Resetting Protection System Complexity

Edmund O. Schweitzer, III and David E. Whitehead
Schweitzer Engineering Laboratories, Inc.

Revised edition released October 2019

Originally presented at the
46th Annual Western Protective Relay Conference, October 2019

Resetting Protection System Complexity

Edmund O. Schweitzer, III and David E. Whitehead, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—In 1962, A. R. van C. Warrington wrote in his seminal book, *Protective Relays – Their Theory and Practice*: "Whereas the main requirement of instrumentation is sustained accuracy, the most important requisite of protective relays is *reliability* since they may supervise a circuit for years before a fault occurs; if a fault then happens, the relay must respond instantly and correctly. For this reason the designers should always attempt to use simple constructions and simple connections of relays. In spite of good intentions in this respect, there is a tendency to extend the operation of relay schemes by adding additional features until complexity results and then it becomes necessary to re-design. In other words, a graph of the progress of relay engineering as regards complexity tends to follow a sawtooth shape." [1]**

In 1984, the world's first microprocessor-based relay reset our industry with simpler construction methods, self-tests, better fault-detection sensitivity, and simple human-machine interfaces consisting of serial ports, a modest set of commands, and less than a page of settings. The new technology was solidly embraced; however, the desire for the inclusion of more features began to drive up complexity that included capabilities such as integration, automation, metering, SCADA protocols, synchrophasors, and sampled values. Today, the amount of code performing automation and communications in a protective relay is nine times larger and more complicated than the code performing the protection algorithms.

As Warrington predicted, the saw-tooth shape of protection complexity has continued to increase, so it is fair to ask:

- **Is today's power system protection too complex?**
- **Is complexity a natural and unavoidable consequence of advancing power system protection?**
- **Is protection, automation, and communication in single devices advantageous, or should these functions be separated into dedicated devices?**

I. Introduction

Fig. 1 shows a simplified diagram of the protection, automation, communications, and associated equipment in a substation at one end of a transmission line.

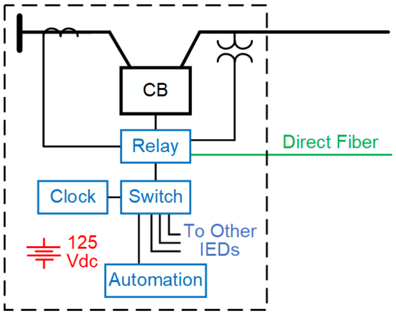

Fig. 1. Simplified Substation Protection, Automation, and Communications Diagram

Elements shown in Fig. 1 include the following:

- **Sensor and Actuators.** These elements measure and control physical systems, e.g., voltage and current transducers and circuit breakers.
- **Relays.** Relays monitor the power system for faults. When a fault is detected, relays issue commands to circuit breakers to clear the fault.
- **Automation.** Automation elements integrate, combine, process, and issue commands to drive the power system to a desired state and provide visibility to operators as part of SCADA systems.
- **Communications.** Communications elements convey information between protective devices, automation devices, and local operator HMIs.
- **Clock.** Clocks generate precise time codes for time-stamping reports, and in some cases, time is used to align data for use in automation and protection functions.
- **Power Supply.** This centralized power source powers devices in substations. Power supplies typically contain batteries in order to continue to provide power in the event that primary power is unavailable.

II. History or How We Got Where We Are

In the 1900s, Edison, Insull, Westinghouse, Tesla, and others created the power system we are familiar with today. Applying theory with the technology available at the time, they developed power systems that safely and economically generate and distribute electric power.

While technology for protecting power systems has advanced, power system protection principles have essentially remained the same for decades. Fig. 2 is a timeline of the advancements in power system protection.

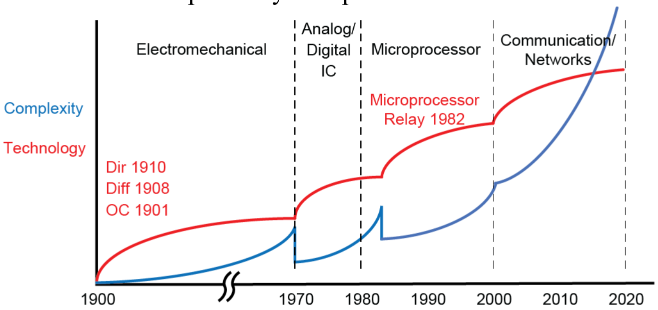

Fig. 2. Timeline of Protection

A. *Evolution of Protection*

Many of the principles presently used in electromechanical relays were developed during the first part of the 20th century, such as overcurrent, directional, distance, and differential protection [2]. Electromechanical relay targets provide little information about what happened to the power system.

In the 1980s, with the advancement of microprocessors, protective relay algorithms were implemented in the first commercially available microprocessor-based relay.

Microprocessor-based protection offered not only the protective features of electromechanical relays but also additional protection innovations, such as negative-sequence overcurrent protection, providing more sensitive fault detection and load encroachment to prevent tripping on load. Microprocessor relays provided innovations not possible with electromechanical and solid-state technology, including locating faults, reporting events, self-testing, and communications. A disadvantage is that cyber risks emerged, but those risks were mitigated from the beginning by multiple levels of password protection, alarm contacts responding to frequent password attempts, firmware locks and checksums, and at the system level, encrypting modems, SCADA-controlled relays isolating the dial-up line from the modems, dial-back modems, etc.

Relays continued to evolve, adding multiple settings groups, more communications capabilities, more protocols, and more automation capabilities. These advancements have also resulted in additional complexity. Table I shows the expanding complexity of relay software.

TABLE I
ADDING CAPABILITIES DRIVES RELAY COMPLEXITY

Year	Capabilities	KLOC[a]	Percent Protection Code
1982	4 samples per cycle, simple serial proprietary protocols	20	40
1996	16 samples per cycle, serial communications, SCADA protocols	80	27
2005	8,000 samples per second, Ethernet, GOOSE[b], MMS[c], DNP3[d]	500	10
2018	8,000 samples per second, Ethernet, GOOSE, MMS, DNP3, sampled values, PTP[e]	600	7

[a] Thousands of lines of code
[b] Generic Object-Oriented Substation Event
[c] Manufacturing Message Specification
[d] Distributed Network Protocol
[e] Precision Time Protocol

B. Evolution of Automation in Protection

Power system automation systems began in the 1920s. They consisted of control and monitoring boards located in the power plant and substation. In the 1930s, utilities began interconnecting their systems to reduce operating costs and improve reliability. To provide better system visibility, analog technologies were developed that monitored and controlled generator output, tie-line power flows, and frequency [3].

In the 1950s, analog computers were developed to schedule generation for each generator in order to provide the lowest cost of generation. These special purpose computers were the beginning of Energy Management Systems (EMSs). In the late 1960s, digital computers and software were developed to replace the analog EMSs. Automation systems began applying remote terminal units (RTUs) in the late 1970s and early 1980s. RTUs measure analog and digital quantities and transmit telemetry back to a SCADA master and EMS.

In 1985, a protective relay terminal unit (PRTU) was released. It was the first device to communicate to multiple relays. The PRTU integrated relay data with SCADA, thus reducing the need for RTUs in the substation.

Today's automation devices have evolved into sophisticated computing platforms that include advanced programming languages such as IEC 61131; dozens of IEEE, IEC, and proprietary protocols; and a multitude of input and output sensor options, e.g., RTDs, analog, and digital. Table II shows the expanding complexity of automation software.

TABLE II
ADDING CAPABILITIES DRIVES AUTOMATION COMPLEXITY

Year	Capabilities	KLOC
1985	Communications gateways and time distribution	10
1995	Basic programmability, a few protocols, digital I/O type	110
2010	Advanced programmability, multiple protocols, many I/O interfaces	12,000

C. Evolution of Communications for Protection

Communications within power systems began with simple contact inputs and outputs. Breaker status was displayed in a control house by using a contact output (that represented the state of a circuit breaker) wired to a light bulb with a voltage source. Similarly, a relay contact wired to the trip coil of a circuit breaker with a voltage source was all that was required to communicate the trip command. Still today, these communications circuits are simple, reliable, and easy to troubleshoot.

As communications technologies advanced, new communications-based protection schemes were introduced, both pilot and line-current differential schemes. Communications also allowed remote access to event reports, sequence-of-events reports, metering, breaker status, and other data.

Networking technologies were implemented and included telephone modems over leased lines, dial-up networks, power-line carrier, direct fiber, time-division multiplexed communications, licensed and unlicensed radio, and Ethernet.

With the introduction of oscillography and sequence-of-events reports, it became advantageous to time-stamp these reports in order to compare records generated by devices throughout a power system. Initially, devices used an internal clock to provide the time stamp. However, internal clocks are subject to clock drift, resulting in differing time stamps produced by devices measuring the same event.

In 1956, the Tele-Communication Working Group (TCWG) of the American Inter Range Instrumentation Group (IRIG) created a standard format for distributing synchronized time signals that resulted in IRIG Document 104-60 [4]. In 1984, relays included the IRIG time code function, resulting in events synchronized to within milliseconds of each other.

On January 6, 1980, the U.S. Naval Observatory began operation of the Global Positioning System (GPS). The GPS provides an accurate position nearly anywhere in the world and also accurate time. Satellite clocks produce various time outputs including IRIG, pulses per second, and Ethernet-based time protocols such as Simple Network Time Protocol (SNTP) and Precision Time Protocol (PTP) with accuracies in the tens of nanoseconds.

While satellite clocks have been broadly adopted in power system protection designs, they are susceptible to interference from space weather, signal jamming, or spoofing. To address these vulnerabilities, a deterministic wide-area terrestrial communications system was released in 2011, capable of time distribution accuracy in the tens of nanoseconds.

Just as relay complexity has increased, so has the time distribution system. Early timing systems consisted of digital logic and did not include software. Now, satellite clocks support IRIG, SNTP, and PTP and require millions of lines of code. Table III illustrates the growth of clock code complexity.

TABLE III
ADDING CAPABILITIES DRIVES TIMING COMPLEXITY

Year	Capabilities	KLOC
1989	Time distribution module	0
2005	GPS satellite clock, IRIG, and pulse outputs	150
2015	Multiconstellation satellite, IRIG, SNTP, PTP, and pulse outputs	17,000

III. WHERE POWER SYSTEM PROTECTION WILL END UP IF LEFT ON THE PRESENT TRAJECTORY

Today's protection systems are impressive because they are:

- **Fast.** Phasor-based relays detect and trip in 8 to 16 ms. Time-domain relays trip in under 2 ms.
- **Automated.** Remote systems collect, process, and issue commands without the need for human intervention.
- **Interconnected.** Communications systems are prevalent within protection systems, allowing the exchange of protection, SCADA, and engineering access information.
- **Flexible.** Programmability of relays, automation controllers, switches, and other devices within substations provides for customized protection and automation schemes.

The digital technology used in protection, automation, and communications opened many new doors. Suppliers and customers worked together solving problems, increasing performance, and improving protection, control, monitoring, automation, and communications.

Things became more and more complex in the process—just as Warrington had observed half a century earlier.

Are we not finding that it has become, in Warrington's words, "necessary to re-design" again? Can we once again reset complexity?

IV. QUANTIFYING POWER SYSTEM COMPLEXITY

Warrington stated, "the most important requisite of protective relays is *reliability*." As we add more protocols, as we sample faster and faster, as we add features, as we add features to features, *and* as we continue to support everything in anything … we are exponentially increasing complexity. Let's quantify this complexity and its effects on availability by using Fault Tree Analysis [3].

Reference [5] describes how to calculate unavailability from a failure rate along with the time required to detect and repair the failure.

$$q \cong \lambda T = \frac{T}{MTBF}$$

where:

q is unavailability
λ is some constant failure rate
T is the average downtime per failure
$MTBF = \frac{1}{\lambda}$ is Mean Time Between Failures.

Each failure causes downtime T. Therefore, the system is unavailable for time T out of total time MTBF. The fraction of time the system is not available is T/MTBF. For the purpose of this analysis, failures are attributed to hardware, software, or misapplication (human factors such as settings errors).

Using the work in [3], we define the unavailability of various substation components in Table IV, including automation, a clock, and a switch. Modern relays share many of the same components used in automation, clocks, and switch hardware. Also, the same design practices and type test standards applied to relays are also applied to automation, clocks, and switches. Therefore, it is reasonable to assign the relay hardware unavailability to those devices.

TABLE IV
HARDWARE-CAUSED UNAVAILABILITY

Component	Unavailability • 10^{-6}
Circuit Breakers	300
Protective Relay Hardware	100
Automation Hardware	100
Clock Hardware	100
Switch Hardware	100
Fiber Channel	100
DC Power System	50
CT (per phase)	10
PT (per phase)	10

When [3] was written, the authors considered human errors, such as settings errors or misapplications, a cause of unavailability and calculated a value 100 • 10^{-6}. The unavailability value was based on a protective device with code of 100 KLOC. If we assume that the opportunity for human error scales linearly with the number of settings in a device (this is a conservative assumption), and the number of device settings scales linearly with KLOCs, we can compute the unavailability caused by human errors for various KLOC code base sizes, as shown in Table V.

TABLE V
HUMAN ERROR-CAUSED UNAVAILABILITY

KLOC	Unavailability • 10^{-6}
100	100
500	500
800	800
1,000	1,000
1,500	1,500
2,000	2,000
2,500	2,500
3,000	3,000
3,500	3,500
4,000	4,000

Finally, we extend the work in [3] to address unavailability caused by coding errors. As code size grows, the opportunity for coding errors increases. For the purpose of calculating unavailability caused by coding errors, we assume the following based on 35 years of protection system firmware development:

1. Software defects manifest themselves as one unavailability event per year for a 100 KLOC device that results in 100 • 10^{-6} unavailability.
2. Our experience is that coding errors don't grow linearly with KLOCs; rather, coding errors increase at a rate closer to the square root of KLOCs.

Table VI defines the unavailability of devices based on software-caused errors.

TABLE VI
SOFTWARE-CAUSED UNAVAILABILITY

KLOC	Unavailability • 10^{-6}
100	100
500	223
800	282
1,000	316
1,500	387
2,000	447
2,500	500
3,000	547
3,500	591
4,000	632

To examine the effects of complexity on unavailability, consider the following two protection system topologies:

- System 1: Conventional Line Current Differential Protection Scheme
- System 2. Sampled Values Line Current Differential Protection Scheme

A. *System 1: Conventional Line Current Differential Protection Scheme Unavailability Calculations*

Fig. 3 shows two substations performing protection on a transmission line. In this example:

1. The relaying protection scheme is line current differential (87L). The 87L communication is via direct fiber.
2. The relays include automation functions and programmable logic, Ethernet communications, IEEE C37.94 communications, and protocols such as DNP3, IEC 61850, IRIG-B, and PTP. The code base for this type of relay is 800 KLOC.
3. Network switches used for communications within the substation have a code base of 4,000 KLOC.
4. The clock used for time distribution within the substation has a code base of 4,000 KLOC.
5. An automation controller used for SCADA, event collection, etc. has a code base of 2,000 KLOC.

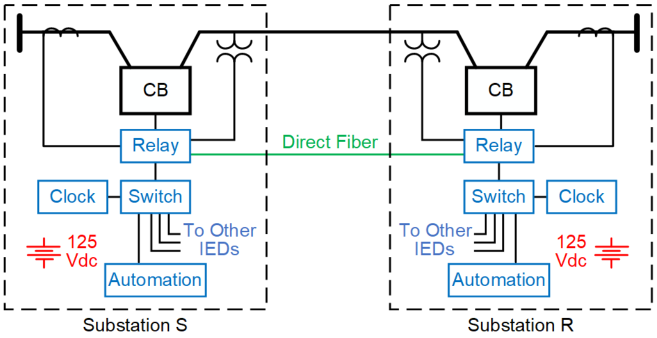

Fig. 3. System 1 Line Protection Substation Configuration

In this example, the relays performing line-current differential protection do not require external time synchronization or communication with other devices, except for the direct fiber connection between the two relays. As a result, the network switch, clock, and automation controller—while providing time synchronization, automation, and SCADA connectivity—are not critical for detecting and clearing faults. Therefore, the fault tree analysis and unavailability calculations do not include those devices. Fig. 4 shows the elements required to detect and clear a fault.

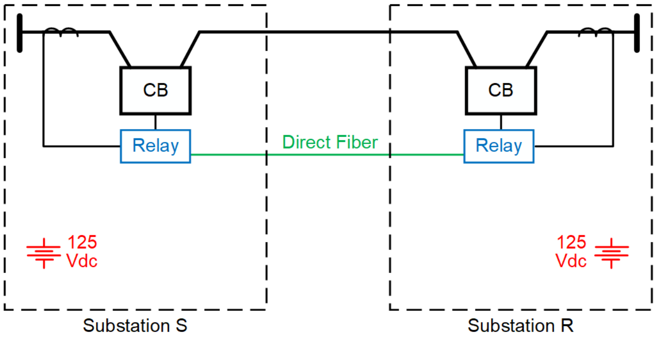

Fig. 4. Protection Elements Required to Detect and Clear a Fault

While the automation, switches, and clocks are not required for detecting faults, the code in the relay and associated user settings still contribute to the unavailability of the relays, i.e., an application error in an Ethernet protocol could cause relay unavailability. Fig. 5 depicts the System 1 line current differential protection fault tree.

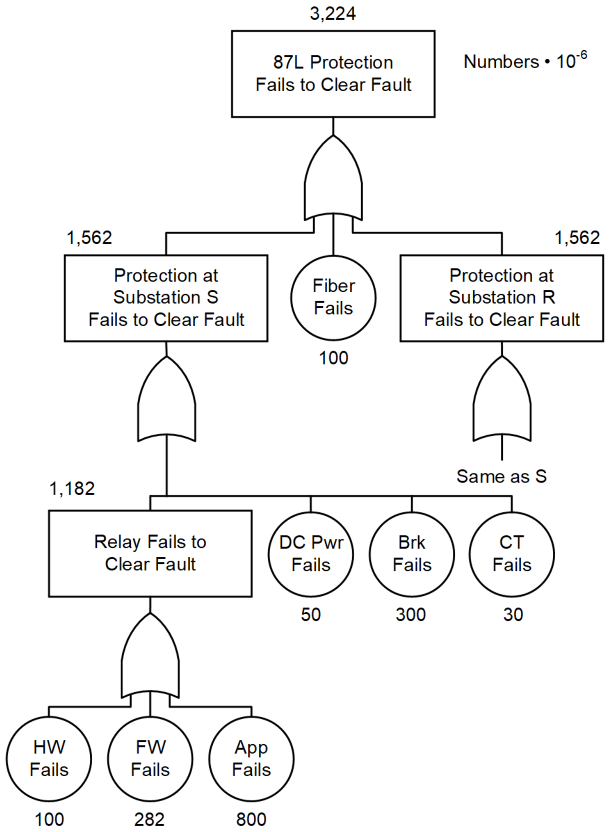
3,224
87L Protection Fails to Clear Fault
Numbers • 10^-6
1,562
Protection at Substation S Fails to Clear Fault
Fiber Fails
100
1,562
Protection at Substation R Fails to Clear Fault
Same as S
1,182
Relay Fails to Clear Fault
DC Pwr Fails
50
Brk Fails
300
CT Fails
30
HW Fails
100
FW Fails
282
App Fails
800

Fig. 5. System 1 Line Current Differential Protection Fault Tree Analysis

Using the same unavailability example in [3], the protection scheme is applied on 100 transmission lines, and each line has 10 faults per year, resulting in 1,000 faults per year. Given the unavailability calculation of 3,224 • 10^{-6} and 1,000 faults, we could expect that 3 to 4 faults per year are not cleared by the line current differential scheme. This example does not include other protection elements, such as backup protection within the relay, like distance elements, or a secondary relay that could detect and clear the fault when the line current protection scheme is unavailable.

B. System 2 Sampled Values Line Current Differential Protection Scheme Unavailability Calculations

Fig. 6 shows two substations performing protection on a transmission line. In this example:

1. The relaying protection scheme is line current differential (87L). The 87L communication is via direct fiber.
2. The relays include automation functions and programmable logic, Ethernet communications, IEEE C37.94 communications, and protocols such as DNP3, IEC 61850, IRIG-B, and PTP. The code base for this type of relay is 800 KLOC.
3. Merging units (MU) are data acquisition devices that require Ethernet networks and precise time to convey information such as volts and amperes to the relay. The MUs have a code base of 100 KLOC.
4. Network switches used for communications within the substation have a code base of 4,000 KLOC.
5. The clocks used for time distribution within the substation have a code base of 4,000 KLOC.
6. An automation controller used for SCADA, event collection, etc. has a code base of 2,000 KLOC.

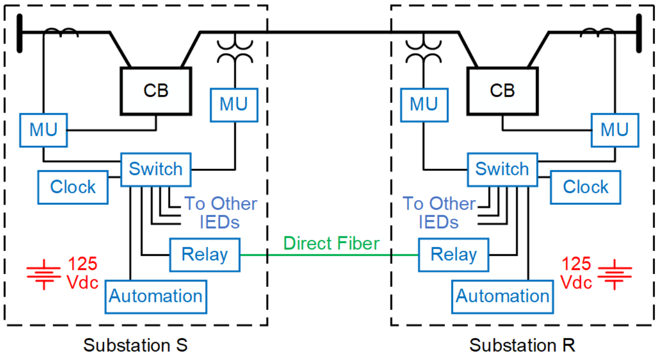

Fig. 6. System 2 Sampled Values Line Protection Substation Configuration

In this example, the network switch and clock, along with the relay and merging units, are required for protection. Again, the automation controller provides automation functionality and visibility to SCADA, but it is not critical for detecting and clearing faults.

Fig. 7 depicts the System 2 sampled values line current differential protection scheme, and Fig. 8 shows the associated fault tree.

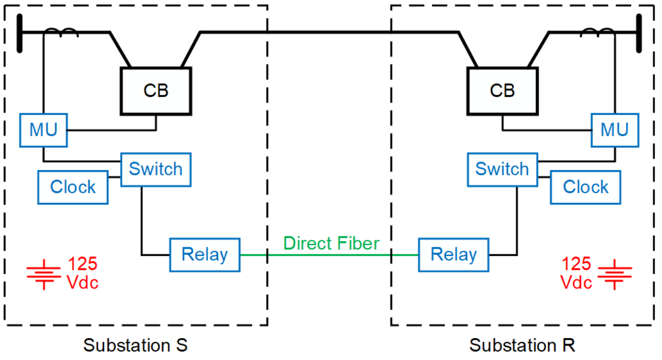

Fig. 7. System 2 Sampled Values Line Current Differential Protection Scheme

Again, assume this scheme is used on 100 transmission lines and each line has 10 faults per year, resulting in 1,000 faults per year. Given the unavailability calculation of 23,820 • 10^{-6} and 1,000 faults, we could expect that 23 to 24 faults per year are not cleared by the line current differential scheme. This increase in unavailability is six times the unavailability of the conventional line current differential scheme.

This example does not include other protection elements, such as backup protection within the relay, like distance elements, or a secondary relay that could clear the fault.

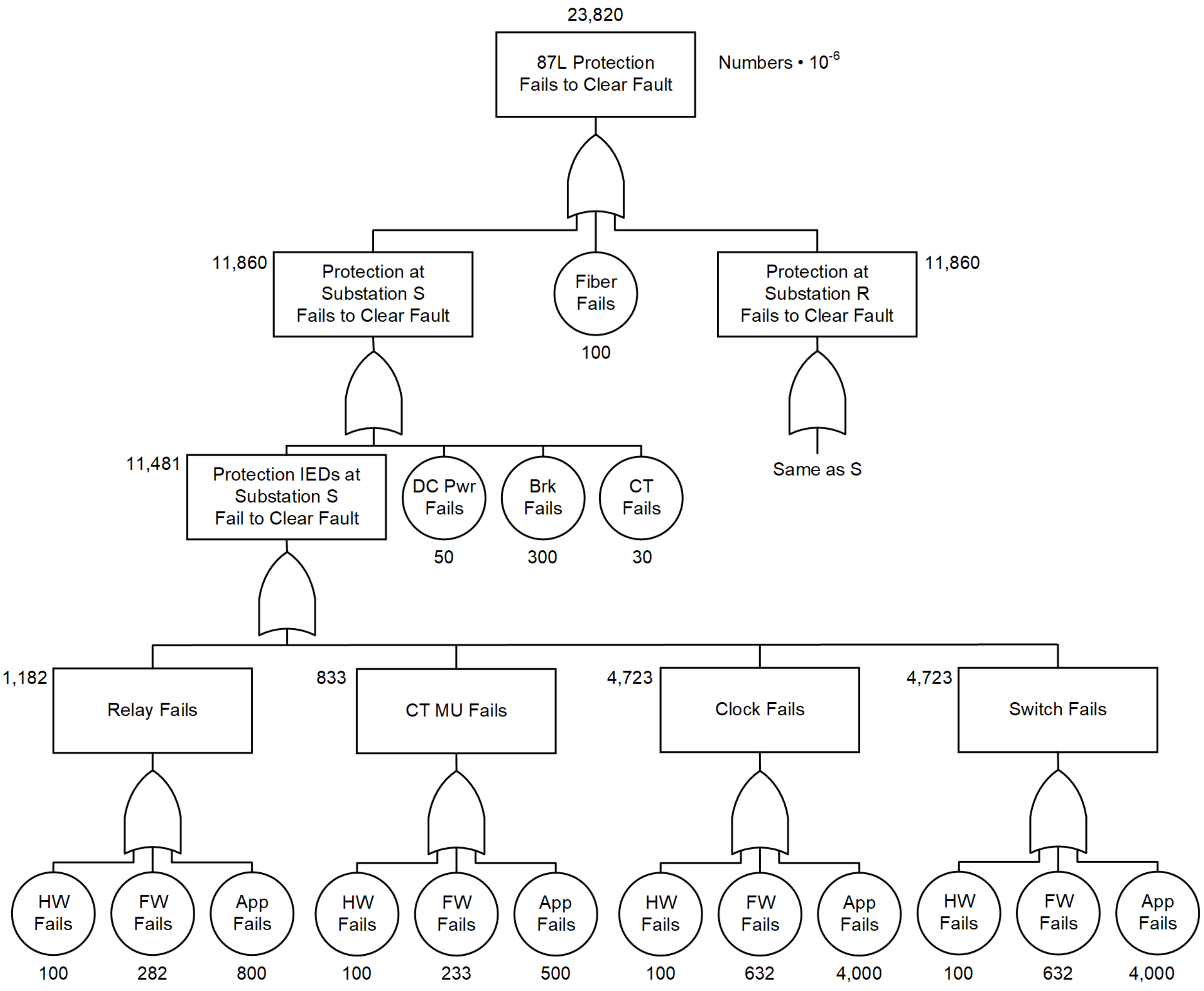

Fig. 8. System 2 Sampled Values Line Current Differential Protection Fault Tree Analysis

This analysis shows that using more devices that are more complicated increases the unavailability of protection systems. Of course, designs can be developed to reduce the unavailability of a protection system, e.g., adding backup protection, incorporating triple modular redundancy (TMR), etc., all of which increase the failure rates, cost, and complexity of protection systems.

Is there an opportunity to reset the complexity curve and still achieve high-speed, sensitive, selective, and simple protection systems that provide automation, system visibility, and cybersecurity? We believe the answer is YES!

V. Resetting the Complexity Curve

"…the designers should always attempt to use simple constructions and simple connections of relays." [1]

Putting protection, automation, protocols, and communications features together into *each* and *every* protective relay comes at a cost. Setting a modern relay requires an individual to be an expert at protection, Ethernet, time codes, programmable logic, communications protocols, network design, cybersecurity, and so on. Not only does the person setting the relay need to be a power system engineer, but a process control expert and a computer scientist too.

Following Warrington's advice, let's design a protection system with the following requirements.

A. Protection: Optimized for Simplicity, Dependability, Reliability, and Performance

Protective relays are special-purpose instruments that measure voltages, currents, and the state of contacts, and they exchange information for the purpose of protection. When the power system faults, the relays must trip circuit breakers FAST and selectively to isolate the problems and not cause excessive loss of service in the process. All other capabilities added to a relay, such as automation and communications features, while providing some advantages, also increase complexity. Further, many automation and communications features expose relays to cyber threats. Taking these observations into consideration, the relay requirements should consist of the following:

- Only protection features. This results in the following:
  - Simpler hardware

  - Less code, which reduces firmware errors
  - Fewer settings, which reduces application settings errors
- A single and simple protocol to communicate with automation or other relays. It is not desirable to use common Ethernet protocols such as IP because of large cybersecurity threat vectors. A single, simple protocol simplifies the design and increases cybersecurity effectiveness.
- The ability to perform unit protection, e.g., include line, bus, and transformer protection in a single device. Don't separate the relay into two devices. This adds cost and complexity. If copper reduction is desirable, place the relays in the substation yard.
- Protection that is not dependent on absolute time. While precise time is valuable, relay protection schemes should not be dependent on external time sources.
- A faster turn-on speed. High-performance relays start in 5 to 10 seconds; others require a minute or more before protection is enabled after power is applied. In the future, relays should start in a second. A faster turn-on speed means higher availability.

By keeping the relay simple, we estimate that the code size can be kept under 100 KLOC. This results in the unavailability numbers shown in Table VII.

TABLE VII
RELAY UNAVAILABILITY

100 KLOC	**Unavailability • 10^{-6}**
Hardware	100
Software	100
Application	100

B. Automation: Integrated SCADA, Automation, and Protocols

The automation controller (AC) is the SCADA interface that provides local automation function. The AC attributes include:

- The simple protocol described above to send data to and receive data from relays. Data types include metering, event reports, sequence-of-events reports, time synchronization, and engineering access.
- To integrate with SCADA, the AC supports traditional protocols, e.g., DNP3, IEC 61850, and MMS.
- The AC is the interface between a user and a relay. From a cybersecurity perspective, this requirement reduces cybersecurity threat vectors to a single device in the substation, versus requiring that all the cybersecurity features be put in all the devices in a substation.
- Failure of the AC does not impact protection.

The unavailability of the AC uses a code base of 4,000 KLOC. The AC code base is large because the AC includes automation functions, multiple communications protocols, and cybersecurity protocols. A large code base is acceptable for the following reasons:

- The increased complexity of the AC is limited to a single device that is not critical to protection.
- Keeping the protocols in the AC results in relays that are simpler and have a higher reliability.
- Cyber threats are managed in the AC and do not need to be managed in the relays.
- The system unavailability is lowered by using a design with simple relays and an AC that performs the automation functions.

Table VIII shows the automation controller unavailability for the simple system.

TABLE VIII
AUTOMATION CONTROLLER UNAVAILABILITY

4,000 KLOC	**Unavailability • 10^{-6}**
Hardware	100
Software	632
Application	4,000

C. Communications: Designed for Resiliency, Determinism, and Cybersecurity

Communications in this system is kept simple and has the following attributes:

- Communications between the relays and AC is a fixed dataset and not based on an Ethernet standard for cybersecurity purposes. A fixed dataset communications system lends itself to deterministic communications links.
- Communications between the relays and AC is point-to-point. This eliminates the need for programing network configurations and eliminates code and settings.
- Communications between the AC and SCADA does include standard networking interfaces and protocols such as DNP3 or MMS.
- Failure of the communications network between the AC and SCADA doesn't impact protection.
- It is acceptable that a communications failure may impact SCADA or remote access to the AC and relays.

The code base for a communications switch is 4,000 KLOC. Table IX shows unavailability caused by hardware, software, and application failures.

TABLE IX
COMMUNICATIONS UNAVAILABILITY

4,000 KLOC	**Unavailability • 10^{-6}**
Hardware	100
Software	632
Application	4,000

D. *Segregation: Separate Protection, Automation, and Communications Functions*

Presently, power system protective devices consist of many overlapping features that require domain-specific expertise to set them properly. Table X shows an example of the number of settings needed for the relays in System 1 and System 2.

TABLE X
EXAMPLE NUMBER OF PROTECTION, AUTOMATION, AND COMMUNICATIONS SETTINGS IN RELAYS

Relay	Protection	Automation	Comms
System 1	1,200	5,500	1,600
System 2	1,200	6,100	2,300

Separating protection, automation, and communications into individual devices provides the following benefits:

- Protection, automation, and communications experts can set and test their devices with minimal overlap from the other disciplines.
- With the simplified protection approach, we remove the requirement that protection engineers need to be experts in automation or network design.

Table XI shows an example of the number of settings needed for a *Simple* relay with segregation of protection, automation, and communications.

TABLE XI
EXAMPLE NUMBER OF SETTINGS FOR THE SIMPLE RELAY

Relay	Protection	Automation	Comms
Simple System	600	50	50

E. *Testing: Devised Easy Testing and Maintenance*

Separating protection, automation, and communications functions into individual devices simplifies testing. With traditional relays, when making settings changes, you must consider the potential impacts on the automation and communications within the relay because all three processes interact within the same device. With the simplified system and its segregation of protection, automation, and communications, the analysis of protection settings changes is limited to the relay.

Maintenance costs are reduced. If we assume there is a problem in the SCADA protocol implemented in the relays that requires a firmware upgrade, all the relays in the substation must be taken out of service during the upgrade. In our simplified substation, only the AC would be taken out of service for a SCADA protocol upgrade and the relays would remain in service during the AC firmware upgrade. Referring to Section II, the KLOC of code for protection is 10 percent, versus 90 percent for nonprotection. The likelihood of the automation and the communications portion of the code having a firmware error is nine times greater than the protection code. The simplified protection system has many more relays than ACs. Eliminating nonprotection features from relays results in less upgrades, which results in a large maintenance savings.

The Simple substation described by the design criteria above is shown in Fig. 9. While this architecture is like System 1, the following differences are significant:

- The Simple relay in Fig. 9 has a sixth of the code as the relay shown in Fig. 3.
- Point-to-point communications between the Simple relay and automation with a defined data packet provides deterministic communications and improves cybersecurity. Note the fiber links between the Simple relay and automation to reduce electromagnetic interference.
- The Simple relay is suitable for installation in traditional control houses or in the substation yard.

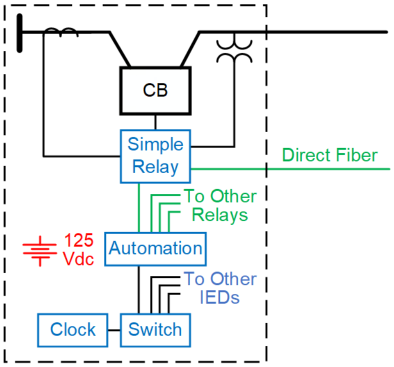

Fig. 9. Simple Protection System Substation Configuration

Returning to the line current differential unavailability example, the automation, switch, and clock are removed from Fig. 9 as they are not necessary to clear a fault. Fig. 10 shows the equipment used in the unavailability calculation. Fig. 11 shows the Simple protection system fault tree.

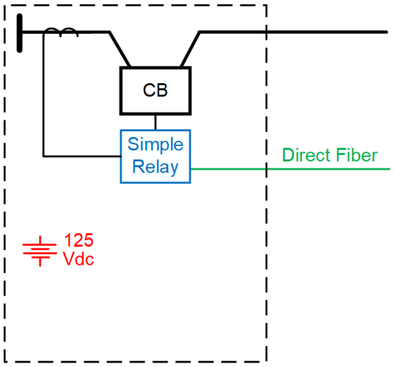

Fig. 10. Simple Protection System Elements Required to Detect and Clear a Fault

Again, assume this scheme is used on 100 transmission lines and each line has 10 faults per year, resulting in 1,000 faults per year. Given the unavailability calculation of $1,460 \cdot 10^{-6}$ and 1,000 faults, we could expect that 1 to 2 faults per year are not cleared by the line current differential scheme. This is a 2x to 4x improvement in reducing unavailability compared to the conventional line current differential system and a 24x improvement in reducing unavailability compared to the sampled values system.

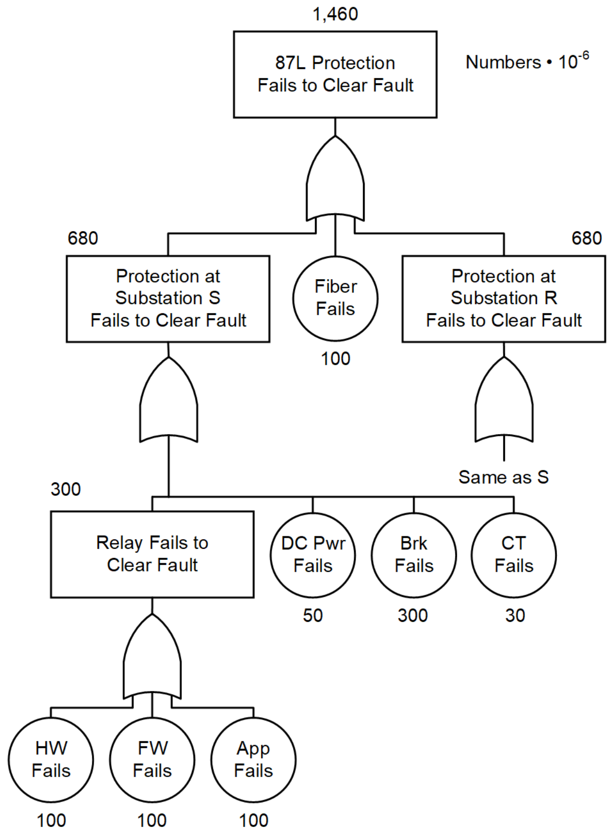
1,460
87L Protection Fails to Clear Fault
Numbers • 10^{-6}
680
Protection at Substation S Fails to Clear Fault
Fiber Fails
100
680
Protection at Substation R Fails to Clear Fault
Same as S
300
Relay Fails to Clear Fault
DC Pwr Fails
50
Brk Fails
300
CT Fails
30
HW Fails
100
FW Fails
100
App Fails
100

Fig. 11. Simple Line Current Differential Protection System Fault Tree Analysis

VI. Conclusion

Modern protection systems have advanced to a point where faults are quickly and accurately cleared, tasks that used to require human input have been automated, and information created at one point in a power system can be shared with multiple devices and processes throughout the power system nearly instantaneously. Power systems are technological marvels.

However, as protection has become faster, automation more prevalent, and communications wide-spread, protection systems have become more complex. The increase in functionality and features has driven complex hardware designs, more code in devices, and more settings that engineers must understand and configure. This complexity ultimately makes systems less reliable.

In this paper, we've shown that the trend in power protection system development is increasing complexity, and that complexity will result in more protection unavailability by a factor of six.

To address this alarming trend, we described a protection system that simplifies the relay to only include protection functions and places the automation and communications applications in other devices. This architecture demonstrates the following benefits:

- Protection system unavailability that is four times better than modern protection systems and twenty-four times better than trending protection system designs.
- Settings simplification by a factor of twelve.
- Reduction of the cybersecurity threat vector from every device in the substation to just a few by removing IT protocols from the relays.

As Warrington suggested, complexity grows until it is necessary to redesign. Now is that time.

VII. References

[1] A. R. van C. Warrington, *Protective Relays: Their Theory and Practice*, Volume One, Chapman and Hall Ltd., London, 1968, pp 11–12.

[2] Z. Q. Bo, X. N. Lin, Q. P. Wang, Y. H. Yi and F. Q. Zhou, "Developments of Power System Protection and Control," *Protection and Control of Modern Power Systems*, Volume 1, Article number: 7 (2016).

[3] E. O. Schweitzer, B. Fleming, T. Lee, and P. Anderson, "Reliability Analysis of Transmission Protection Using Fault Tree Methods," proceedings of the 24th Annual Western Protective Relay Conference, Spokane, WA, October 1997.

[4] K. Behrendt and K. Fodero, "The Perfect Time: An Examination of Time-Synchronization Techniques," proceedings of the 32nd Annual Western Protective Relay Conference, Spokane, WA, October 2005.

[5] N. H. Roberts, W. E. Vesely, D. F. Haasl, and F. F. Goldberg, "Fault Tree Handbook," NUREG-0492m U.S. Nuclear Regulatory Commission, Washington DC, 1981.

VIII. Biographies

Dr. Edmund O. Schweitzer, III is recognized as a pioneer in digital protection and holds the grade of Fellow in the IEEE, a title bestowed on less than one percent of IEEE members. In 2002, he was elected as a member of the National Academy of Engineering. Dr. Schweitzer received the 2012 Medal in Power Engineering, the highest award given by IEEE, for his leadership in revolutionizing the performance of electrical power systems with computer-based protection and control equipment. In 2019, Dr. Schweitzer was inducted into the National Inventors Hall of Fame for his invention of the first digital protective relay. Dr. Schweitzer is the recipient of the Regents' Distinguished Alumnus Award and Graduate Alumni Achievement Award from Washington State University and the Purdue University Outstanding Electrical and Computer Engineer Award. He has also been awarded honorary doctorates from both the Universidad Autónoma de Nuevo León, in Monterrey, Mexico, and the Universidad Autónoma de San Luis Potosí, in San Luis Potosí, Mexico, for his contributions to the development of electric power systems worldwide. He has written dozens of technical papers in the areas of digital relay design and reliability and holds more than 200 patents worldwide pertaining to electric power system protection, metering, monitoring and control. Dr. Schweitzer received his bachelor's and master's degrees in electrical engineering from Purdue University, and his doctorate from Washington State University. He served on the electrical engineering faculties of Ohio University and Washington State University, and in 1982, he founded Schweitzer Engineering Laboratories, Inc. (SEL), to develop and manufacture digital protective relays and related products and services.

David E. Whitehead is chief operating officer at Schweitzer Engineering Laboratories where he oversees the company's global operations. For more than a decade, Whitehead led the SEL Research and Development Division, an 800-person multidisciplinary team responsible for the research, design, development, and testing of systems that manage, monitor, and control critical electric infrastructure. A recognized leader in utility and industrial control system cybersecurity, Whitehead has testified before the U.S. Senate and the Federal Energy Regulatory Commission on the importance of innovation and protecting against cyberattacks. He has presented at numerous cybersecurity conferences and authored dozens of papers on the topic. Since joining SEL in 1994, he has been a driver of product and talent development and been instrumental in the development of the steady stream of inventions to come out of SEL. He has been awarded more than 73 patents around the world. Whitehead received his BSEE from Washington State University and his MSEE from Rensselaer Polytechnic Institute. He is a senior member of IEEE and a registered Professional Engineer in Washington, New York, Michigan, and North Carolina.

20191014 • TP6932-01