation of the modern digital system roots from this era by the industry pioneers understanding the interworks of the electro-mechanical relationship to engage the revolutionary computer scientist replacing induction discs and spring constants with data acquisition, digital conversion and four point algorithms. These early devices were based on 8-bit microprocessors and programmed in highly optimized assembly source code as the algorithms had to be extremely efficient and program memory size of 64 kilobytes was a luxury.

The microprocessor relay is our industries first venture into The Digital World and it has revolutionized our protection and control systems. The key benefit of the microprocessor relay has been the significant reduction of panel space required to accomplish the same protection system. Figure 1 depicts a line protection system for 1 ½ breaker arrangement.

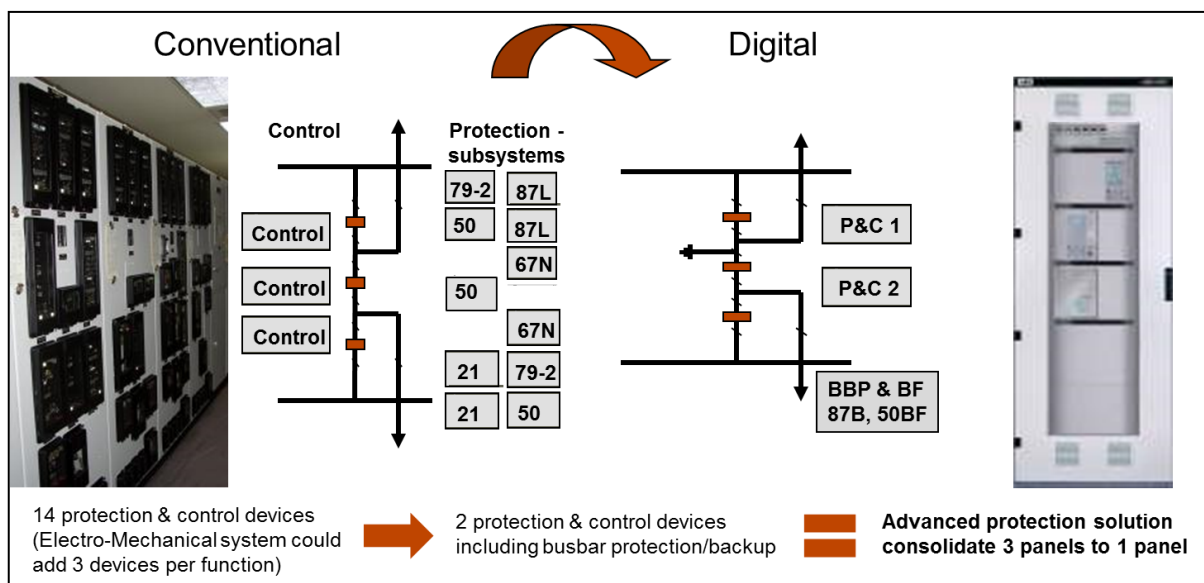


Figure 1: Substations secondary systems showing the same application with electro-mechanical relays versus modern digital system

In the Figure 1 example, the protection function indicated by the ANSI relay elements were traditionally implemented utilizing discrete relays requiring several relay panels to protect this scheme. The utilization of modern multi-object (protection of more than one primary apparatus) relays and open standards for device to device communications allows for functional consolidation, elimination of control and interlocking copper wire interconnections greatly improving the system performance while increasing both reliability and personnel safety.

The most significant change, good and bad, was the introduction of software systems to perform these system protections. Early implementation had limited software source code as the microprocessor power and memory size limited the amount of functionality permissible. As the multi-functional relay advanced and started communicating to RTU and gateways, the complexity of the device software system also increased. The good is that protection system performance increased tenfold while the bad was the introduction of the undocumented feature also known as software bugs. The firmware version management is now a crucial element of the utility fleet management to ensure that the installed protection devices do not lead to unwanted system performance. For the American Bulk Energy System, the North American Reliability Corporation (NERC) has developed a set of reliability and critical infrastructure protection standards to support overall grid reliability, stability and security.

The protection and control system may seldom be called upon to operate until the abnormal condition threatens the apparatus. It is this instance that the system must operate to protect the utility assets. A major benefit of the modern protection devices is the advanced self-diagnostics and self-supervision to ensure the highest availability of the system. Electro-mechanical and solid state relays were only found to be non-operational when a fault occurred resulting in a misoperation or during routine testing. The modern protection device has advanced diagnostics to ensure performance or indicate of pending problems.

Today, the digital world continues to morph as modern primary apparatus embeds digital technology and the benefits of non-conventional instrument transformers further improve system performance and personnel safety. These enablers on the primary system process level will continue revolutionizing the next generation of system protection, control and automation.

### 3 The Digital Systems

In the digital system, sampled analog values are communicated according IEC 61850-9-2 from merging units or non-conventional instrument transformers (NCITs) to the protection and control IEDs and trip commands are sent as IEC 61850 GOOSE messages to the circuit breaker interfaces. By this, the communication system becomes a critical part in the fault clearance chain affecting the total fault clearance time of the protection system.

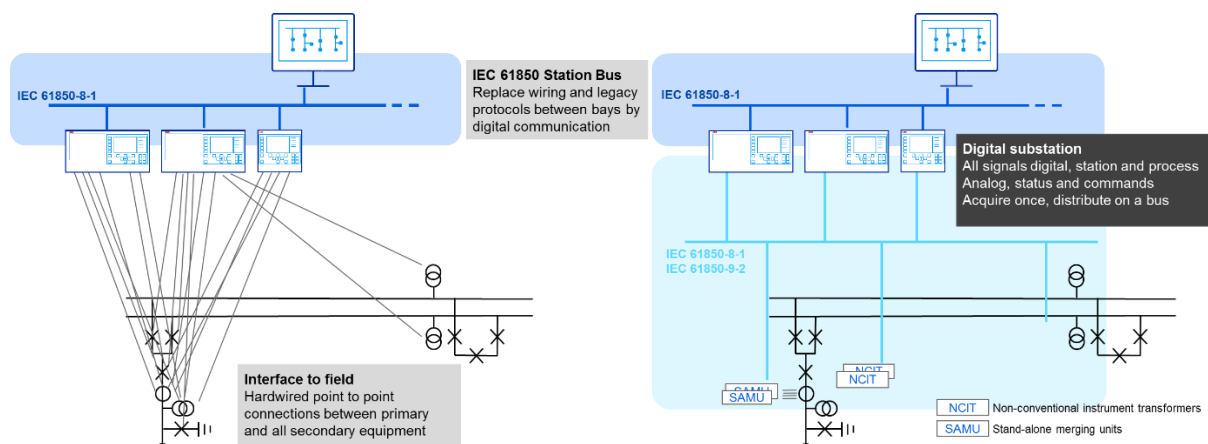


Figure 2: Substations secondary systems with direct point-to-point wiring and process bus communication network

## 4 From copper wiring to process bus

Approaching the installation of a process bus communication network, which connects the bay level equipment like protection and control IEDs or metering devices to the merging units and breaker IEDs located at process level, is motivated by different aspects:

### 4.1 Increased safety

By replacing conventional CTs with non-conventional ones like optical CTs, the risks attached to open CT circuits are equally eliminated as the risk of exploding CTs or VTs, as no copper windings are involved and no oil filling is required.

Every copper wire in a substation is a potential risk whether it is from a CT or PT circuit or a 125V DC control wire. The highly inductive current transformer secondary circuit poses the largest safety concern. The hazard results when an energized current transformer wire is unknowingly disconnected. From inductive circuit theory, current flowing through an inductive circuit cannot be instantaneously changed from 5 Amps to zero. A quick thanks to Wikipedia;

$$v(t) = L \frac{di}{dt}$$

the mathematics formula implicitly states that a voltage is induced across an inductor, equal to the product of the inductor's inductance, and current's rate of change through the inductor. As the inductance does not change during the open circuit, the rate of change in current from 5 to 0 Amps instantaneously has the derivative (di/dt) resultant go to infinity. Thus, the formula's product voltage is dominated by the derivative blowing up to infinity and produces a very large voltage across the open circuited wires. Related to the substation application, an open CT secondary is equivalent to the inductive current going to zero and depending on the secondary load, arcing will occur as these dangerously high voltages build putting field personnel at risk of serious injury or even fatality and the substation equipment at risk from electrical fire. Minimizing copper leads to greatly improved safety.

### 4.2 Less material

Using fiber optics instead of copper cables not only reduces the copper cabling in a substation by around 80%, depending on voltage level and switchgear type and layout. It also means less material transport to site.

If conventional instrument transformers are replaced by non-conventional ones, further weight can be saved. An optical CT for a 400kV AIS installation weighs about 20% of its conventional (SF<sub>6</sub> filled) counterpart.

### 4.3 Shorter installation time and shorter outage time for secondary system retrofits

Less cables to be pulled, less equipment to be connected and less connections to be tested. This leads on one hand to shorter installation times of new secondary systems, on the other hand it also helps to reduce outage times during secondary system replacements. The outage time in the latter case can be reduced due to the shorter time required to install the new equipment, but also because the new equipment comes from the factory fully tested from SCADA through protection and control IEDs to process interfaces. Hence testing of the new system that requires outages is reduced.

## 5 Fault clearance times of digital substations

When approaching to use NCITs and Ethernet communication to transfer mission critical analog and binary data for protection functions, the tripping speed does not depend anymore only on the protection IED and tripping relays. In digital systems, the fault clearance time is depending on the performance of all involved electronic components like NCITs, merging units, protection IEDs and breaker IEDs, as well as on the design of the process bus communication system.

The expectation on the digital system is that they fulfill today's specifications and regulations regarding fault clearance time and that they perform at least as good as today's protection systems. A

typical figure for fault clearance times under normal conditions (without failures in protection system or circuit breaker) is four power cycles. Two cycles are considered for the circuit breaker opening with extinguishing of the arc and two cycles are assumed for the protection system. These figures can be found in international standard like IEC 60834 [3] and national regulations like NERC's technical paper on protection system reliability [6] or National Grid UK's grid code [5].

Figure Overview on the time budget from fault inception to fault clearance with typical operating times of the protection system in a traditional system without NCITs and process bus communication.

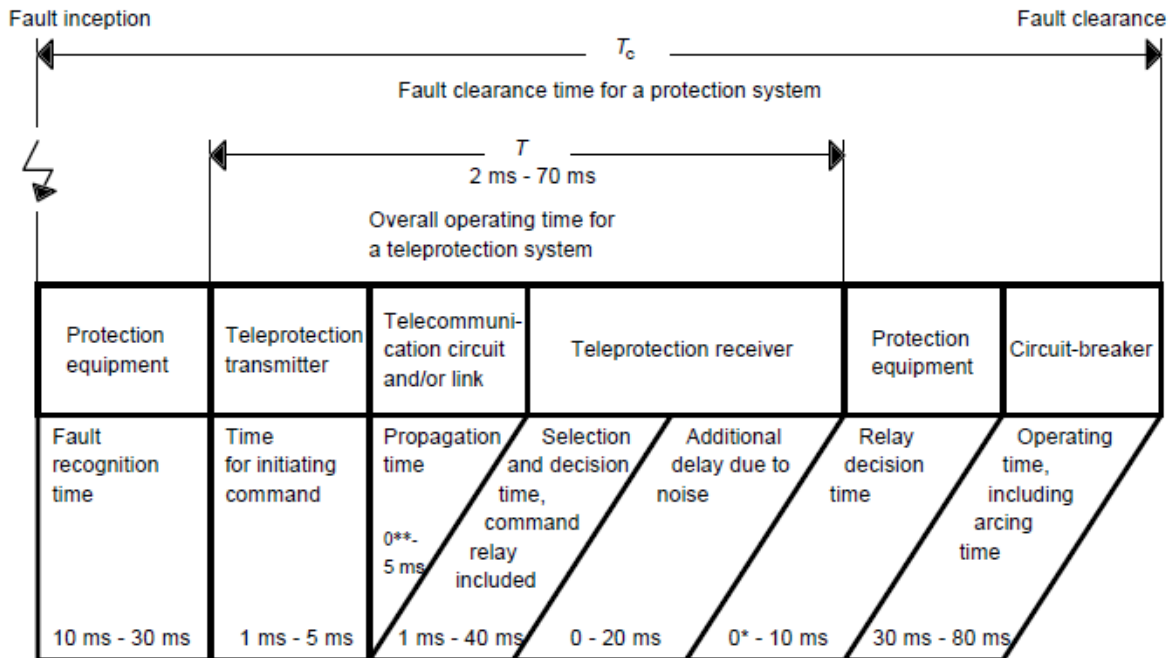


Figure 3: Time budget with typical operating times [3]

Moving to the digital world, Figure depicts the fault clearance chain from NCIT through protection relay to breaker IED and circuit breaker.

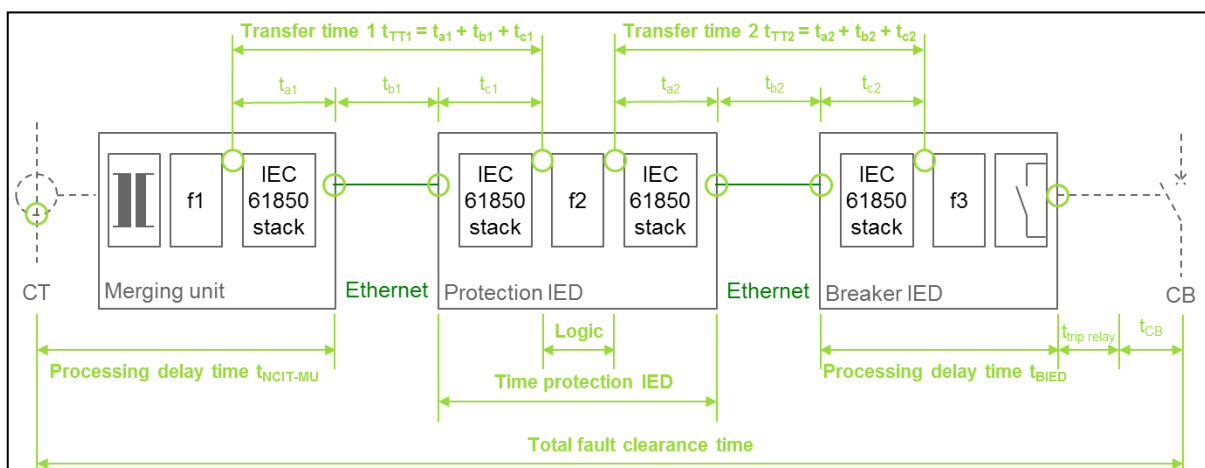


Figure 4: Time budget in digital systems

Two of the times in the above figure are defined and categorized by international standards. The "processing delay time" of NCITs and merging units is defined in IEC 60044-8 [12] as rated delay time, which shall not exceed 3ms for protection applications. The "Transfer time" definition is part of IEC 61850-5 [9]. For both, sampled values and trip commands sent via GOOSE, the highest transfer time performance class applies, which shall be 3ms or less. The transfer time is the sum of the times required by the stack of the sending device, the stack of the receiving device and the communication

system. According to IEC 61850-10 [10] and IEC 61850-90-4 [14], the 3ms are assumed to be split 80% to the processing times in the IED stacks (2.4ms) and the remaining 20% (0.6ms) for the communication network.

Table 1 Overview of the standard or typical timings in the fault clearance chain, as well as the timings that are achievable with modern devices and appropriate communication system design. The IED logic processing time, ie the time required by the protection algorithm is assumed to be one 60Hz power cycle in both cases.

Step	Standard	Standard or typical time [ms]	Today possible time [ms]	
NCIT&MU processing delay time	$t_{NCIT-MU}$	IEC 60044	3.0	0.8
Network transfer time (sampled values)	$t_{b1}$	IEC 61850	0.6	0.4
IED stack processing time	$t_{c1}$	IEC 61850	1.2	1.2
IED logic processing time	$t_{Logic}$		16.0	16.0
IED stack processing time	$t_{a2}$	IEC 61850	1.2	0.6
Network transfer time (GOOSE trip)	$t_{b2}$	IEC 61850	0.6	0.3
BIED tripping time	$t_{BIED}$		7.0	4.0
External trip relay	$t_{trip\ relay}$		5.0	0.0
Circuit breaker opening time (2 cycles)	$t_{CB}$		32.0	32.0
<b>Total fault clearance time</b>			<b>66.6</b>	<b>55.3</b>

Table 1: Time budget with standard respectively typical times and possible times with modern devices

One important point in the second column with the today possible times, is that the external trip relay is omitted and the circuit breaker is directly tripped by the breaker IEDs power outputs. But even if the trip relay is in place, the total fault clearance time requirement of 4 power cycles, as mentioned above, can be undercut significantly.

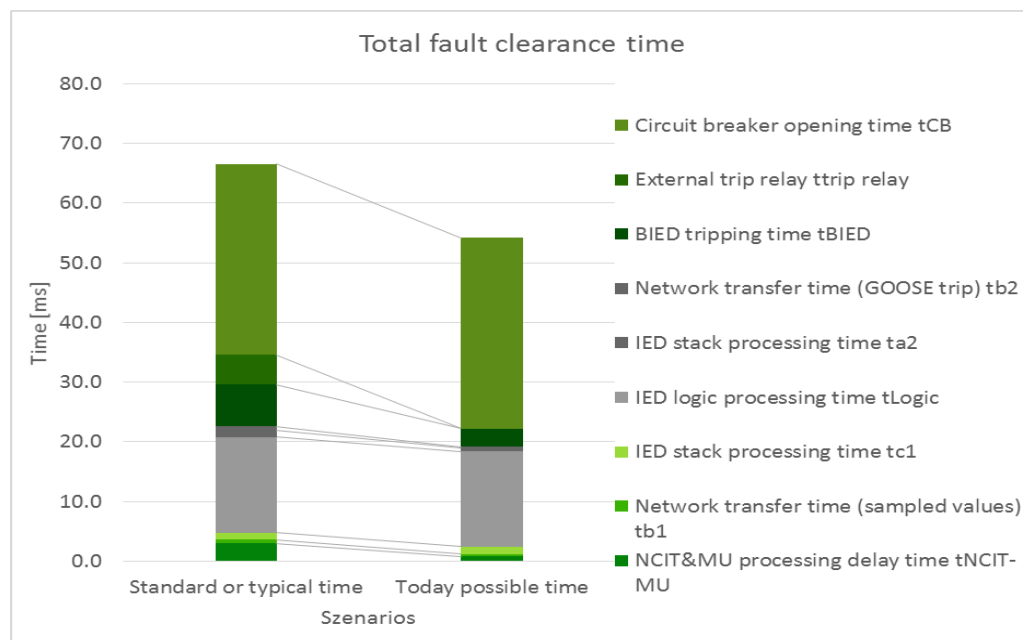


Figure 5: Time budget with standard respectively typical times and possible times with modern devices

More details on the above used calculation scheme, as well as more in depth explanations and analysis can be found in [2].

## 6 Impacts of non-conventional instrument transformers

### 6.1 Accuracy

That non-conventional instrument transformers can provide excellent accuracy of 0.2% or better has been demonstrated in various installations, where the NCITs have been connected to IEC 61850-9-2 process bus enabled grid meters. To verify the accuracy of the digital measuring chain, they have been installed in parallel to a conventional metering system. The installation described in [8], showed that after three years of operation the difference of the accumulated energy measured by the conventional and the digital system was at around 0.35%. This is not the absolute accuracy but the difference of the two measuring systems, which could be up to 0.8% as both systems were allowed to introduce errors of 0.2% for current and voltage.

Even better results are presented in [7], which describes two installations with NCITs, process bus and grid meters. Here the observed differences for active energy between conventional and non-conventional systems range from 0.01 to 0.19%, far lower than the tolerable error given the accuracy classes of the installed conventional instrument transformers and NCITs of class 0.2 and 0.2s respectively.

### 6.2 Transient performance

Transient performance classes of instrument transformers play important roles in dimensioning protection applications. The protection performance and transient performance is defined in IEC 60044 and IEC 61869. Instrument transformers standard IEC 61869 is replacing the old IEC 60044 standard. The parts for conventional instrument transformers are already released, but for non-conventional or electronic CTs and VTs, still the old standard has to be used. In both cases they describe the behavior at the secondary interface of the instrument transformers, which are the terminal blocks in case of conventional CTs and VTs and the communication interface in case of their non-conventional variants.

Along with the definitions of IEC 61850-9-2 and also the "Implementation Guideline for Digital Interface to Instrument Transformers using IEC 61850-9-2" [13], commonly known as IEC 61850-9-2LE, the instrument transformer standards hence allow to sufficiently describe NCITs and enable building multivendor installations.

If decided to use conventional instrument transformers in combination with so-called stand-alone merging units, that convert the analog input data to IEC 61850-9-2 sampled values, the measuring chain is not fully covered anymore by standard definitions, as shown in Figure 6. Part 13 of IEC 61869 will be dedicated to the stand-alone merging units, but is yet to be released.

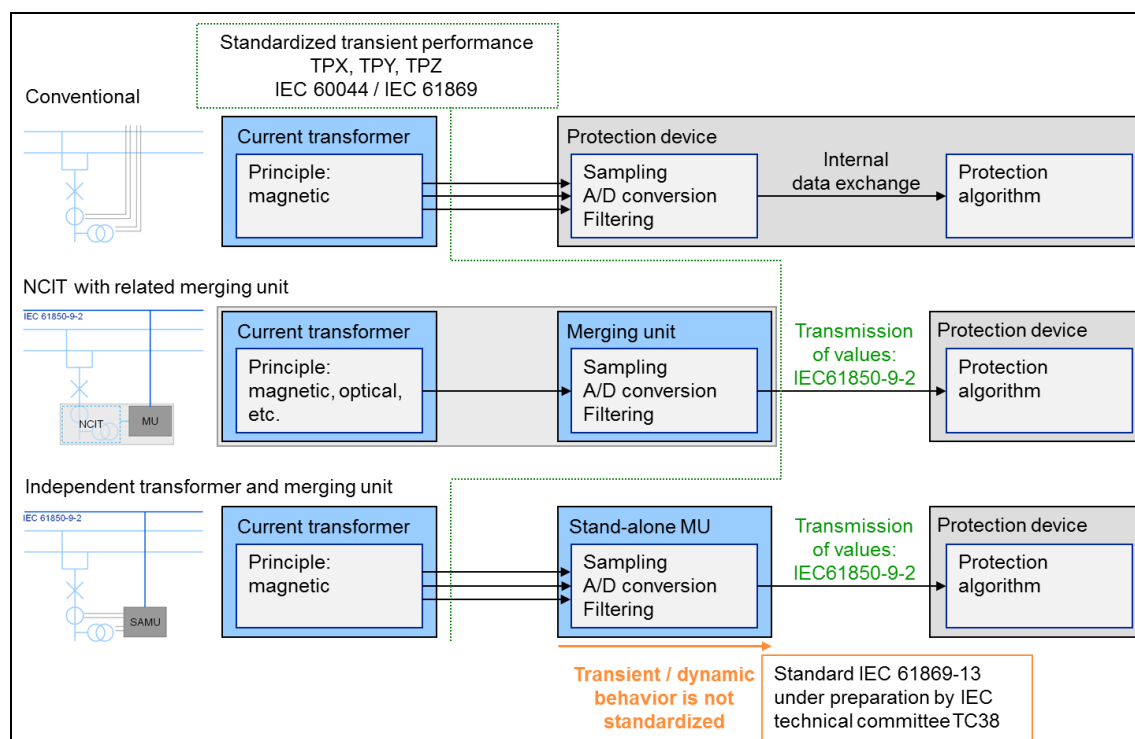


Figure 6: Interfaces and standardization

Until the IEC 61869 standard part is ready, interoperability beyond communication of the stand-alone merging unit of one vendor with the protection relay of another vendor has to be carefully verified. Complete system testing stressing the dynamic performance and transient response of the analog conversion is critical to ensure proper system operation.

### 6.3 Optimized placing of measuring points in the substation

Thanks to its compact nature, the placement of non-conventional current and/or voltage transformers in the switchyard can be optimized to improve overlapping of protection zones. Figure gives an example of a simplified 1 ½ breaker arrangement with NCITs installed at each side of the circuit breakers. In this setup the protection zones of busbar and line protection as well as the protected zones by the line protection overlap. In case of air-insulated systems, the NCITs can be integrated in the bushings of the circuit breaker or in case of gas-insulated systems; they can be located at each side of the circuit breaker between breaker and disconnectors.

The NCITs in the figure above are measuring either current or current and voltage. In case of combined NCITs for current and voltage, more voltage measuring points than normal are available in a diameter, which results in biggest flexibility in choosing voltage sources for e.g., synchrocheck and distance protection functions.

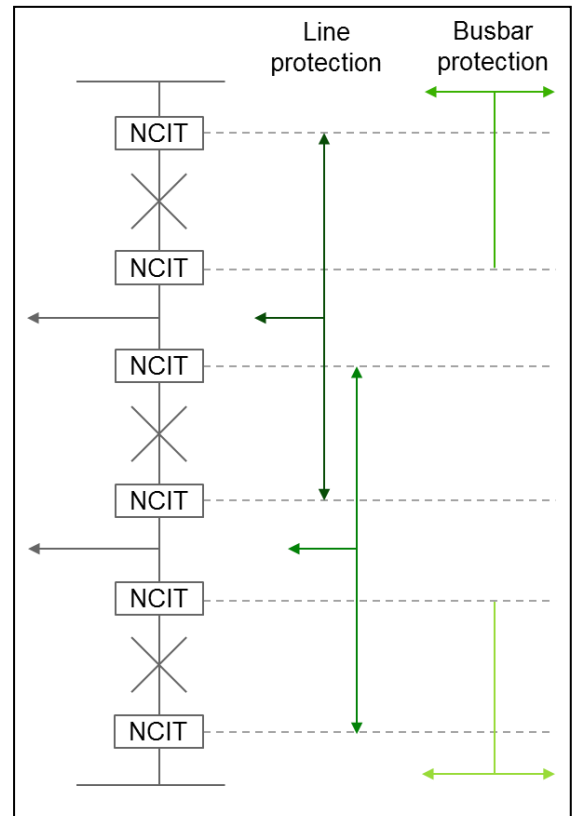


Figure 7: NCIT solution with fully overlapping protection zones

### 6.4 Benefit of sensors not saturating

The result of using a current sensor that does not saturate can have a profound effect on the setting, and thus the sensitivity of a relay. Take for example, the differential relay. A differential relay relies on current sensors to provide the exact reproduction of the primary currents to it for analysis. It then adds the current vectors together and computes a differential current. Then using an operating curve, as shown in Figure 8 determines whether to operate or not. If the differential current falls above the characteristic curve for a given restraint current, the relay operates. If not, it restrains.

The slopes in red section, and green section are there to adjust for the performance of a conventional current transformer. As the restraint current goes up, the chances of two conventional current transformer operating exactly the same reduces. This output difference between the current transformers is compensated for by increasing the slope of the characteristic such that more differential current is needed to operate as the restraint current increases. The red section

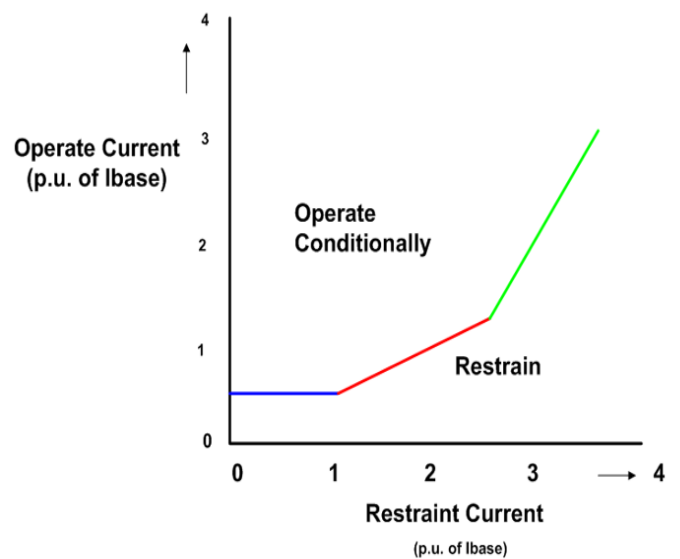


Figure 8: Differential Curve with segmented slopes

typically has a slope of 40%, and the green section typically has a slope of 80%. While this compensation is necessary for conventional current transformers to make it secure during current transformer saturation, it has the effect of decreasing the sensitivity of the differential scheme. With the use of non-conventional current sensors, these slopes can be set to close to zero which increases the sensitivity of the differential scheme during high current conditions.

## 7 The Digital World opens up Cyber Threats

Cyber security creates fear in our industry as mentioning NERC/CIP compliance can lead to the wrong behavior. The information available in our utility systems is essential for advancing system performance, proactive control and improved operations and maintenance. Cyber security standards provide the framework and requirements either towards compliance or technical solutions. The educational benefits to understanding these requirements is paramount in the adoption and embracing cyber security as a key enabler to our modern monitoring and control systems.

The fact exists that substation automation, protection and control systems have changed significantly in the past decade and will continue to change with technology advancements. Systems have become more interconnected and provide end users with much more information to allow for higher reliability and greater levels of control. Interoperability between different vendor products and systems has been achieved by developing products and solutions based on open standards and by leveraging commercial technology like standard Ethernet technology. This change in technology has not only brought huge benefits from an operational point of view as discussed in the previous sections, it also permits substation automation, protection and control systems to address cyber security issues similar to other traditional, enterprise systems which have been facing the same industry challenges for years.

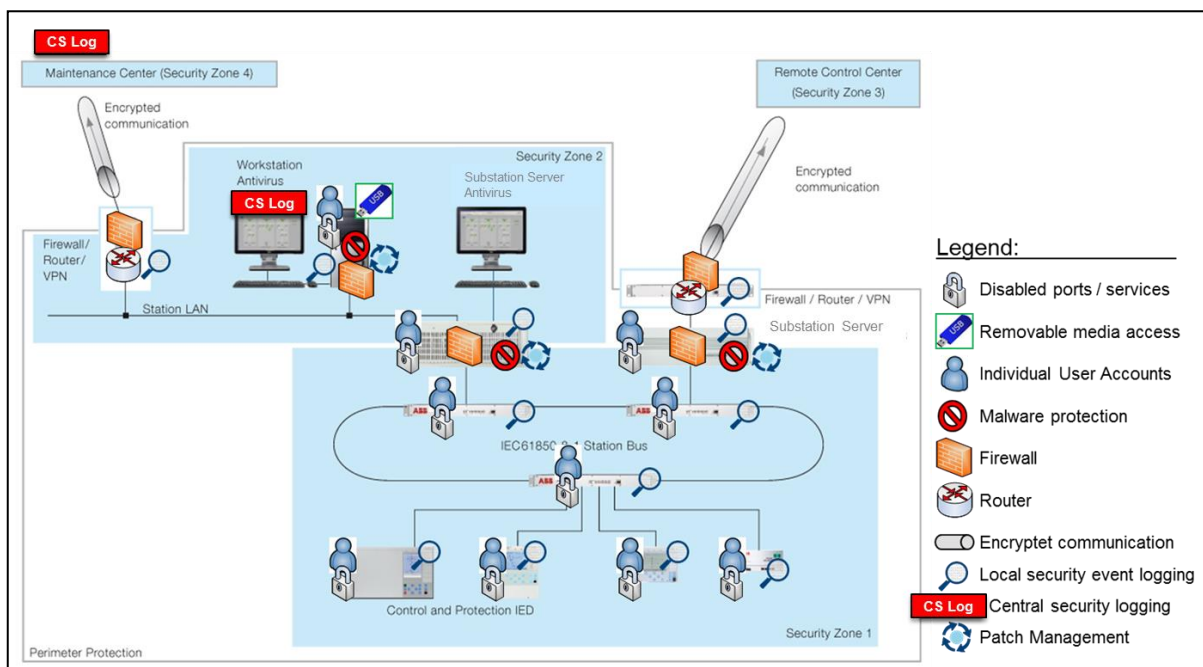


Figure 9: Example Substation Automation System Reference Architecture for Defence in Depth

Tightly integrating the control system components and allowing inter-connected control systems with the external systems not only allows for more and faster information exchange, but, it also provides entry points for hackers and increases the need to protect against cyber-attacks. Using Ethernet and TCP/IP based communications not only make systems more interoperable, but also opened the door for trojans, worms, viruses and Internet based attacks, etc. The need for secure substation automation protection and control systems as well as the entire utility Information Technology infrastructure is being pushed in many markets by regulations to ensure national security due to the potential impact that a coordinated cyber-attack on the electric utility control system could have on wide scale outages. The key to any successful security system is deploying Defense-in-depth

strategy as shown in Figure 9. Threat models are constantly changing, the bad guys are getting smarter and the monitoring and management of the overall IT systems is paramount to keep the power system control equipment safe and secure.

In addition to government driven efforts the increased importance of cyber security for power systems has also led to various standard bodies and working groups taking on the challenging topic. The focus, level of detail and maturity of these efforts are quite broad. At the moment five initiatives seem to be most advanced, which we will discuss in the following paragraphs and should be included in your utility overall cyber security policy and practices.

### **7.1 NERC CIP**

The NERC CIP regulations have had the biggest impact on electric utilities so far and been the focal point of most security programs. The regulation makes a clear statement that the main responsibility for securing the electric grid lies with the utilities and that it is not just about technology but also about processes. There are some shortcomings of the current version, i.e. the exclusion of serial protocols or the focus on a single electronic security perimeter. An additional area for improvement is the definition of critical assets and critical cyber assets. While the definition of what is deemed critical and what is not has been made a bit clearer within the NERC/CIP standard version 4 and 5 [17], protection of critical (cyber) assets is still done in an all or nothing fashion. If a cyber-asset is classified as critical all NERC CIP requirements apply, if it is not classified as critical then it must not be protected at all (unless it is within the electronic security perimeter).

This all or nothing approach does not take into account different levels of criticality and does not allow for different levels of security, which is a common best practice for security of computer based systems. However, the ongoing revisions are constantly looking at different levels of criticality, which will hopefully lead to a more realistic and more granular approach to cyber security. It is important to note that the NERC standards are performance based standards that inform the utility what security measures need to be implemented and monitored. Therefore, no product or technical solution can claim to be NERC CIP compliant but rather the technical solution can support the utilities compliance to these standards. On the other hand, the IEEE and IEC develop technical standards that provide the technical blueprint or the “How” for the utility security solution and the most important standards are listed below.

### **7.2 IEEE C37.240**

Jointly within IEEE PES Substations and PSRC, this standard is based on the applicability and the technical implementation of the NERC CIP and NIST Smart Grid security efforts for substation automation, protection and control systems. The standard on “Cyber Security Requirements for Substation Automation, Protection and Control Systems” provides technical requirements for substation cyber security. It presents sound engineering practices that can be applied to achieve high levels of cyber security of automation, protection and control systems independent of voltage level or criticality of cyber assets. Cyber security includes trust and assurance of data in motion, data at rest and incident response.

### **7.3 IEC 62351**

IEC 62351 is a technical security standard that aims to secure power system specific communication protocols such as IEC 61850 or IEC 60870-5-104. While most parts of the standard have been released in 2009 more work is needed before systems compliant to IEC 62351 can be put on the market. First of all, the affected communication standards must be changed to support IEC 62351. In addition there are some technical challenges with securing real time traffic that must be addressed by the working group of IEC 62351.

### **7.4 IEEE 1686**

Security of intelligent electronic devices is the scope of IEEE 1686. The document defines in technical detail security requirements for IED's, e.g. for user authentication or security event logging. The standard very nicely points out that a) adherence to the standard does not ensure adequate cyber security, i.e. that adherence to the standard is only one piece in the overall puzzle, and that b) adherence to every clause in the standard may not be required for every cyber security program. With this the standard gives vendors clear technical requirements for product features but at the same time leaves room for specific, tailored system solutions at the customer site.

## **8.0 Summary Benefits of the Digital Substation**

A fully digital substation is smaller, more reliable, has a reduced life-cycle cost and is simpler to maintain and extend than an analog one. It offers increased safety and is more efficient than its analog equivalent. Not every substation needs to be catapulted into a wholesale digital world – it depends on the substation size and type, and whether it is a new station or a retrofit of the secondary system. Different approaches and solutions are required. Flexible solutions allow utilities to set their own pace on their way toward the digital substation.

- Increased system availability by replacing of electromechanical, static or old fashioned digital secondary equipment with modern numerical devices bundled to a real-time communication network and connected to a higher level system such as a substation automation system or SCADA, allows continuous monitoring of all connected secondary equipment.
- Increased system and personnel safety utilizing remote control combined with authority and rule-based access and remote testing, allows increased system safety and security. Personnel safety is increased since more tests can be done without putting the test personnel close to primary equipment or without the risk of inadvertently opening current transformer (CT) circuits.
- Increased functionality with a fully distributed architecture coupled with un-restricted communication and process capability enables the system to add new functions easily with zero or minimal outage time, giving the user additional benefit with respect to safe and secure system.
- Interoperability through deployment of IEC 61850 compliant solutions, interoperability with regard to communications with other manufacturer's equipment can be achieved. The benefit is IEDs from different suppliers can be mixed on the same bus without concern for communication incompatibilities.

## **9.0 Conclusion**

Technology has changed significantly from over the past 30 years and will continue advance enabling more benefits from The Digital World. The early adoption of microprocessor relays started the era into The Digital World. Along with their significant advantages, they also introduced our world to software and communicating devices to the realm of Cyber Threats in our changing environment. The introduction of the IEC 61850 station and process bus standards for substations has provided a platform that all manufactures can develop upon to achieve the overall goal of interoperability. John Burger's visionary ideas are being realized with the technology available today. In addition to the interoperability benefits, footprint of primary switchgear reduction using sensors (NCIT) replacing conventional measuring transformers and breaker controls allows a much safer work environment and a massive reduction of cabling by going from a lot of copper cables to a few fiber optic communication cables. As for the challenges presented by the cyber threats, the industry must embrace modern device capabilities to deter, delay and detect the bad guys. Let us not forget that the multifunction relay is today the source of information that can enable higher level systems to be proactive in the overall power system stability. Most importantly, the "R" in NERC means reliability so while CIP standards might drive organizations to shutdown communication access to the substation information, it is so crucial that the substation data be accessible to higher level systems.

## 8 References

- [1] S. Meier, "Enabling digital substations," in ABB Review, 4/2014
- [2] T. Werner, S. Meier, "Performance considerations in digital substation applications", PACWorld conference Glasgow, 2015
- [3] IEC 60831, "Teleprotection equipment of power systems – performance and testing – Part 1: Command Systems," IEC, Tech. Rep., 1999
- [4] IEC 62271-100, "High-voltage switchgear and control gear – Part 100: Alternating-current circuit-breakers", IEC, International standard, 2012
- [5] "The Grid Code, Issue 5," National Grid Electricity Transmission plc., Revision 13, 2015
- [6] "Protection System Reliability", "A technical paper", NERC System Protection and control taskforce, 2008
- [7] J. Widmer, Cigré paper B3-211 "From IEC 61850 based substations with sampled values to billing metering", Cigré Session Paris, 2014
- [8] D. Fuechle, M. Stanek, GCC Power paper "Experiences with Non-Conventional Instrument Transformers (NCITs)", GCC Power, 2009
- [9] IEC 61850-5, "Communication networks and systems for power utility automation – Part 5: Communication Requirements for Functions and Device Models," IEC, International standard, 2013
- [10] IEC 61850-10, "Communication networks and systems for power utility automation – Part 10: Communication Requirements for Functions and Device Models," IEC, International standard, 2013
- [11] IEC 60044-7, "Instrument transformers – Part 7: Electronic voltage transformers", IEC, International standard, 1999
- [12] IEC 60044-8, "Instrument transformers – Part 8: Electronic current transformers", IEC, International standard, 2002
- [13] "Implementation Guideline for Digital Interface to Instrument Transformers using IEC 61850-9-2", published by UCA International Users Groups, 2004
- [14] IEC 61850-90-4, "Communication Networks and Systems for Power utility automation - Part 90-4: Network Engineering Guidelines," IEC, Tech. Rep., 2013
- [15] S. Kunsman, N. Price, et al, "Protection and Control System Utilization of NCIT & Process Bus", PACWorld conference Raleigh, 2015
- [16] S. Kunsman, M. Braendle, et al, "Replacing Fear with Knowledge - Cyber Security for Substation Automation, Protection and Control Systems", 69<sup>th</sup> Annual Georgia Tech Relay Conference, 2015
- [17] "Implementation Study Final Report CIP Version 5 Transition Program", NERC Website, October 2014

## **Authors Information**

**Steven A. Kunsman** - Vice-President Business Development and Marketing, ABB Power Systems - Substation Automation North America

Steve joined ABB Inc. in 1984 and has over 31 years of experience in Substation Automation, Protection and Control. He graduated from Lafayette College with a BS in Electrical Engineering and Lehigh University with an MBA concentrated in Management of Technology. Today, Steve is responsible for ABB North American Power Systems Substation Automation business. He is an active member of the IEEE Power Engineering Society PSRC has held multiple working group chairs, an IEC TC57 US delegate in the development of the IEC61850 communication standard and UCA International Users Group Executive Committee co-chairperson.



**Stefan Meier** - Product manager, ABB Substation Automation Systems

Stefan is working with ABB Switzerland since more than 15 years, where he held several positions, from commissioning of substation automation systems, through technical support and project management. Today he is a global product manager for process bus solutions, where he coordinates the introduction IEC 61850 process bus in pilot and commercial projects.

Stefan studied electrical science at the University of Applied Sciences Northwestern Switzerland, and holds a master degree in business administration from Edinburgh Business School of Heriot-Watt University, Scotland.



**Roger Hedding** - Senior Consultant, ABB Power Systems - Substation Automation North America.

Roger graduated with a BSEE from Marquette University, and a Masters degree in Electrical Engineering from the University of Pittsburgh. Roger is currently a Senior Consultant for the ABB Power System Automation and Communications business unit. He guides the development of relay products, and applications for the ANSI market. Roger is an IEEE senior life member, and past Chair of the IEEE Power Systems Relay Committee. Roger has authored or co-authored many papers in power systems protection. His hobbies include travel, golf, and playing with his 4 grandchildren.

