JEFF HUSSEY, TEMPERED NETWORKS

A BETTER WAY TO MEET CYBER STANDARDS

A new option for secure networking is helping companies crack the code

Does it make sense to use technology that was developed in the 1970s to support the standards in place today?

That would be like driving a 1966 Chevy Camaro, which produced an estimated 5.4 mpg, to match modern fuel standards. Things just don't accurately scale that far in the future. Yet, that's how most manufacturing plants today attempt to secure, connect, and protect their networks by using TCP/IP.

Don't get me wrong, TCP/IP remains a valid way to set up your underlying infrastructure. There's no need to rip and replace it. But know that TCP/IP is a promiscuous protocol: It was engineered to respond to any request without having a way to natively verify the source's authenticity. It was never designed to protect manufacturing systems and networks against the worldwide relentless pursuit of hackers. This is why we read about breaches daily.

In plain English, what does this mean for the modern manufacturing environment?

Manufacturing in 2019 looks a lot different than it did in 1983. The industrial internet of things (IIoT) has arrived and promises to make aging and fractured manufacturing processes obsolete. The benefits of fully embracing the IIoT are plentiful, but realizing them requires having reliable and secure connectivity to work seamlessly.

With such connectivity spread out all over the world to various networking environments – including those you don't control – there are more access points than ever before. While this offers tremendous flexibility, having more access points opens up greater possibilities for intrusion and breaches. A smarter way to network these conventional and unconventional endpoints is needed, because traditional network and security solutions are not designed for this environment and are vulnerable to the pitfalls of TCP/IP.

NIST: ON A MISSION TO PROTECT

After its inception in the late 1970s, TCP/IP was adopted by ARPANET – the precursor to the web – in 1983. IP-based networking is still the standard that virtually every organization relies upon for its networking needs. With the understanding that technology has progressed by leaps and bounds since then, why do we still rely on an antiquated IP-based technology to connect the most valuable machines, systems, and data of our manufacturing facilities?

Until recently, the simple answer was that no better option existed. Meanwhile, the National Institute of Standards and Technology (NIST) devised the Cybersecurity Framework (CSF) to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security. NIST has made recommendations that affect any manufacturer that works with controlled unclassified information from certain government agencies anywhere along the supply chain. Earlier this year, the U.S. Department of Defense (DoD) disclosed that it plans to release tougher standards in 2019 to strengthen the cyberdefenses of subcontractors farther down the supply chain.

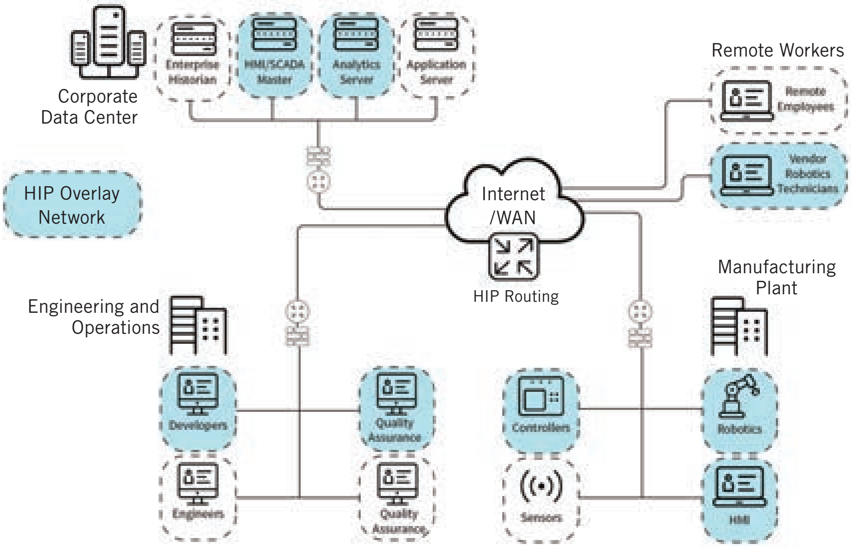
THE BENEFITS OF EMBRACING THE IIoT ARE PLENTIFUL, BUT REALIZING THEM REQUIRES HAVING RELIABLE, SECURE CONNECTIVITY TO WORK SEAMLESSLY.

The CSF offers a dynamic set of cybersecurity practices and outcomes as well as technical, operational, and managerial security controls designed to help organizations manage cybersecurity risk. These controls support the five risk management functions of the CSF: Identify, Protect, Detect, Respond, and Recover.

What most networking practitioners may not realize is that an innovation for modern manufacturing and industrial networks was made available in 2015. The Host Identity Protocol (HIP), an open standard ratified by the Internet Engineering Task Force (IETF), squarely addresses TCP/IP's inherent vulnerability.

HIP-BASED TECHNOLOGY: BORN IN MANUFACTURING

HIP technology was pioneered by a successful Fortune 50 global manufacturing company in collaboration with respected organizations such as the DoD, Siemens, Honeywell, Cisco, Ericsson, and Shell and is based on International Society of Automation (ISA) standards. With intense pressure to step up production and meet customer demands, the manufacturer had to transform its aging systems from fixed monolithic tooling to lean mobile robotics. The new mobile manufacturing systems required secure connectivity and segmentation over wireless communications. Security was paramount because the company's intellectual property is a high-value target for hackers. The manufacturer solved its connectiv-



HIP-enabled secure overlays ensure that secure communications can occur only between trusted endpoints and no others unless they are explicitly added to the overlay. HIP overlays are highly scalable and simple for OT staff to manage.

ity challenges by developing a secure networking solution that leveraged the Host Identity Protocol (HIP).

Let's take a look at how HIP helps organizations align with the CSF standard. HIP-based technology addresses the need for more-secure connections by creating invisible overlays to the existing network that communicate independent of location. It authorizes only trusted endpoints before TCP session establishment, acting as a zero-trust verification policy for anything connected to the network. HIP provides an unprecedented level of security and also helps organizations meet the specifications outlined by the NIST cybersecurity framework.

For example, consider factory robots that need to communicate with different end points throughout the facility, such as:

- The process controllers
- Engineering offices with developers needing a constant influx of new data
- Vendor technicians delivering firmware updates from their staging server
- Quality-assurance personnel collecting data for reports
- InfoSec team members needing access to logs

In this situation, a HIP-enabled network dedicates one overlay for all robotics. Any designated "trusted" device or endpoint that needs to communicate with the robots must be whitelisted by the overlay using a central management console. The HIP overlay overcomes complex IP addressing schemes and VLANs, internal firewalls, NATs, and VPNs across the LAN and WAN. The other good news is that it's simple to deploy and maintain, requiring no advanced IT skills.

MEETING NIST CSF STANDARDS

To significantly reduce cybersecurity risk and increase operational efficiency, today's manufacturing organizations must set their sights on building an integrated, automated, simple, and secure network architecture to align with the business outcomes in the NIST CSF.

The challenge for most manufacturers is that traditional networking solutions involve exorbitant costs, require advanced IT skills, and are complex to manage. With HIP-enabled technology, it's simple to align with the CSF Core and achieve secure connectivity and segmentation at scale for any networked machine or system.

Further enhancing the argument for HIP technology is that no costly or cumbersome teardown of existing architecture is required. HIP works over your existing infrastructure, supports legacy endpoints, and is forward and backward compatible with IPv4 or IPv6 networks. Why continue managing outdated, costly, and insecure networks when a better solution is already available?

Let's get real now. If you have a 1966 Chevy Camaro, ignore the stigma associated with a gas-guzzling American muscle car, because sometimes you have to break the rules and have some fun. Data breaches, service interruption, and brand tarnishing, however, clearly are no fun. Enjoy the ride, but going forward, research HIP for your modern manufacturing connectivity and NIST compliance to ensure a smooth journey, unprecedented operational efficiency, and radical security.

Jeff Hussey is the president and CEO of Tempered Networks (www.temperednetworks.com). He is an accomplished entrepreneur and business leader with a proven track record in the networking and security markets. Hussey also founded F5 Networks, a global leader in application delivery and an S&P 500 listed company. He maintains numerous board positions across a variety of technology, not-for-profit and philanthropic organizations. He is the chairman of the board for Carena and chairman and co-owner of Ecofiltro and Pura Vida Create Good.