Innovating Securely with Standards-based Cybersecurity Product Certification

Khalid Ansari, Principal ICS Cybersecurity Engineer, FM Approvals

Digital innovation inevitably entails increased connectivity of products and systems. Seamless flow of information and democratization of data are the hallmarks of digital transformation. Data is demanded by a wider audience, from remote locations and on myriad of devices. This is made possible not just by converging Information Technology (IT) and Operational Technology (OT) but going a step further and connecting the plant directly to the cloud, i.e., by building an Industrial Internet of Things (IIoT).

However, increased connectivity and need for constant availability of information brought about by digital innovation exposes industrial control systems (ICS) and components to an ever-increasing cyber-attack surface. PLCs and DCSs were originally designed to operate on the production floor and in process plants in isolation, with reliability and safety as their key goals. Cybersecurity was not a major concern. This must change now for innovation to be successful. We cannot innovate at the expense of security. We may be putting production, environment, and even human life at risk by doing so.

To address this lack of cybersecurity of ICS systems and IIoT devices, industry has come together and created security standards, foremost of which is the ISA/IEC-62443 series of standards. These set of standards and technical reports address overall security of ICS systems including policies & procedures, security programs, risk assessment, zones-and-conduits based architecture, and security levels among other topics. Security controls expected of systems and components and their manufacturers are addressed in parts 3-3, 4-2 and 4-1 of the standards, respectively.

FM Approvals is accredited by ISASecure® and the Standards Council of Canada (SCC) to independently assess and certify ICS products for their conformance to the ISA/IEC-62443 series of standards. In addition to the rigorous testing of the ICS system as per part 3-3, and component or device per part 4-2, ISASecure® is launching a certification scheme for IIoT devices and gateways based on part 4-2. Most importantly, part 4-1 requires product manufacturers to adopt and practice security development lifecycle best practices. This ensures the product is designed with security as a key goal right from its inception and is supported throughout its lifecycle.

ICS and IIoT products that successfully complete FM Approvals’ cybersecurity evaluation program will bear the FM Diamond along with the specific security level/tier. These ICS and IIoT products will be listed in a special ICS cybersecurity section of the Approval Guide.

Come to Hall 11.1 Booth G73, to learn how both product manufacturers and end-users may benefit from cybersecurity certification of ICS and IIoT systems and products.

1 Contact: khalid.ansari@fmapprovals.com