CASE STUDY

Schneider Electric HMI/IPC

intel

# Enhance OT Security with Schneider Electric* HMI/IPC and Intel® Hardware-Enabled Security Solutions

## How Does Operational Technology (OT) Endpoint Protection Help to Reduce Risk to Critical Infrastructure for Businesses

Table of Contents:



> Security is critical to keep our customers' facilities running and increased security means they can operate more efficiently, while protecting their people, processes and operations. The objective of our solutions is to be both breach-resistant and breach-ready to support customers in their own cybersecurity framework. Schneider Electric is proud to work with Intel on their journey to bring to market processors which feature multiple hardware-based security measures that help protect data from the silicon up.
>
> Andrew Kling,
> Chief Technology Officer

Schneider Electric

## How Does OT Endpoint Protection Help to Reduce Risk to Critical Infrastructure for Businesses

As businesses and industries shift towards digital transformation due to its advantages, operational technology (OT) endpoint protection will now need to assess all of the potential cybersecurity risks associated with those decisions. Integration of digital technology into all aspects of a business has fundamentally changed the way operations are run. With digital transformation, businesses these days can use different kinds of devices to access a business network, such as workstations or mobile devices, which has helped boost work efficiency, allowing them to create new business processes, make changes in real-time to meet the ever-changing business and market requirements as well as customer's demand remotely.

Though the adoption of digital technology has opened up endless possibilities with interconnection, enabling companies to transfer data between these assets, it also makes it more susceptible to cyber threats as this interconnection, if unprotected, can be exploited by hackers. The real-world consequences of a successful cyberattack severely affect not only the information technology (IT) system but also the entire operational processes in production.

The worlds of IT and OT are converging, and with cyber-attacks posing as the unprecedented threat in today's increasingly complex business operation infrastructure the need for OT endpoint protection has grown exponentially. Without proper protection, companies are at risk of cybersecurity threats such as ransomware, theft of intellectual property, and more. Securing hardware is fundamental root of trust. Intel hardware-enabled security helps boosts protection and helps enable the ecosystem to defend against evolving and modern cybersecurity threats. Schneider Electric's Harmony P6 industrial PC powered by Intel's 8th generation processor is built with security in mind. Security is a system property rooted in hardware, with every component from software to silicon playing a role in helping secure data and maintain device integrity. Intel has a suite of technologies to build and execute on a defense in-depth strategy, helping Schneider Electric solutions to be more breach-resistant and breach-ready to support its customers in their own cybersecurity framework in the OT space.

As cybersecurity attacks and data breaches cannot be realistically evaded entirely, the objective of Schneider Electric solutions is to be both more breach-resistant and breach-ready to support its customers in their own cybersecurity framework in the OT space.

## Empowering Innovation with Enhanced Security

Security is a system property rooted in hardware, with every component from hardware to software playing a role in helping secure data and maintain device integrity. Intel has a suite of hardware-enabled security technologies to build and execute on a defense in-depth strategy, with solutions spanning threat detection, data/content protection, memory protection and more.

Intel hardware-enabled security technology meet specific challenges centered around three key priorities:

- Foundational Security
  Critical protection to help verify trustworthiness of devices and data.

- Workload and Data Protection
  Trusted execution for hardware-isolated data protection.

- Software Reliability
  Platforms that help protect against a range of cybersecurity threats.

Together, these innovations help drive our vision for a world where all data is secured in a safe execution environment.

8th Generation Intel® Core™ hardware security features:

1. **Intel® Boot Guard**
   Intel® Boot Guard provides a key element of hardware-based integrity that meets Microsoft Windows* requirements for UEFI Secure Boot Secure Boot aimed at mitigating unauthorized BIOS boot block modifications. It is designed to verify the correctness of this code before the CPU runs the Initial Boot Block (IBB). When booting with Intel® Boot Guard enabled, the boot integrity is unalterable since it is anchored in hardware fuses. Intel® Boot Guard becomes a hardware root of trust adding robustness to the chain of trust process where UEFI boot process cryptographically verifies and/or measures each software module before executing it. The result of the Intel® Boot Guard process is a reduction in a chance of malware exploiting the hardware or software components on the platform.[4]

2. **Intel® Platform Trust Technology**
   A trusted element of the platform execution that provides enhanced security by verifying the boot portion of the boot sequence which helps protect against viruses and malicious software attacks.

3. **Intel® BIOS Guard**
   An augmentation of existing chipset-based BIOS flash protection capabilities targeted to address the increasing malware threat to BIOS flash storage. It helps protect the BIOS flash from modification without platform manufacturer authorization, helps defend the platform against low-level DOS (denial of service) attacks, and restores BIOS to a known good state after an attack.

4. **Intel® Trusted Execution Technology**
   Intel® Trusted Execution Technology (Intel® TXT) is the technology that the OS or hypervisor could use to initiate a measured and controlled launch of system software called the Measured Launch Environment (MLE). OS or hypervisor uses Intel® TXT to establish the MLE generally at OS boot time. This MLE is a protected environment for itself and anything that may run within this environment. Intel® TXT measures key components executed during the launch of MLE and allows the OS to check the consistency in behaviors and launch time configurations against a "known good" sequence. Using this verified benchmark, the system can quickly assess whether any attempts have been made to alter or tamper with the launch time environment.[4]

5. **Intel® AES-NI**
   Intel® AES New Instructions (Intel® AES-NI) is a new encryption instruction set that improves on the Advanced Encryption Standard (AES) algorithm and accelerates the encryption of data in the Intel® Xeon® processor family and the Intel® Core™ processor family. Composed of seven new instructions, Intel® AES-NI gives your IT environment amazingly fast, more affordable data protection, and great security, helping make pervasive encryption feasible in areas where previously it was not.[5]

6. **Intel® Secure Key**
   Security hardware-based random number generator that can be used for generating high-quality keys for cryptographic (encryption and decryption) protocols. Provides quality entropy that is highly sought after in the cryptography world for added security.

7. **Intel® Active Management Technology**
   Complete manageability features included as part of Intel® vPro® Enterprise for Windows, helps reduce overall PC maintenance and administrative costs. With features to remotely discover, repair, and help protect networked computing assets, Intel® Active Management Technology allows IT to support a highly dispersed workforce.

At Intel, the security of our products is one of our most important priorities. Our goal is to build the most secure hardware in the market, from world-class CPUs to XPUs and related technology, enabled by software. We have sophisticated systems to find and address security vulnerabilities in our products, allowing us to grow, adapt, and advance security to continuously improve our products. We follow rigorous policies and procedures spelled out in our Security Development Lifecycle (SDL) to integrate security principles and privacy tenets at every step of hardware and software development. Our processors feature enhanced cryptography to accelerate performance and help secure global commerce. By working with our industry partner, Schneider Electric, we can achieve the levels of secure performance people expect and deliver technology they trust.

| Platform Feature [partial list] | Brief Description |
|---|---|
| Intel® Active Management Technology | Remote out-of-band management for efficient proactive and reactive system maintenance |
| Intel® Runtime BIOS Resilience | Intel® Hardware Shield technology providing hardened protection for system firmware |
| Intel® Trusted Execution Technology | Intel® Hardware Shield technology providing hardware root-of-trust for critical software |
| Intel® System Security Report | Communities Intel® Hardware Shield security policies to the operating system |
| Intel® Virtualization Technology | Enables a variety of operating system security services |
| Intel® Threat Detection Technology | Accelerates third party security software |

## Drive Efficiency and Productivity with Schneider Electric's HMI/IPC

Easy to install, to set up and to operate, Schneider Electric's Human Machine Interfaces (HMI) provide a simple and effective means of connecting systems, collecting data and presenting information in a meaningful format. From the smallest text display to the most sophisticated industrial PC (IPC) incorporating the latest technologies, Schneider Electric's HMI gives businesses a clear window into their operations. Not only does it let you know when all systems are good but more importantly, it helps keep them that way.[6]

### Intuitive Industrial PC: Harmony P6*

**HARMONY P6 TO DIGITIZE INDUSTRIAL MACHINES AND PROCESSES**

| | |
|---|---|
| **Smart Design & Engineering** | Shorten time to implement for automation people, and economical |
| **Workforce Empowerment** | Visualisation and control with associated software |
| **Asset Performance** | Connecting OT and IT for data management and optimization |
| **Cybersecurity** | End-to-end cyber security, including for remote connections |
| **Investment Continuity** | Most reliable and best care of user experience all along the life cycle |

Figure 1. Harmony P6 highlights

The Harmony P6, running at the Edge of EcoStruxure, improves productivity and performance. Running on associated software, it is reliable, and delivers the next stage of digital transformation and experience with end-to-end cybersecurity for more efficient operation and maintenance of capital assets. Harmony P6 connects OT to the field of Information Technology for the Industrial IoT (IIoT). With flow-based programming (FBP), WiFi, Bluetooth, and Windows operating systems running on an Intel® Core/Celeron CPU, it is an efficient solution compared with wire to the IoT.

Schneider Electric believes that by providing a comprehensive solution of both software and hardware for the customers, the Harmony P6 is a unique solution that distinguishes itself from the rest of the HMI of the competitors in the market (refer to Figure 2).

| Customer Value | Customer Benefit | Features |
|---|---|---|
| **Smart Design & Engineering** | **Asset Performance** | |
| Associated software | Save time and money + reduce risks | Tested and validated software and even pre-installed |
| Data management | Easy IT-OT connection | Node-Red with IIoT solution and EcoStruxure Machine SCADA Expert support IoT Edge to Cloud connection |
| Secured Remote connection | Remote access to installation | EcoStruxure Secure Connect Advisor for remote connections |

| Workforce Empowerment | | |
|---|---|---|
| New Technology | High-end specification and connectivity by modular design | Latest (8th-Gen) quad-core CPU in Intel IOTG, millions of possible configurations, interfaces, multi-displays |
| Operation | Easy Operation | Resisitive-multi touch, Glass touch with three noise preventive setting |
| **Cybersecurity** | **Investment Continuity** | |
| Cybersecurity | Security of data and assets | Designed with IEC-62443/Achilles, TPM for hardware encryption, UEFI BIOS and secure boot |
| Robustness | Environmental resistance | Wide temp., IP66/67, NEMA, C1D2, ATEX, Conformal coating... |
| Quick delivery and Long availability | Short lead time and Long lifetime of installation | Quick delivery (US, IT, FR, CH, JP) 10+ years availability, keep compatibility |

Figure 2. Harmony P6 features

## Enforces Cybersecurity

The Harmony P6 is ready with end-to-end cybersecurity systems to help protect data and assets. Based on Intel® Boot Guard, the boot integrity technology, the Harmony P6 runs on security enhanced hardware and software to strengthen its ability to mitigate cybersecurity risk. It is designed according to the Secure Development Lifecycle (SDL) process that is compliant to IEC 62443 and Achilles standards for industrial automation and control, such as:

- Designed according to standard guidelines for security analysis, threat modeling and tests, user documentation, etc.
- Compliant with Achilles standard, with McAfee Whitelisting* available as an option.
- Hardware encryption of operating system, storage, and passwords can be activated with Windows BitLocker* running the Trusted Platform Module (TPM) (available default) on the motherboard.
- Secure boot and secure operating system settings (passwords, patches, etc.).

The Harmony P6 together with the Edge Box* are also validated with EcoStruxure Secure Connect Advisor* to create end-to-end cybersecured infrastructure for remote connection to automation sites in the field.

Schneider Electric's preferred software that are tested and validated with the optimum hardware configuration are:

- EcoStruxure Machine SCADA Expert*
- EcoStruxure Automation Expert*
- EcoStruxure Plant Data Expert*
- EcoStruxure Secure Connect Advisor*
- EcoStruxure Augmented Operator Advisor*
- EcoStruxure Machine Advisor*
- EcoStruxure Traceability Advisor*
- EcoStruxure Clean-in-Place Advisor*

## Built for Connectivity

One of the key benefits of the Harmony P6 is being people-focused. Traditional computing, which relies on an on-premises centralized data center and the average internet bandwidth may not be well suited for the endless growth of real-world data. Schneider Electric provides businesses with the ability to respond to real-world data through the use of edge computing architecture and the Harmony P6. Through its interactive user-friendly dashboard, operators and engineers can easily understand the large amount of data that is collected from various sensors within the factory. It filters large data and aligns the information collected according to the routine operations of the factory, and automatically populates and shows this data on the screen. By doing so, operators and engineers are now able to identify challenges faced within the factory and deploy the necessary measures to target these issues in the shortest amount of time possible.

## Workforce Empowerment

The Harmony P6 offers fully-fledged customization for factories that are planning to adopt digitalization. It leverages asset performance with predictive maintenance, IoT Edge-to-Cloud connection, Smart Factory, and digitization which can meet the increasing demands of data management, analytics, and dashboards at the edge.

There are two main IIoT architectures that can run on Harmony P6:

1. HMI and Supervisory Control and Data Acquisition (SCADA) software visualization and connections with drivers available on software like Open Platform Communications United Architecture (OPC UA) and MQ Telemetry Transport (MQTT).
2. IIoT solutions with Flow-Based Programming (FBP) running Schneider nodes or more advanced IIoT software making the data wiring of the connected products to the apps, analytics, and services at the IT and Cloud levels.

Besides that, the Harmony P6 can run all software on Windows and offers improved application with:

- Solution guide and Tested Validated Documented Architectures (TVDAs) make ease of selection, integration, and maintenance of software association with Harmony P6, and provide a single contact window for technical support and repair.
- Configured-To-Order (CTO) Harmony P6 with associated software is selected with the online configurator. Customers can select the best combination of solutions for their application.
- Kitting for repetitive business allows users to define and validate a personalized software configuration and place repetitive orders to Schneider Electric's regional Flex Centers.

**How Schneider Electric's Harmony P6 Helped a Smart Factory to Run Operations More Efficiently**

An example of a successful adoption case study of Schneider Electric's Harmony P6 can be seen in a global company that provides solutions to the Pharmaceutical industry for its high purity water, clean utility requirements and process application. The Harmony P6 provides an innovative display with best-in-class visualization for the smart factory's production processes, but it also ensures ease of maintenance for troubleshooting with its reliable design. This unique solution is powered by 8th Generation Intel® Core™ Processors for a boost of data integration response and an additional layer of cybersecurity protection.

Harmony P6 Adoption Key Success Factors

- Critical parameters are shown for ease of decision making.
- Reduce overall service costs with remote maintenance & troubleshooting.
- Enhanced operator experience with innovative display and high-performing Intel® Core™ processors.

## Don't Trade Off Usability for Security

Today's digital transformation allows users to leverage real-time, data-driven insights to make more informed, productive decisions on-site and remotely. However, the exponential growth of technology and digitalization have undoubtedly led to a significant growth of high profile cyberattack incidents. Majority of critical business infrastructures are largely dependent on computer networks and IT solutions, which is why it is becoming increasingly critical for businesses to increase their cyber defense. As technology advances, so do the skills of cyber hackers. At Intel, we are committed to helping customers respond to attack vectors and keep their systems and data more protected by building layers of defense using our hardware, software, and security assurance expertise. We integrate hardware-based security that prioritizes capabilities such as authentication, encryption, and resilience. The Intel hardware-enabled security technology found with Intel® processors in the Harmony P6 offers an end-to-end cybersecurity system that is designed to increase security that protects your valuable and critical systems, sensitive data, and ultimately, your business against unwanted threats. Equip your business with the Harmony P6 to be both breach-resistant and breach-ready in the OT space.

**Summary of Harmony P6 Benefits**

- As the worlds of IT and OT converge, the need for endpoint protection of OT systems has grown exponentially. This is due to the increased risk of cyber-attacks, which can pose a serious threat to businesses. Securing hardware is fundamental root of trust.
- The three key priorities that Intel hardware-enabled security technology center around to meet specific challenges are Foundational Security, Workload and Data Protection, and Software Reliability.
- The Harmony P6 is powered by the 8th Generation Intel® Core™ Processors for a boost of hardware security.
- Harmony P6 is designed accordingly to the SDL process that is compliant to IEC 62443 and Achilles standards for industrial automation and control.

For more information, contact your Intel/Schneider Electric sales representative.

**Learn More**

- To know more about Harmony P6: https://www.se.com/ww/en/product-range/22953172-harmony-p6/
- Engage your Intel representative and find the resources your organization needs.

## References and Resources:


1. Colonial Pipeline ransomware attack: Everything you need to know https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/
2. How a major oil pipeline got held for ransom https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices
3. Hackers Breached Colonial Pipeline Using Compromised Password https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password
4. Intel® Hardware Shield – Below-the-OS Security White Paper https://www.intel.com/content/www/us/en/architecture-and-technology/hardware-shield-vpro-platform-security-paper.html
5. Use Intel Virtualization Technologies to Help Protect Endpoint Applications and Data without Impacting the User Experience White Paper https://www.intel.com/content/www/us/en/architecture-and-technology/cybersecurity-virtualization-technologies-paper.html
6. Discover Harmony P6 iPC with Intel | Schneider Electric https://www.youtube.com/watch?v=1evS1OBmRYA
7. Security Made Simple with the New 8th Gen Intel® Core™ Processors https://www.intel.com/content/www/us/en/developer/articles/technical/security-made-simple-with-new-8th-gen-intel-core-processor.html?wapkw=8th%20gen%20core%20
8. Brief: 8th Gen Intel® Core™ Processor U-Series https://www.intel.com/content/www/us/en/processors/core/8th-gen-core-family-mobile-brief.html?wapkw=8th%20gen%20core%20ptt
9. 8th Gen Intel® Core™ vPro™ Processor Product Brief https://www.intel.com/content/dam/www/public/us/en/documents/product-briefs/8th-gen-core-vpro-processor-brief.pdf
10. Intel® Active Management Technology https://www.intel.com/content/www/us/en/architecture-and-technology/intel-active-management-technology.html




0622/KSW/In2/PDF