Safety Impact of Instrumentation and Control Systems

Gary Scheer and Mark Zeller
Schweitzer Engineering Laboratories, Inc.

Presented at the
8th Annual Western Power Delivery Automation Conference
Spokane, Washington
April 11–13, 2006

Safety Impact of Instrumentation and Control Systems

Gary Scheer and Mark Zeller, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—The engineers designing and applying automation, control, protection, and monitoring systems often provide a business case for each project based on savings due to improved efficiencies and reduced downtime. These instrumentation and control (I&C) systems can also improve the safety of personnel and others; improved safety can be another clear benefit of an I&C project, and help to justify the case for the overall system, or for specific components, features, or subsystems in the project. Most importantly, I&C system design decisions can help reduce deaths and injuries.**

I. Introduction

Instrumentation and Control (I&C) systems gather, save, and present useful information and provide the mechanisms for automatic and manual control of processes, systems, and devices. Some electric power industry I&C systems:

- Supervisory Control and Data Acquisition (SCADA) systems include components in substations, on power poles, in underground vaults, and in control centers.
- Substation automation systems include substation SCADA functions, plus local automatic control and human-machine interfaces.
- Plant Distributed Control Systems (DCS) include devices throughout a generating plant and in the plant control room.
- Other data acquisition and equipment monitoring systems include components in underground vaults, at water-intake sites, in electrical apparatus, on poles, and at other sites.

I&C systems help operators to efficiently operate plants and systems, determine the root causes of problems, and prevent damage and downtime by predicting failures before they occur. Remote control reduces travel time and eliminates the need to staff most substations. Automatic control components protect lines and apparatus in real time, improve system efficiency, quickly restore power after faults, and adapt to changing conditions in the system or plant.

I&C systems already have some features to improve safety. The most prevalent is safety tags, implemented in SCADA and DCS software, that are interlocked with apparatus control software and device outputs. Another safety-related feature is logic to select and enforce local and remote control modes, which helps prevent accidental operations.

This paper describes additional methods for reducing accidents and injuries that I&C systems designers, consultants, project managers, and operations personnel should consider in the specification, design, and justification of new systems and modifications.

II. Reduce Exposure by Reducing Entry to Hazardous Areas

One way to reduce accidents is to reduce the number of times that personnel must enter hazardous areas. I&C system designers can reduce time spent in hazardous areas by:

- Using I&C systems with communications links to remotely monitor and control equipment located in hazardous areas, minimizing entry into unsafe areas.
- Designing and applying very reliable systems so that I&C system maintenance does not cause more exposure to hazardous locations than it prevents.

A. Underground Vaults

Underground vaults for electric power distribution systems are members of the class "confined spaces" defined by the USA Occupational Safety and Health Administration. In the US, "OSHA estimates that about 239,000 general industry establishments employing 12 million people have confined spaces. Approximately 1.6 million people enter confined spaces annually… If employers comply with the [appropriate safety standards], OSHA estimates 53 worker deaths, 5,000 lost-day cases and 5,700 other accidents can be avoided annually." [1]

Electric utilities make extensive use of underground vaults for distribution feeders and equipment. Underground vaults present many dangers, including the following:

- Atmospheric, including insufficient oxygen, flammable or explosive gases, and toxic gases. Heavier-than-air gases can settle in underground vaults from other sources, or may be generated by electrical apparatus [1]. For example, damaged secondary transformer windings have caused explosive gas buildup from melting insulating material [2].
- Electrical, including exposure to conductors or to arc flashes. Accumulation of water in underground vaults contributes to the electrical hazards.
- Suffocation because gases, liquids, or solids fill the confined space
- Extreme heat or cold

Remotely monitoring faulted circuit indicators and other equipment in underground vaults reduces the number of times that personnel must enter vaults searching for faulted cable segments.

B. Arc-Flash Hazards Near Apparatus

Electrical equipment can generate dangerous arcs that are the subject of considerable focus by industry safety professionals and regulators. Remotely monitor, control, and reset equipment in arc-flash zones to directly reduce time spent exposed to arc-flash hazards, and to eliminate opportunities for personnel to misjudge special protective clothing requirements.

C. Traffic

When working on underground apparatus below streets, or on overhead poles from a road, street, or highway, personnel are exposed to the dangers from traffic, and drivers and pedestrians are exposed to hazards from the traffic diversion cones, warning signs, and at night, warning lights. Systems designed to include nearby wireless communications links to reduce vault entries and pole access also reduce hazards involving traffic.

D. Power Poles and Structures

Personnel working on power and communications poles, towers, and structures have increased danger of falling or contacting live electrical conductors. Distributed generation with inadequate or failed connection safeguards can energize lines that maintenance personnel believe to be de-energized. "Falls from power transmission structures are among the most serious hazards faced by electric utility workers" [3].

Where feasible, use wireless communications to pole-mounted equipment to reduce the times that personnel must climb power poles.

E. Electric Substation

Electric substation fences enclose many electric hazards. Using remote communications or nearby wireless communications can reduce the number of times that personnel must actually enter a substation to accomplish their work. You may be able to eliminate physical access for those personnel that can accomplish all of their substation tasks with remote access.

F. Line Patrol

Aircraft searches for electrical faults in wind, precipitation, and lightning from storms are clearly hazardous. Vehicular or foot patrol of the line exposes personnel to weather, traffic, and electrical hazards. Remote-access devices that calculate fault locations and faulted circuit indicators minimize the time spent locating the fault and avoid the dangers of line patrol.

G. Security Perimeters

Opening locked gates or doors to access secure areas provides an opportunity for unauthorized people to enter the secured area by coercing or following authorized personnel. Reduce the opportunities for unauthorized entry by providing remote or nearby wireless communications links to reduce the number of times personnel pass through security perimeters. You may be able to reduce the number of key holders if some personnel require only remote access.

H. Natural Hazards

Wireless communications from the safety of a vehicle can reduce exposure to extreme hot and cold temperatures, blowing snow, ice, and debris, floodwater, snakes, predators, and insects.

III. Improve Situational Awareness to Prevent Accidents and Reduce Injuries

Accident and injury prevention and containment depend on many human factors. Koval and Floyd [4] summarize these in an accident-injury sequence model. They note that it is important to recognize hazard and injury potential. People must be alert and assess potentially hazardous situations by applying training, experience, and logic to understand the hazards and injury potential.

I&C systems provide data that people can use to reduce accidents and the severity of injuries. Information should be easily available to people trained to take action to reduce their risk of accident or injury.

A. Monitor and Report Protective Relay Readiness

Protective relays detect electrical faults and respond by opening circuit breakers to protect people, equipment, and power systems. Modern protective relays include self-diagnostics that detect problems, report warnings, and automatically disable the relays for failures that impair reliable operation. The unavailability of a device is the ratio of the time a relay is out of service to the time it is in service. The Mean Time to Fail (MTTF) is the reciprocal of the failure rate. The Mean Time to Repair (MTTR) is the time to detect and correct a failure, and is the out-of-service time. By strict definition, the Mean Time Between Failures (MTBF) is the sum of the MTTF and the MTTR, but for practical purposes the MTTR is generally so much smaller than the MTTF that it is neglected, and MTBF is treated as equal to MTTR. For example, consider a protective relay with a 200-year MTTF and a 48-hour MTTR. Adding MTTF and MTTR yields an MTBF of 200.0055 years, which is equivalent to 200 years for most purposes. The unavailability is MTTR/ MTBF [5].

To minimize the out-of-service time (MTTR), the failure needs to be detected and reported, and action initiated to restore the device to service. Distributed control systems, SCADA, or other I&C systems connected to protective relays can detect relay failures through transmitted diagnostic information and loss-of-communications. Other systems use digital inputs to sense the state of alarm-output contacts on relays, and report these via annunciator alarm panels or communications links to operators. Reference [5] discusses methods to compare the unavailability of protective relaying alternatives for transmission lines. If the relay status is not reported to a staffed location, a relay failure will not be detected until someone visits the site. If the relay status is not easily available locally, a failed relay will probably not be detected until a periodically scheduled relay maintenance cycle. Until failures are detected and fixed, apparatus are not protected as planned, and the risks are higher.

B. Detect and Report Hazardous Conditions

Sensors and controllers can provide information to warn of conditions that are becoming dangerous, or that already are dangerous. Armed with this information, personnel can prevent hazardous conditions from becoming worse, and can be warned of dangers ahead of time so they can plan the safest actions. For example, a system can sense and report water level, oxygen, temperature, and flammable or toxic gases, and report detected hazards to personnel who will initiate counter measures.

SCADA systems that are designed for electric power applications often include software to implement clearance tags, to prevent closing tagged breakers. As a backup to operating procedures, designers could provide the enhanced capability of determining from breaker position information whether sources are disconnected from tagged lines or apparatus. For example, automatic controls are typically required to quickly disconnect distributed generation from a de-energized feeder. If the breaker or logic fails, the breaker position would remain closed, and the SCADA system could explicitly warn operating personnel that the line is still energized.

1) Human Factors and Safety Alerts

When an I&C system detects a dangerous or potentially dangerous condition, it must convey the relevant information so that it reaches the people in danger. This may be directly through audible and visible warning indicators, and through alarm notifications to operators, that in turn notify other personnel. To effectively transfer the needed information, the following considerations are important:

- The safety-related information should be easily distinguished from other data and alarms, to prevent safety information from being delayed or overlooked.
- If the unsafe condition is detected as a result of action by the operator, such as entering a safety clearance tag, an immediate safety alert by the I&C system is an effective way to convey the information quickly enough to prevent an accident.
- The personnel receiving the information need to be trained to understand the importance of safety information, and know how to efficiently act on the information.
- If field personnel involved in work can remotely access a SCADA or other I&C system to easily check on safety-related items, they can improve their situational awareness and reduce the likelihood of an accident or injury. Training is important so that these personnel recognize the need to get data, understand how to retrieve and analyze the information, and know how to act on the data that they receive. Consider presenting alarm displays or annunciators with instructions at the points of entry to a hazardous area to increase personnel awareness of conditions.

An I&C system could be designed to provide a time-tagged log of unsafe conditions, clearance tag activity, and safety data inquiries, to aid in understanding the root cause of accidents, verify procedures are followed, identify procedural gaps and training opportunities, and to improve operating procedure clarity.

IV. Design I&C Systems Without Introducing Hazards

Design I&C systems so that they do not introduce safety problems.

A. Use Fiber-Optic Communications Instead of Wire for I/O

Use optical fiber communications links instead of wire for input and output.

- Provide improved isolation from ground potential rise and other electrical hazards compared to copper connections
- Specify eye-safe Class 1 LED or laser products to protect eyes
- Prevent dangerous false operations by using electrically noise-immune fiber optics
- Reduce time spent in trenches pulling wire by replacing large bundles of wire with small bundles of optical fiber
- Minimize maintenance exposure through the increased reliability of remote fiber-optic I/O compared to hardwired I/O [6]

B. Use Encrypted Communications Links

Use bump-in-the-wire or built-in encryption per Federal Information Processing Standards (FIPS) to lock out unauthorized intruders that attempt to eavesdrop on data or cause unauthorized, dangerous operations. Encryption enables deployment of wireless communications links as described above, without introducing additional cyberintrusion hazards.

C. Use Very Reliable, Robust Equipment to Reduce Visits

Consider the example of an electric utility that has 100 substations with computers in them to gather data and forward information to a control center and their power-quality engineering group. They have a choice of using common office-grade computers that include a power supply with a MTBF of five years, or hardened, rugged computers that include a power supply with a MTBF in excess of 5,000 years.

- 100 installations, MTBF = 5; predict 20 failures in one year
- 100 installations, MTBF > 5000; predict essentially no (0.02) failures in one year

Using the computers with lower-reliability power supplies would mean:

- 20 more instances of system downtime and loss of data until the power supplies are replaced
- 20 extra round trips to substations per year, with added labor and travel costs, plus greater exposure to traffic and substation hazards
- 20 extra instances of equipment replacement or repair costs caused by the short warranty period of office computers

The cost of the consequences of the downtime can be far greater. For example, if a loss of information and situational

awareness caused by a low-reliability PC contributes to a major system outage, the monetary and societal consequences of the outage could have been easily avoided.

Fault trees and other tools described in [5]–[9] contrast the reliability of the system designs that you consider. Select systems that use very reliable devices to reduce maintenance, in very reliable architectures to reduce system unavailability.

V. Conclusions

I&C system designers can help reduce accidents and injuries to personnel and others via the following:

- Provide wireless monitoring connections to portable computers or other remote devices that allow personnel to monitor and control equipment in underground vaults, on poles, in substations, and other hazardous areas. Use encryption and authentication on these links to prevent undesired and unsafe operation by hackers.
- Where permanent communications links are feasible, provide remote monitoring and control with fiber-optic or encrypted wireless isolation.
- Report automatically calculated fault locations and use them to reduce line-patrol trips.
- Connect sensors that detect potentially hazardous conditions and report them to the instrumentation system. Process the information to clearly present safety-related alarms so they are not lost in the flood of other data.
- Provide alarm indication near the points of entry to hazardous areas to warn personnel of unsafe conditions.
- Monitor the status of protective relays and other equipment, and report this status as safety alarm issues; if protective relays are out of service, the consequences of a fault are more dangerous.
- Use very reliable I&C equipment to reduce the time that I&C repair personnel spend in hazardous areas. Without the I&C system in operation, there is heightened danger because of the unknown state of safety-related conditions.

Improving safety is the right thing to do, as the IEEE Code of Ethics reminds us; members agree "to accept responsibility in making engineering decisions consistent with the safety, health and welfare of the public…" [10]. Safety improvements reduce accidents and injuries, which also reduces associated costs and liabilities. As you design new systems or additions to existing I&C systems, be sure to consider the ways that your design decisions and recommendations can help protect people from accidental death or injury.

VI. References

[1] N.C. Department of Labor Division of Occupational Safety and Health, *A Guide to Safety in Confined Spaces*, 1101 Mail Service Center, Raleigh, NC.

[2] IBEW Local 77 Safety Alerts and News: http://www.ibew77.com/safetyalerts.htm

[3] EH-9402, *Occupational Safety Observer*, issue no. 2, Feb. 1994

[4] D. O. Koval, H. L. Floyd, II, "Human Element Factors Affecting Reliability and Safety," *IEEE Transactions on Industry Applications*, vol. 34, no. 2, March/April 1998, pp.406–414.

[5] P. M. Anderson, E. O. Schweitzer III, B. Fleming, and T. J. Lee, "Reliability Analysis of Transmission Protection Using Fault Tree Methods," in *Proceedings of the 24th Annual Western Protective Relay Conference*, Spokane, WA, October 21–23, 1997.

[6] G. W. Scheer and R. E. Moxley, "Digital Communications Improve Contact I/O Reliability," in *Proceedings of the Western Power Delivery Automation Conference*, Spokane, WA, May 10–12, 2005.

[7] G. W. Scheer, "Answering Substation Automation Questions Through Fault Tree Analysis," in *Proceedings of the 4th Annual Texas A&M Substation Automation Conference*, College Station, TX, April 8–9, 1998.

[8] G. W. Scheer and D. J. Dolezilek, "Comparing the Reliability of Ethernet Network Topologies in Substation Control and Monitoring Networks," in *Proceedings of the 2nd Annual Western Power Delivery Automation Conference*, Spokane, WA, April 4–6, 2000.

[9] G. W. Scheer and D. Woodward, "Speed and Reliability of Ethernet Networks for Teleprotection and Control," in *Proceedings of the 3rd Annual Western Power Delivery Automation Conference*, Spokane, WA, April 2001.

[10] Institute of Electrical and Electronic Engineers (IEEE), *IEEE Code of Ethics*, Approved by the IEEE Board of Directors, August 1990.

VII. Biographies

Gary W. Scheer received his B.S. in Electrical Engineering from Montana State University in 1977. He worked for the Montana Power Company and the MPC subsidiary, The Tetragenics Company, before joining Schweitzer Engineering Laboratories, Inc. in 1990 as a development engineer. He has served as Vice President of the Research and Development Division, and of the Automation and Engineering Services Division of SEL. Mr. Scheer is now in the Marketing, Research and Development Division as Senior Marketing Engineer for automation and communications products. His biography appears in Who's Who in America. He holds two patents related to teleprotection. He is a registered professional engineer and member of the IEEE and the ISA.

Mark Zeller received his BS from the University of Idaho in 1985. He has broad experience in industrial power system maintenance, operations and protection. Upon graduating, he worked more than 15 years in the pulp and paper industry, where he worked in engineering and maintenance with responsibility for power system protection and engineering. Prior to joining Schweitzer Engineering Laboratories in 2003, he was employed by Fluor to provide engineering and consulting services for Alcoa Aluminum. He has been a member of IEEE since 1985.

20060303
TP6236-01