WHITE PAPER

Enhance Control System Security Using Process Switches

UNITED ELECTRIC CONTROLS

www.ueonline.com

Enhance Control System Security Using Process Switches

In today's world of standardized communications, no man is an island and neither is any process control system. Networking is about to expand greatly, thanks to the increasing adoption of integrated devices, the internet, and a proliferation of open operating systems. Increasing attacks that exploit weaknesses in the network may not be far behind. Real world examples have shown that control systems can be hacked, sometimes with deadly results.

This white paper looks at how open Microsoft technology used in virtually all contemporary control systems, such as distributed control systems (DCS) and supervisory control and data acquisition (SCADA), can mean less security. The paper explores why current solutions may not be up to the task of protection. It also shows how simple, yet reliable electro-mechanical switch-based protection can improve cyber defenses by complementing traditional techniques with another layer of protection independent of centralized control systems.

Better Technology, Less Security

A long running trend is behind the increasing vulnerability of control systems to hacking and other forms of cyber mischief. Centralized control systems are typically tied together through an open network and software that is susceptible to cyber-attack. What's more, the network extends out beyond the plant floor. Indeed, a part of the plant floor network is increasingly reaching around the world, thanks to web-based tools and interfaces.

Networking adds extra capabilities, information sharing, and lowers the cost of commercial off-the-shelf components used in process control systems. Data from a control system can be fed into enterprise management software, enabling the use of business intelligence techniques to tackle problems and improve overall performance.

However, current networked systems are more vulnerable to attack than yesterday's stand-alone and analog-based setups. This increased susceptibility arises from expanding exposure on two fronts. First, an open standardized network that can be accessed around the world for good can also be manipulated globally for bad. Second, the more complex a network becomes, in terms of connected devices and topology, the more likely it is that some vulnerability will open up, particularly if system updates are not deployed in a timely manner.

Perhaps the best known and most complete example of this in a SCADA setting is the Stuxnet worm, which was discovered in June 2010. Stuxnet infects computers through infected USB flash drives and exploits multiple Microsoft Windows security vulnerabilities. More recently, another worm related to Stuxnet dubbed Duqu was discovered by a Budapest University. Built on the same source code as Stuxnet, Duqu may be one of many malware worms floating in cyberspace ready to attack.

An investigation by the Idaho National Laboratory demonstrated potential physical damage with a 27-ton power generator by sending conflicting instructions governing speed and other characteristics that induced the generator to literally shake apart, destroying it. In a simulation, Sandia National Laboratory engineers showed that turning off a recirculation pump while upping heat could incapacitate an entire oil refinery by simply destroying a critical component.

Current Solutions Need Improvement

Traditional solutions are not as effective as they once were. One aspect of the traditional approach is to patch software to plug vulnerabilities. Doing this prevents an attacker from gaining control of a system through the use of a trick - such as a buffer overflow overloading the software – thereby allowing an attacker free reign.

Yet another approach is to employ firewalls and intrusion detection devices to keep intruders out and prevent the exploitation of weaknesses. Very sensitive and critical control applications are further hardened through network segregation to limit points of contact to the outside world, making the systems more secure. Costly redundant components and controllers can also be used, if control applications are vital enough to warrant the extra expense.

In today's world, unfortunately, all of these tactics can – and do – fail due to the efforts of smart savvy attackers. On the software side, the list of vulnerabilities in Linux, Windows, iOS, Android and other operating systems is long and growing. Despite the valiant efforts of the control system suppliers, attacks can succeed if an un-patched operating system or applications exist inside a trusted area due to lax system upgrades.

In addition, the growth of newer technologies, such as fieldbus networks, industrial wireless networks, and mobile hand-held devices is another potential path for hackers. The new crop of safety instrumented systems (SIS) shift from separated analog systems to digital networking architectures may be susceptible to operating system weaknesses. Wireless networks are new and even with the extraordinary security measures included in the standards, only one entry point out of an infinite amount due to ubiquitous access points through sensors and mobile devices is needed to create havoc.

In total, this situation means that the most secure approach possible – network segregation – is much less effective.

Turning to Tried and True Technology

Clearly, there is a need to add to the defense against cyber-attack. Ideally, the defense would operate in the event of a compromised control system. The solution has to be fast acting, as even small delays can lead to damaged equipment, toxic environmental exposure, loss of life, and long downtimes. It also has to be reliable, working when needed and not triggering at the wrong times. Finally, it has to be hack-proof and support current infrastructure.

Electro-mechanical process switches, a robust and proven technology, meet all of these requirements. At first glance, this is somewhat surprising since the technology is not typically considered for cyber security. However, electro-mechanical switches do not have software or an operating system susceptible to cyber attack. When properly applied, electro-mechanical switches can provide safety functions independent of a central control system. There is no processor involved, which means there is nothing to hack. Electro-mechanical switches are also fast, tripping quickly when milliseconds count. What's more, modern implementations, like United Electric's 100, 120 and 400 Series of pressure and temperature switches, have virtually no false positives. When these switches trip, it is because a safe operating limit has been exceeded, dangerous conditions exist, or both.

The key to this approach is the placement of switches so that they monitor suitable process parameters. They also must be connected so that they can take the appropriate action. In the event of an out-of-limit process condition, the switches will trip. Since the switches can power relays, they can be wired so as to shut down compressors, pumps, turbines or whatever is needed to correct the situation and limit the damage.

Of course, the choice of what parameters to measure and where to do so will be dictated by the particular process in question. Likewise, what to have a switch act upon will also be process specific. They could, for example, shut off a compressor to keep a vessel from an overpressure situation or they could trip relays to take an entire plant floor offline.

To see the power of this approach, consider that one of the first actions taken in Sandia National Laboratory oil refinery attack simulation was to put the system on manual, thereby overriding automated safeguards. This hack attempt would have failed, though, given an appropriately placed and configured electro-mechanical switch. The switch would have tripped once the temperature exceeded a set point. There would be nothing the attacker could have done.

As an added bonus, switches protect against both deliberate and accidental catastrophes. After all, they do not care why a temperature limit, for example, has been exceeded. The situation could be due to malicious hacking or the failure of a pump circulating coolant. In either case, though, the switch would take the same action and provide an emergency shutdown.

Conclusion

As has been shown, increasing connectivity and automation have brought benefits, such as diagnostics, predictive maintenance, and process optimization to process control. However, by bridging the gap between control systems and the world, these advances have also made automated control systems vulnerable to attack. Traditional solutions may not be adequate to safeguard systems in an environment where multiple, rapidly evolving technologies combine to create many potential weak links.

The solution involves a properly designed safety layer of electro-mechanical process switches to complement traditional software solutions. Switches are fast, reliable, hack-proof, and act independent of the control system. Electro-mechanical switches should be considered as the primary or redundant layer to protect critical equipment in today's dangerous landscape. So, while no control system today may be an island, electro-mechanical switches can, in effect, provide protection from intruders before they can cause damage.

100 Series
Pressure & Temperature Switches

120 Series
Pressure & Temperature Switches

400 Series
Pressure & Temperature Switches