Fending off Attacks On the Robots: TCG Specification for Network Segmentation

While much is made of an *'attack of the robots'* displacing tens of millions of workers from once job-rich industries, but those charged with safeguarding the workings of modern society are preoccupied with another assault – attacks ***on*** the robots and other automated cyber-physical systems.

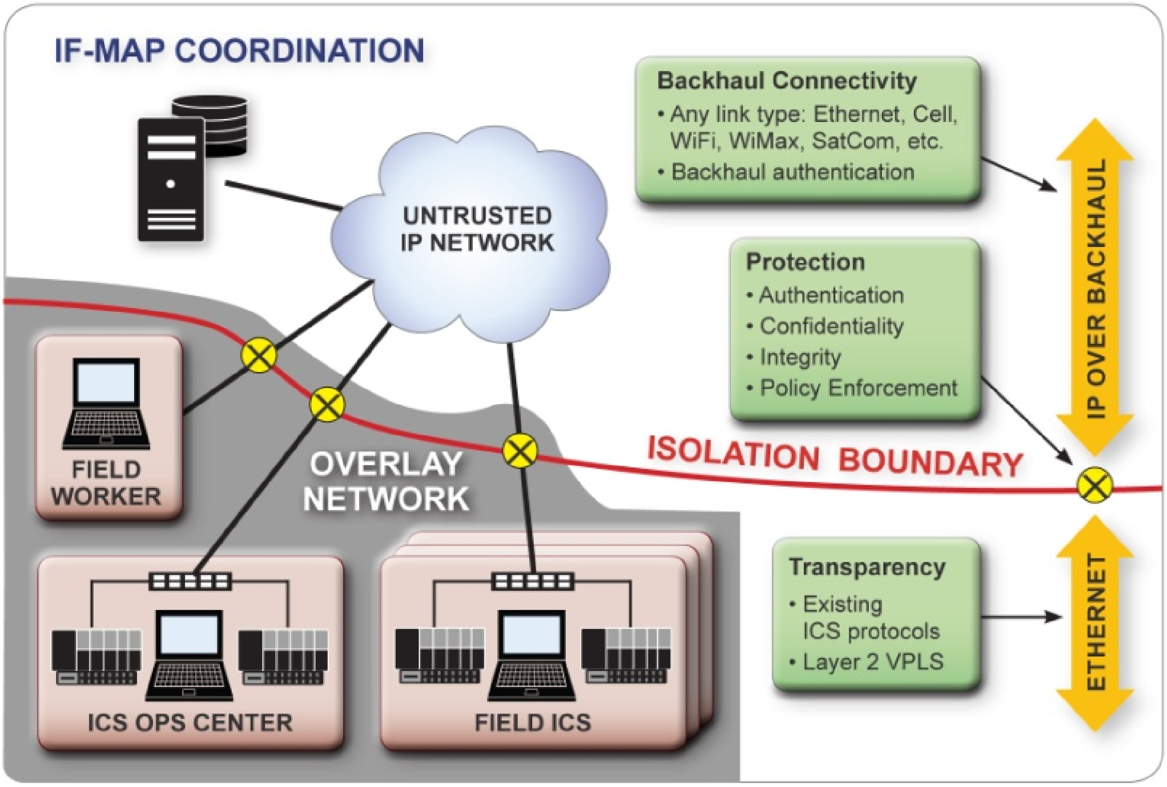
It doesn't take an engineer to appreciate persistent warnings of a coming "Cyber Pearl Harbor" targeting the automated devices that run critical infrastructure. The much-publicized Stuxnet attack in Iran proved a well-placed virus can wreak havoc on industrial sites. Closer to home, hackers employ many methods (including the unnerving Shodan search engine) to worm their way into sensitive industrial control systems – often targeting automation that is running vital infrastructure including power grids, public water systems, oil and gas infrastructure (pipelines, refineries, depots, etc.) and transportation systems. Federal and state agencies such as DHS ICS-CERT, assisted by industry associations, are responding with real-time alerts detailing the latest attacks targeting control systems; they note that attackers often find it easiest to compromise automated cyber-physical systems at the network edge, rather than attacking the more powerful servers and laptops that run best-of-breed security controls.

A tidal wave of increasing connectivity is being driven deeper and deeper into automation in order to improve operating efficiency and reliability. For this reason, industrial automation networks are in dire need of improved security still allowing them to retain their flexibility and compatibility with existing automation protocols which often have little-to-no communications security features. Fortunately, we now have a standardized means for frustrating the attacks on these systems by securely segmenting communications on top of standard IP protocols. This approach was developed by me and my colleagues at Boeing and is now being commercialized far beyond the aerospace industry.

The approach is based on the ISA TR100.15.01 architecture and ISA99 security models for segmenting, securing, and managing vulnerable communication channels over both trusted intranets and untrusted networks. Our network whitelisting approach – combining the IF-MAP and ICS security coordination and automation standards from the Trusted Computing Group (TCG) with standards for identity-based secure communications using the Host Identity Protocol (HIP) from the Internet Engineering Task Force (IETF) – has created a scalable and more easily manageable cyber security approach inspired by work in-sourced at The Boeing Company.
Conceding commercial off-the-shelf products are a poor fit for the manufacturing floor, Boeing set me and colleagues to work engineering a capability for efficient network segmentation when it transitioned from fixed monolithic tooling to lean mobile manufacturing on its 777 manufacturing line. (*Network World*, April 22, 2013, http://www.networkworld.com/news/2013/042213-boeing-

268986.html). New mobile robots needed to communicate with a supervisory station and each other, and to be remotely accessible to tooling engineers and vendors. (*IETF 81*, July 28, 2011, http://www.ietf.org/proceedings/81/slides/HIPRG-2.pdf).

Though based on the isolation and security models of VLAN and VPN, the resulting work significantly departs from these traditional approaches by building network 'sandboxes' on top of arbitrary IP networks—with each 'sandbox' defined by an explicit collection of secure cryptographic identities. A standalone security appliance acts as the network policy enforcement point and the connectivity proxy to standard and managed interfaces used to access any underlying shared network. In fact the shared network can be any routable network, including enterprise WANs, cellular networks, process VLANs, customer networks, Internet ISPs, etc. Inside each sandbox, the automation devices are isolated in their own private network, with its own private network addressing and broadcast domain, effectively making the connectivity invisible to prying eyes hacking into the underlying corporate network. Industrial device connectivity is explicitly defined and documented, minimizing the connectivity between components. This private overlay network is set up in minutes, versus the days and weeks necessary to deploy a VLAN across a complex infrastructure.



This outcome is a generational leap: Security ultimately derived from existing VPN and Stateful Packet Inspection (SPI) firewall technologies now can be packaged with a network whitelisting approach creating flexible architecture and a sophisticated yet simple management platform that, indeed, does get work done more efficiently, without risking the security of operations. IF-MAP promises the opportunity to continue adding defense-in-depth capabilities at the isolation boundary and close to edge automation devices.

The first to commercialize the standards-based architecture engineered for the 777 manufacturing line is Asguard Networks, a Seattle company I founded two years ago after leaving my job at The Boeing

Company to popularize the solution we named SimpleConnect™. Already, Asguard Networks counts several influential corporations among its first customers, including companies in the oil, gas and industrial chemical industries. Additionally, a number of public utilities are deploying SimpleConnect in defense of the power grid and public water systems.

"We've been looking for this solution for years, because whenever we're working in an industrial environment, we've long needed a secure data connection from the devices to a SCADA and historian," said Robert Landick, principal at CB Engineering Pacific. "Boeing's support for the development of SimpleConnect was inspired: our partners absolutely light up when they understand what Asguard Networks is accomplishing."

Indeed, SimpleConnect points the way to combining TCG's IF-MAP specification with the IETF's HIP protocol to create a remarkably simple-to-connect, easy-to-use industrial connectivity solution that's more secure by default. Formal publication of the TCG's IF-MAP Metadata for ICS Security specification heralds a dramatic game-changer in the real battle – the fight to thwart attacks *on* the robots.

Editor's Note: Asguard Networks Founder and CTO David Mattes is an invited expert to the Trusted Computing Group and co-editor of the TCG TNC IF-MAP Metadata for ICS Security specification.