Without security, safety in the IIoT is of little value

JONATHAN BERG
Supervisor, Software Engineering
Moore Industries

For more information:
www.miinet.com
(818)-894-7111

As technology progresses and economies of scale continue to work their magic, more powerful microcontrollers are finding their way into smaller, smarter instruments. This additional processing power allows real-time operating systems (RTOS) and network stack software to run. And gloriously, these purpose-specific devices are brought onto the Internet. And while the engineers are basking in the glow from their new IIOT device they fail to notice that they just painted a big red X on their instrument; it has become a potential target.

Imagine that the device has a sensor providing information to a control system. What happens if an electronic intruder is able to make that sensor lie, or for it to be misinterpreted, such that the controller uses incorrect values? This could have an extreme range of implications ranging from inconsequential to loss of life. If you can drive a truck through the instrument's security holes, will anyone care about its safety rating?

One way for manufacturers to address security needs is to look to IEC/ISA 62443 and its seven foundational requirements (FR). Based on how well the devices implement these requirements, one of 5 security levels (SL) will be awarded for each FR. Depending on the results of a plant/facility cybersecurity audit, different network zones and segments will be determined to require different levels of protection. The different security levels are:

- Security Level 0 - No specific requirements or security protection necessary.
- Security Level 1 - Protection against casual or coincidental violation.
- Security Level 2 - Protection against intentional violation using simple means with low resources, generic skills and low motivation.
- Security Level 3 - Protection against intentional violation using sophisticated means with moderate resources, industrial automation and control system (IACS) specific skills and moderate motivation.
- Security Level 4 - Protection against intentional violation using sophisticated means with extended resources, IACS-specific skills and high motivation.

As one would expect, security levels start from providing no real protection, and move up through protection against attackers with more sophistication, resources, skills and motivation. Depending on the nature of your IIoT device, your security needs may not be very extreme. However, if your device is the last line of defense in a safety system, then your needs *are* extreme.

The reality of the situation is that instrument manufacturers' safety related devices are designed from the beginning to meet a particular SIL rating. Their hardware and software development and management processes as well as the resulting paper trails *must* be up to the task and hold up to audits. Companies that are capable of this level of excellence when it comes to making SIL-rated devices are also likely to meet the levels of rigor needed to achieve their targeted security level.

Sure, adding a network interface to an embedded device is getting easier and easier, but following good safety and responsible cybersecurity practices is becoming more critical. With every news story about a data breach, hacking, or other cybersecurity attack, the stakes get higher. The good news is that like other engineering areas risks can be reduced. Implementing policies and training employees on how to use security features present in modern instrumentation will help. Ensuring their compliance can go a long way to plugging holes.

I like to believe that people are basically good and want to do their jobs properly, keeping things safe and secure. Therefore, microprocessor-based instrumentation, sensors, control systems and final control elements should be designed from the ground up to enable them in this mission. In today's world, a device performing a critical function cannot reach its safest levels unless it is also secure.