Indiana University School of Infromatics and Computing

HATS Researach Group

SDN: Industrial Controls Case Study Writeup

Cyber-Physical Use Case 2: Industrial Control Systems

Industrial control systems are also of critical concern because of a modern state's near-total dependency on civilian utility networks.

Operators and Stakeholders

The most important utility from the critical-infrastructure viewpoint is electric power, without which almost everything else comes to a standstill; but there are other critical systems such as oil refining, railway signalling and water treatment. It was realised fifteen years ago that such networks were becoming exposed to cyber-attack because of the rapid adoption of IP networking. The protocols most commonly used in industrial control systems evolved in a world of closed and dedicated networks with no need for authentication or encryption. The move to IP was driven by cost pressures but left operators vulnerable; anyone in the world who knew the IP address of a sensor could read it, and anyone who knew the address of an actuator could operate it. Since the alarm was sounded in 1998, and especially since 9/11, considerable efforts have been expended by both state and private-sector actors in protecting critical control systems. In what follows we will discuss the electricity industry; similar comments apply, mutatis mutandis, to petrochemicals, signalling, water-treatment and indeed industrial production.

Technical Operations

A small installation such as an electricity substation might have 100-200 programmable devices attached to a substation LAN, including transformers, circuit breakers, reclosers and meters. Traffic on the LAN is not encrypted or authenticated, as there are stringent latency requirements, so anyone with access to the wiring could disrupt operations. Anyone with physical access could do this anyway by operating manual override switches, so the issue is whether an attacker might get remote access to a device on the LAN. Security at present depends on a station controller, which is on the LAN, and a gateway which is attached to the controller and also to WAN communications (typically over the Internet to a network operations center, protected by TLS). It is critical that these devices not be vulnerable to remote software attack, and that they provide effective protection to internal devices.

Vulnerabilities

Power stations, network control centres and large-scale substations are likely targets in the event of cyber-attack by a hostile state, or by a capable substate group such as militant environmentalists. A power station has been affected accidentally by malware when a flash worm spammed the monitoring network, which would have caused a safety shutdown had it been operational at the time. A more deliberate attack might follow the Stuxnet model, with targeted malware introduced via USB drives left lying in the car park. An important line of defence is to prevent software making its way from open systems to the SIL1 and higher domains. The strict network separation that SDN networks can support is attractive here.

A typical system has network vulnerabilities that arise spontaneously. A search engine built to discover control systems found over a thousand of them accessible on the Internet. Traditional network management technologies make it hard to manage separation dependably; the combination of complexity and obscurity makes it hard for people to understand what's connected to what, and as people modify

things to get their work done, paths open up to the wider Internet. The principal benefit of SDN lies in providing much better tools to enforce perimeters, providing high assurance that critical sensors and actuators never become accessible from outside.

Requirements for a Resilience Architecture

As before, a resilient network will ensure connectivity and quality of service for critical services in decreasing priority order, starting with SIL3, then SIL2, then SIL1, then corporate communications. It will also use virtualisationto protect each layer against lower layers.

Organization Requirements

A power station is, like an airport, a major capital asset with a lifespan measured in decades. Even if an individual nuclear reactor is decommissioned after 40 years, it's common for new reactors to be built next to old ones, as the local communities accept them and value the jobs. Power station operators are regulated; the regulation is even fiercer for transmission and distribution operators who maintain the power grid. A big issue in the USA (and also in much of Europe) is that security expenditures are not part of the regulated cost base, and thus they come directly off the company's bottom line. As the operators are typically funded by debt as well as equity this creates major resistance to any security investment that cannot save money directly.