Critical Infrastructure Protection with Modern Protection Relays

Daniel L. Ransom, PE
Senior Member IEEE
General Electric Grid Solutions
Tacoma, WA 98444
USA
d.ransom.pe@ieee.org

Abstract—Hardening the electric-power grid has become important today because of threats to the electric infrastructure. These threats are not only from bad actors targeting operational security; threats come from protective-relay design problems and aging. Modern microprocessor relays employ significant cyber defense and firmware advancements, as well as in physical improvements that increase reliability. These advancements include improved cybersecurity, power-supply longevity improvements, electromotive pulse (EMP) and geomagnetic disturbance (GMD) withstand, and advanced memory-map/bit-integrity safeguards. Misoperations data show greatly reduced incidents with new technology. New-generation relay designs include ease of upgrade from older relays via plug-n'-play retrofit solutions. Furthermore, software advances make settings and communications configurations easier, with fewer errors, which increase reliability of the electrical infrastructure. This paper reviews the latest advancements in relay design, construction, and software. In addition are recommendations for managing an aging relay fleet.

Index terms—critical infrastructure, cybersecurity, EMP, GMD, soft error, bit integrity, management software, upgrade, retrofit

I. INTRODUCTION

Protecting the electric-power infrastructure requires many methods that address the complex nature of the resources and assets that comprise the electric grid. First, it is necessary to understand the importance of the grid and how it relates to other vital aspects of modern life.

A. *Definition of Critical Infrastructure*

The term "critical infrastructure" describes physical and virtual systems/assets "…that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" [1].

Historically, critical infrastructures were separate independent systems with little interdependence. These infrastructures have become more linked and automated to automate processes and to increase efficiency. However, these advances have increased vulnerabilities such as cyber-attacks, equipment failure, physical and natural attacks, and human error.

Particularly the energy sector, and specifically the electric grid, is vitally important to the fabric of modern society and to modern commercial production. Today, threats to the electric infrastructure require action to harden and protect the electric grid. These threats are not only from bad actors targeting operational security, threats come from protective-relay design problems and aging, physical and natural attacks such as electromotive pulse (EMP) and geomagnetic disturbance (GMD), as well as human-error generated connection and configuration errors.

B. *Significant Advancements*

There have been significant advancements in modern microprocessor relays in firmware and security, as well as in physical improvements that increase reliability. In system protection, reliability is comprised of dependability—making the (correct) protection action every time, and of security—the protection operates only as prescribed; it does not operate incorrectly. These significant advancements are the following:

- Increased cybersecurity for firmware/software and operational technology (OT)
- Advanced memory-map/bit-integrity safeguards
- Enhanced withstand for electromotive pulse (EMP)/geomagnetic disturbance (GMD)
- Improved, error-checking configuration software—software advances improve settings; avoid errors

II. INCREASED CYBERSECURITY

Electrical infrastructure—generation, transmission, and distribution, is essential to modern industrial processes and is the foundation of modern society. This infrastructure relies on industrial control systems (ICS), in particular, SCADA (supervisory control and data acquisition), and electrical system resilience via protection and automation relays. These controls provide automated command and remote management of essential services to millions of people. In addition to electricity, these services include water, energy (natural gas and petroleum pumping/processing), and transportation. Dangers to these protection and control systems comes from firmware/software attacks, and from physical attacks. In addition, firmware and physical remedies can harden the process.

A. *Mitigating Firmware/Software Threats to Critical Relays, Automation, and OT*

Modern protection relays and automation controllers run on embedded firmware that operates the device functions. Interconnections among these devices are via smart Ethernet switches and other operational technology (OT). This is hardware/embedded firmware that controls communications routing and other processes common in SCADA (supervisory control and data acquisition) and industrial control systems (ICS). In addition, there is IT (information technology, i.e., the business network) human-interface software for programming and monitoring these devices.

The firmware/software and hardware that comprise these systems are susceptible to cyber-attacks that could bring down any part of this critical infrastructure. It is important to put in place the right security and practices to keep these systems operating correctly. Also, security protects the significant monetary investments that organizations make to establish and operate the critical infrastructure and controls.

Before microprocessor technology, protection was by electromechanical relays, and automation control was rudimentary dedicated lines and hard-wired solutions. Personnel visited important stations to report the system state and to calibrate the analog controls.

With microprocessor-based intelligent electronic devices (IEDs) came miniaturization, speed, and greatly increased scope of protection and automation. Local-area network (LAN) communication and signal routing enabled the distributed SCADA network. Next came the wide-area network (WAN), which tied more of the protection and controls together, relying on communication based upon internet protocol (IP). Although fast, efficient, and easier to implement, protection and control systems have become vulnerable to the security risks of IP-based systems.

Critical infrastructure remains a target for bad actors who want to disrupt and/or hold processes for ransom. There are well-documented ways to safeguard critical infrastructure protection and control [2]:

- Use secure-access gateways/VPNs
- Authenticate all external access points with multi-factor authentication (MFA)
- Segment OT
- Allow only authorized system and user connections
- Review trust relationships
- Employ network-assessment and monitoring tools

B. *Use Secure-Access Gateways/VPNs*

SCADA network attacks exploit both physical and cyber vulnerabilities. Secure-access gateways and virtual private networks (VPNs) are essential defenses. These devices control the way that a computer/HMI connects to the network and enforce security policies that define access to the network only for specific endpoint devices. In addition, the gateway can analyze and filter malicious network traffic in real time, as well as restrict access to only certain sites and applications. Some offer data-leak protection—alerting for larger-than-normal file transfers.

A virtual private network is a system on an existing network that encrypts the end-to-end network traffic. Thus, machine-in-the-middle (MTM) attacks are no longer effective. In such an attack a bad actor intercepts the traffic, modifies, and injects a troublesome data control, and then forwards the information to the intended receiver. The VPN protects the data traffic from interception, foiling the MTM attack. It does this by providing a secret certificate to the parties at one or both ends of the connection; successful communication means that the certificate keys must match to allow communication.

C. *Allow Only Authorized System and User Connections*

In the early days of remote computer control of SCADA stations, the equipment was air gapped. There was no network connection to the controlled/monitored equipment. Although expensive and difficult to maintain, security was not a major concern—there was no access point for outside actors. Now that ICS equipment is connected to the Internet, these assets that provide real-time operations data are valued targets to threat groups that want to disrupt or gain money by attacking these systems [3].

Today, many operators use remote connections for everyday operation. Remote access is used for ongoing control and monitoring of remote field sites because one technician can manage many sites, maximizing efficiency and reducing cost. As for system maintenance, there are fewer qualified technicians to perform maintenance work; thus, remote access to update and modify the ICS system is more popular. (Also, there are no travel costs in maintaining the gear remotely.) For example, flying a technician to the site when there is a need to diagnose, program, and update the SCADA/ICS is expensive. It is preferable if the technician connects remotely to the equipment—the work occurs immediately, with no travel cost.

Remote connections must be limited to authorized systems and users. There have been several successful and notorious cyber-attacks, including the Dragonfly spear-fishing crusade of 2014, the Ukraine power-grid attack in 2015, and the Oldsmar, FL water supply incident of 2021 [4].

It is important to follow best practices for remote connections into SCADA/ICS. These limit attacks and help identify the threat actors pursuing these systems. The primary tool is a connection through a DMZ (de-militarized zone), an IT/OT security boundary. Remote connections enter the system via multiple DMZs, using authentication services, firewalls, jump servers, and file servers that make these connections secure. Once in the DMZ, remote access connections enforce the policy of least privilege to provide only the functions that a remote user needs to do a specific job. There is no cross scripting or jumping to another function allowed. For protection relays, the RADIUS (remote authentication dial-in user service) server performs this function. Upon attempting to access a relay with RADIUS security, the relay checks with the remote server to validate the log-in credentials, then, if correct, allows access. Also, this server manages passwords, making easy the NERC CIP-007 task of using hardened passwords and of changing passwords regularly.

D. *Authenticate All External Access Points with Multi-Factor Authentication (MFA)*

Connections into network OT, protection relays, and automation controllers should be provided according to the least privileged role to perform the work. Role-based access into these systems occurs via authentication (usually a password or passphrase). All log-in accounts should be named—there are no shared accounts—so that there is access accountability. To do this, the user employs a VPN to connect to a jump host inside the DMZ behind a firewall. Another factor provides additional authentication. The three common methods are the following [3]:

- Something you know: password/passphrase, memorized PIN (personal identification number)
- Something you have: smartphone, a secure USB (universal serial bus) token
- Something you are: fingerprint, iris scan, facial recognition

Other examples are a question challenge, and an out-of-band confirmation (text message, html link, or email code).

E. *Segment OT*

It is important to segment control networks into security zones, to reduce the attack surface. Traditionally, the focus has been on perimeter security, with no additional, internal segmentation. Thus, threat actors navigate the unsegmented, flat network easily once inside the perimeter security. Attack exploits on poorly segmented networks are from malware finding the path of least resistance through perimeter security, then penetrating valuable assets inside the SCADA/ICS/OT wide-area network (WAN).

Security-zone segmentation has the following benefits:

- Attack surface is reduced
- Critical assets have limited exposure of critical production assets
- Access controls restrict movement among segments
- Monitoring and controls focus security in the most effective segments
- Incident and forensics have better data for improved detection and mitigation

F. *Review Trust Relationships*

It used to be that everything inside the organization control system was trusted. After authentication, any communication or application was allowed without challenge to gather data, generate reports, and to make control changes in the protection and automation environment. Today, the movement is to review regularly trusted relationships in the network, and to adopt a zero-trust approach [5].

The approach is to view the entire environment as untrusted or compromised. This is a change in thinking in that, not only protecting against outside-in attacks, now it is important to protect against internal data traffic until it is validated and approved. This could be as innocent as an unknowing employee getting into areas into which they should not be poking, or a malicious actor making unacceptable control actions or gathering data for a future attack. The zero-trust approach features traditional perimeter defense along with network segmentation and identity controls; these move the security perimeter as close as possible to privileged applications and controlled devices.

G. *Employ Network-Assessment and Monitoring Tools*

Network assessment and monitoring is a method to audit security systems and is part of the risk-management process [6]. Necessary for good cyber hygiene, this can be as simple as downloading and analyzing the protection relay syslog file (all relays should have one of these), to deploying enterprise-wide, software-assisted, real-time monitoring. Most entities use a risk-based approach to focus on the SCADA/ICS/OT processes and keeping these secure. Tools such as Nmap scan a network for open, vulnerable ports [7]. Wireshark examines actual network data packets. Brute-force intrusion/penetration tools harden authentication usernames and passwords. Fuzzing tools are similar; an automated testing software that provides invalid and random data and detects authentication program crashes, failed code assertions, and memory leaks.

H. *Cyber-informed Engineering (CIE)*

When building software and firmware solutions there is the process that engineers can employ to harden these products. Cyber-informed engineering (CEI) leverages engineering knowledge to structure cybersecurity into the design and architecture processes [8]. Thus, the services and security of the components are hardened. Cybersecurity is built in, not bolted on.

I. *Resources for Securing SCADA/ICS/OT*

Software/firmware hardening is vital to securing critical infrastructure. For advice, contact agencies like CISA (US Cybersecurity and Infrastructure Security Agency) office, which has resources and references to guide threat mitigation. In addition, many companies specialize in providing services to harden SCADA/ICS/OT networks.

III. ADVANCED MEMORY-MAP/ BIT-INTEGRITY SAFEGUARDS

Another aspect of protection critical infrastructure is whether the protection and control devices can survive a physical failure or attack. These can be internal and external events such as the following:

- Miniaturized-circuit malfunction
- Electromagnetic pulse (EMP)
- Geomagnetically induced currents (GIC)/geomagnetic disturbance (GMD)

A. *Efficiency Brings Problems*

The integrated circuits, memory, and signal-processing components in microprocessor relays are miniaturized circuits on a silicon substrate. These semiconductor components use integrated memory to run programs and calculations.

Very small electrical charges cross extremely small distances to represent digital logic and analog signals. Decreasing the power-supply voltage in semiconductors provides faster calculation speed. These qualities make the circuit faster and more efficient, generating less heat—thereby increasing longevity for normal service. However, these qualities increase the probability of soft errors and premature wear out. The ionizing particle that causes a bit flip is from ubiquitous cosmic-ray radiation. This random soft error, called a single event upset (SEU), leads to irregular calculations and program errors [9]. Miniaturization increases integrated-circuit vulnerability from GMD and EMP, as well.

B. *Repairing Memory Soft Errors*

Firmware algorithms can repair a memory soft error. A repeating memory scan detects these errors; then, a recovery program corrects and preserves the true memory value. The relay records this correction in self-test diagnostics. Symptoms vary depending on the detection algorithm speed and the memory bit location.

Protection relays and grid automation devices function in real-time, requiring millisecond parameter evaluation to execute appropriate control actions. Misoperations have revealed that fast elements, specifically current-differential and instantaneous overcurrent elements can operate before the relay firmware completes the memory scan. Thus, a bit-flip causes an incorrect protection trip.

A faster memory scan increases supervision at the logical application layer to detect and correct these fast bit flips. This improvement does not impact performance and does not require setting changes. The faster scan and enhanced firmware security add validity checks without affecting relay performance/specifications. A recent study from a major manufacturer's misoperations data show improvements in a majority of cases [10].

IV. ENHANCED WITHSTAND FOR ELECTROMOTIVE PULSE (EMP)/GEOMAGNETIC DISTURBANCE (GMD)

Modern, microprocessor-based automation and protection IEDs are susceptible to electromagnetic disturbances such as geomagnetically induced currents (GIC)/geomagnetic disturbances (GMD) and electromagnetic pulse (EMP). Theses phenomena have the potential to damage lines and transformers, as well as protection and automation IEDs, and thereby degrade/disrupt the electric-power grid and other critical infrastructures. Human-made and naturally occurring electromagnetic disturbances can affect large areas, blacking out power for a sustained period. Based on widely available electric power, the loss of this critical infrastructure would destabilizing nations' security and economic prosperity. The existence and possible impacts of these threats provides motivation to protect and harden the modern smart grid.

A. *Electromagnetic Pulse Disturbances*

High-altitude nuclear detonations, specialized conventional munitions, and non-nuclear, directed-energy sources are intentional methods to generate an EMP. A high-altitude electromagnetic pulse (HEMP) from an atmospheric nuclear explosion can damage permanently electric-power protection and automation IEDs over an entire continent. A truck-mounted electromagnetic interference generator can wipe out power and automatic control for a local/regional area.

Researchers have developed a generic HEMP waveform (Meta-R-324), shown in Fig. n [12]. It shows the fast-transient electromagnetic fields that induce damaging voltages on power lines and cause upsets to unprotected IEDs.

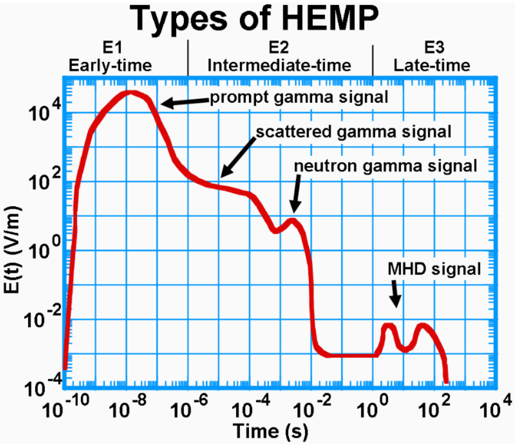


Fig. 1 High-altitude electromotive pulse (HEMP) waveform

Voltages from the E1 portion of the wave are as great as 70 kV when coupled into vertical cables and 20 kV for horizontal buried cables in generation facilities. IEDs subjected to these levels will not survive unless these devices are hardened.

There are many strategies for hardening the power system against EMP. These are shielding, grounding, fiber-optic cabling, and transient suppression [12].

1) Shielding: A Faraday cage shields against the radiated E1 field; the control-house construction is with highly conductive coatings on the outside. Additional EMI filtering includes gasketed entry ways, EM filtered air intakes, and shielded cable entryways. Inside the control house are properly shielded copper cables (when copper must be used).

2) Grounding: Proper grounding discharges the large, induced voltages to prevent EMP damage. Minimum ground impedance is necessary to reduce the common-mode impedance. A wide, flat copper strap or braid has less inductive reactance than a solid copper wire; flat strap is a best practice in rack ground wiring. Connect this strap to a buried copper plate for a low-impedance discharge path. A ground rod is suitable for lightning protection but has too large an impedance for EMP E1 pulses.

3) Fiber-optic cabling: For effective EMP hardening, fiber optic cables are used for communications and interconnections. Fiber-optic cables are not susceptible to induced voltages from the damaging E1 wavefront. Additionally, modern digital substations use process bus over optical cable and thus, all entries into the control house have no EMP-induced field.

4) Transient suppression: Manufacturers have begun hardening their equipment offerings with fast, high-energy absorption devices such as transient voltage suppression (TVS) diodes. These devices protect against voltage transient events, like lightning surges, switching transients, and electrostatic discharges. TVS diodes are placed at IED AC current/voltage inputs and power-supply inputs to prevent damage.

B. *Geomagnetic Disturbance (GMD)*

A GMD is a coronal mass ejection (CME) of plasma from the sun with an embedded magnetic field. When a CME arrives at Earth it can cause widespread and long-lasting damage to electric power systems assets and the relays and automation controllers that protect and operate grid components. Operators must protect these systems against the shock of a GMD (and EMP) event.

Extreme, damaging, GMD events are rare. The first recorded G5 (largest geomagnetic storm) event was the Carrington Event in 1859, disrupting telegraph lines. In March of 1989 the Hydro-Quebec grid located in Canada lost power for more than nine hours, affecting six million customers. In the next few months there were increased transformer failures throughout North America. Large G5 storms occur approximately every 33 months. The North American Electric Reliability Corporation (NERC) GMD standard, TPL-

007-4, requires utility operators to assess their system only to a 100-year GMD storm [13].

1) GMD regulations: Government agencies have mandated steps to protect the power grid. In the United States, NERC has issued Emergency Preparedness and Operations (EOP) 010-1, "Geomagnetic Disturbance Operations" [99]. This directive requires regional coordinators and grid operators to implement specific plans and procedures. In addition, FERC has approved the requirements of the NERC Transmission Planning document, TPL-007-4. These standards help prevent a catastrophic GMD event. Research is ongoing to understand GMD and its impact on the bulk power system and the optimization of mitigating measures.

2) Hardening systems against GMD: Power-system operators and industry have employed methods to mitigate the effects of GMD events [15]. GMDs produce harmonics in the power system. These harmonics cause protection equipment to meter the status of system voltage and current incorrectly and make the protection system undependable. Electromechanical and solid-state relays are susceptible to this effect, whereas microprocessor relays filter the harmonics and can operate properly on the fundamental frequency only. Review settings to add some margin to sensitive overcurrent, differential, and distance protection. GMDs create currents in transformer and capacitor-bank neutrals. Capacitor-bank protection that uses neutral current is susceptible. GMDs raise the voltage equally at the two taps in a capacitor-bank voltage differential scheme, so it does not affect this protection.

GMD mitigation includes blocking the quasi-DC currents in transformer neutrals that put the transformer into saturation and raise the core temperature to dangerous levels. One method uses capacitors in series in the transformer neutral. However, this method creates poor operation of regular ground-fault protection in the power system. Some power-system operators have had good success with switching the blocking capacitors into service when GMD currents occur. A successful monitoring system uses Hall-effect sensors to detect DC on the transformer neutral along with harmonic and distortion detection on the transformer output phases. GMD currents have larger even harmonics than the adjacent odd harmonics (i.e., 2nd larger than 3rd, 4th larger than 5th, etc.). In addition, a GIC monitor receives temperature data from the transformer hot spot and oil sensors. The GIC monitor signals an operator to remove the transformer from service and can control circuit breakers to apply neutral blocking capacitors.

V. SOFTWARE ADVANCES IMPROVE SETTINGS; AVOID ERRORS

Another aspect of protecting critical infrastructure is managing power-system studies and relay settings. Consistent processes and good data, and thereby a more-secure electrical infrastructure, are achieved by these processes:

- Establishing a consistent method for relay-settings development
- Confirming periodic, wide-area coordination validation
- Conducting in-depth confirmations of the short-circuit studies

These tasks require a significant amount of labor that the software can automate. Thus, the software aids in keeping the electrical infrastructure operating while eliminating time-consuming activities on an already busy engineering staff. NIST cites the aging workforce as a concern in workforce capability—software can remediate this problem [16].

A utility or industrial power-system operator of any size has thousands of configuration settings and templates to supervise. Managing these settings in spreadsheets is impractical. Mistakes can cause significant economic impact and jeopardize safety. Today, software is available to automate the process and store the results safely. These softwares perform the following functions [17], [18], [19]:

- Reduce calculation and review time
- Eliminate errors when producing settings
- Generate comprehensive reports

These softwares automate conventional workflow to streamline relay settings development, as well as simplifying the review process. The softwares communicate with modeling programs for fault calculation and generate a relay setting file and comprehensive, well-ordered reports for compliance documentation.

VI. MANAGING PROTECTION AND AUTOMATION DEVICES

Ensuring long-term viability of the electrical power system infrastructure requires maintaining the protection and automation devices that guard the system. The key to managing the protection and control IEDs is to treat these as assets; thus, there should be a wear-out and replacement plan. Recommendations for managing these IEDs include the following:

- Power-supply longevity
- Environmental monitor

- Development of plug-n’-play retrofits

A. *Power-Supply Longevity*

All circuits in a microprocessor relay rely on the power supply. An important design advancement is making the relay power supply more robust, increasing power-supply longevity. The improvements are these:

- Temperature reduction
- Improved electrolytic capacitors
- High-frequency switching

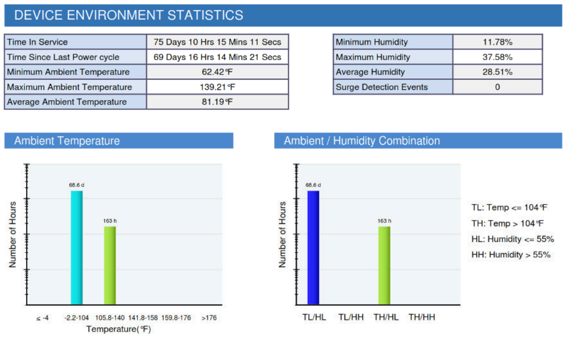
In early days, the relay power supply was basic [20]. It had rudimentary components such as steering diodes, step-down resistors/integrated-circuit regulators, and smoothing electrolytic capacitors. The design and component specifications were not optimized for long life. In addition, the initial microprocessor components consumed large currents and generated much heat. Excess internal relay temperature reduces life span. For example, a 10-degree C drop in temperature improves electrolytic capacitor longevity by twice [21].

Progress in component specifications and application-specific derating has improved longevity. Modern electrolytic capacitors last twice as long, with a useable life approaching 20 years. Today, power supplies are a high-frequency-switching design, which requires less smoothing capacitance, delivered by more reliable film and ceramic capacitors. When designers specify an electrolytic capacitor, they can choose the improved, long-life versions. In addition, electronic components operate with more efficiency, making chassis temperature less, leading to longer relay life. IED manufacturers have added extensive heat sinks to the device chassis. Airflow over the heat-sink fins reduces the internal component temperature, further increasing reliability and longevity.

B. *Environmental Monitor*

Along with temperature, excess humidity and input-power spikes reduce relay longevity. High temperature causes premature component failure. Humidity is like a blanket on the components increasing temperature, as well as oxidizing connections. Random excursions in input voltage can damage the power supply, shortening relay life. Today, relays are available that monitor and trend these environmental variables [22]. Monitoring the environmental health report gives feedback on the switchgear or substation environment. If temperature is too great, if the humidity is at stress level, if the relay input power is unconditioned, then take quick action to modify the situation. This action protects the relay as well as the other equipment in the switchgear/substation.

Relay manufacturers are including an environmental monitor. This feature records the largest and smallest temperature, the relative humidity excursions, and occurrences of damaging surge pulses. It accumulates the events every hour in pre-determined threshold buckets over a period of 15 years. Retrieve this data in the form of a histogram to ensure that any change in the operating condition switchgear/substation is identified quickly. Thus, there is data, an early warning, so that remedial action can be taken. **Error! Reference source not found.** shows a typical report from the environmental monitor.



DEVICE ENVIRONMENT STATISTICS

Time In Service	75 Days 10 Hrs 15 Mins 11 Secs
Time Since Last Power cycle	69 Days 16 Hrs 14 Mins 21 Secs
Minimum Ambient Temperature	62.42℉
Maximum Ambient Temperature	139.21℉
Average Ambient Temperature	81.19℉

Minimum Humidity	11.78%
Maximum Humidity	37.58%
Average Humidity	28.51%
Surge Detection Events	0

Fig. 2 Environmental health monitor report

C. *Replacements and Retrofits*

Eventually, all electronic devices fail. Replacing the relay introduces many variables that can be detrimental to operation of the critical infrastructure. These are incorrect wiring, corrupted/misinterpreted settings, and incomplete documentation after the change. If not in a main/standby protection scheme, the time that it takes for the relay swap to occur compromises asset protection. Upstream protection to cover the asset is less sensitive and slower than the replacement-candidate relay.

A method to minimize the many variables in changing relays is a plug-n’-play retrofit [23]. The retrofit fits the same panel cutout and has the same termination jacks for the old relay wiring plugs, the blue plugs in **Error! Reference source not found.**. An adapter wires the existing plug connections to the new relay. Depth adjustment via front-panel collar keeps the wiring at the same place behind the switchgear panel, eliminating physical stress on the wiring harness (preserving reliable connections).

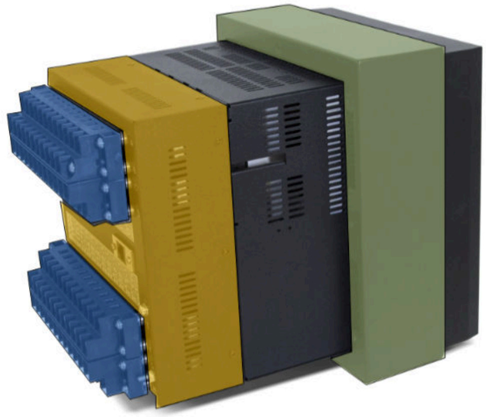


Fig. 3 Retrofit chassis adapter (orange) and reused wiring plugs (blue)

An engineer converts the old relay file to the new relay format, taking appropriate time to inspect and prove the new settings. Then, a technician changes the relay hardware, with no rewiring because the plugs from the old relay fit the new relay. Next, the technician loads the new settings file, does quick metering and trip checks, and then puts the new relay into service. Typically, the time to change the relay is 30 minutes; providing greater infrastructure availability and reliability.

VII. CONCLUSIONS

It is vitally important to address the significant threats to critical infrastructure. This is especially true for the electric-power grid because many other critical infrastructures depend on reliable electricity. Threats can come not only from bad actors targeting operational technology (OT) security, problems can occur from protective-relay design and aging. Now, cybersecurity is more robust in the IEDs, and employing cyber network best practices such as cyber-informed engineering (CEI) secures the protection, automation, and control architecture. Firmware advancements such as advanced memory-map/bit-integrity safeguards in modern microprocessor relays; misoperations data show greatly reduced incidents with new technology. Physical improvements increase reliability, with protection and control IEDs employing effective electromotive pulse (EMP) filtering and shielding, geomagnetic disturbance (GMD) monitoring and transformer-neutral DC protection, and power-supply longevity improvements. Software advances automate settings development and management, with fewer errors, which increases reliability of the electrical infrastructure. Managing protection and control IEDs as assets includes taking advantage of replaceable power supplies, securing environmental operating conditions and planning device replacement. Retrofit relays ease the effort and improve reliability when facing the eventual wear out and replacement of the devices that protect critical infrastructure.

VIII. REFERENCES

[1] U. S. Congress, 107th Congress. (2001, October 26) Public Law 107 - 56 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. Available: https://www.govinfo.gov/content/pkg/PLAW-107publ56/html/PLAW-107publ56.htm.

[2] S. Mathezer, "Introduction to ICS Security Part 3." https://www.sans.org/blog/introduction-to-ics-security-part-3/ (accessed Jan. 26, 2022).

[3] North American Reliability Council "Guidance for Secure Interactive Remote Access," July, 2011 [Online]. Available: https://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf

[4] K. Hemsley, R. Fisher, "History of Industrial Control System Cyber Incidents," Idaho National Laboratories, INL/CON-18-44411-Revision-2, Dec. 2018.

[5] National Institute of Standards and Technology, "Zero Trust Architecture," Special Publication 800-207. Aug. 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-207

[6] National Institute of Standards and Technology, "Guide to Industrial Control Systems (ICS) Security" Special Publication 800-82, May 2015. [Online] available https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

[7] L. Rosa et al., "Comprehensive Security Analysis of a SCADA Protocol: From OSINT to Mitigation," DOI 10.1109/ACCESS.2019.2906926. March 22, 2019. [Online] available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8672892

[8] R. Anderson, et al., "Cyber-Informed Engineering," Idaho National Laboratories, USDOE Office of Scientific and Technical Information, doi:10.2172/1369373. 2017 [Online] available https://www.osti.gov/servlets/purl/1369373.

[9] J. F. Ziegler and W. A. Lanford, "Effect of Cosmic Rays on Computer Memories," Science, Vol. 206, Issue 4420, pp. 776–788, Nov. 1979.

[10] I. Voloh, “DSP Analysis,” GE Grid Solutions, June, 2021, unpublished.

[11] W. Radasky, E. Savage, “High-Frequency Protection Concepts for the Electric Power Grid,” Meta-R-324, Metatech Corporation for Oak Ridge National Laboratory, 2010.

[12] National Coordinating Center for Communications (NCC), “Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment,” Version 2.2, Feb. 2019. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/19_0307_CISA_EMP-Protection-Resilience-Guidelines.pdf.

[13] North American Electric Reliability Corporation (NERC) TPL-007-4, “Establish requirements for Transmission system planned performance during geomagnetic disturbance (GMD) events” https://www.nerc.com/pa/Stand/Reliability%20Standards/TPL-007-4.pdf (accessed Jan. 26, 2022).

[14] North American Reliability Corporation (NERC), “Geomagnetic Disturbance Operations” Nov. 2013 [Online] available https://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-010-1.pdf.

[15] IEEE Power and Energy Society, “Geomagnetic Disturbances (GMD) Impacts on Protection Systems” IEEE Power System Relaying and Control Committee, K Substation Protection Subcommittee, Working Group K17, PES-TR72. Sept. 2019. [Online] Available: https://www.pes-psrc.org/kb/published/reports/PSRC%20-%20K17_Report_Final%2020190927.pdf.

[16] Department of Homeland Security, “Energy Sector-Specific Plan” 2015. [Online] Available: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf.

[17] Aspen Users Group, “Utilizing ASPEN OlxAPI for Advanced Protection Modeling and Analysis Applications,” May 2020. [Online]. Available: https://www.aspeninc.com/may2020ug/UtilizingASPENOlxAPI.pdf (accessed Jan. 26, 2022).

[18] Doble Engineering Company, “Powerbase” https://www.doble.com/product/powerbase/ (accessed Jan. 26, 2022).

[19] GE Renewable Energy, “Device Management DvM” ____________________________(accessed Jan. 27, 2022).

[20] D. Ransom, “Upgrading Relay Protection?—Be Prepared,” presented at the 49th IEEE/IAS Industrial and Commercial Power Systems Technical Conference, Stone Mountain, GA USA, May 2013. **DOI:** 10.1109/ICPS.2013.6547351.

[21] D. Williams, “Calculating the Lifespan of Electrolytic Capacitors with De-Rating” All About Circuits, Dec. 26, 2016. [Online]. Available: https://www.allaboutcircuits.com/news/calculating-the-lifespan-of-electrolytic-capacitors-with-de-rating/ (accessed Jan. 26, 2022).

[22] GE Grid Solutions “Multilin 8 Series – Application Note,” [Online] available https://www.gegridsolutions.com/products/applications/8series/850_comprehensive_equipment_monitoring.pdf (accessed Jan. 26, 2022).

[23] GE Grid Solutions “Multilin 8 Series Retrofit,” https://resources.gegridsolutions.com/distribution-protection/multilin-8-series-retrofit (accessed Jan. 26, 2022).

IX. VITAE

Daniel (Dan) Ransom, PE has many years of industrial and utility power-systems experience, specializing in protection products development and applications support. He has worked as an engineer in power systems and in communications systems. Dan is an engineering graduate, BSEE, of Gonzaga University, Spokane, Washington. In addition, he holds a liberal-arts degree from Washington State University, Pullman. Dan is a Senior Member of the IEEE, with membership and participation in the Industry Applications Society, Power and Energy Society, Communications Society, and in the IEEE Standards Association. To date, he has one US patent. He is a licensed, professional engineer in numerous USA states. Dan is a Senior Technical Application Engineer at GE Grid Solutions/GE Renewable Energy, in Tacoma, Washington USA.