CHESS-E: Deep Isolator for IIoT

Application Note
February 2022

SECURWEAVE

SECURWEAVE.COM
INFO@SECURWEAVE.COM
+91-8790532463

SECURWEAVE

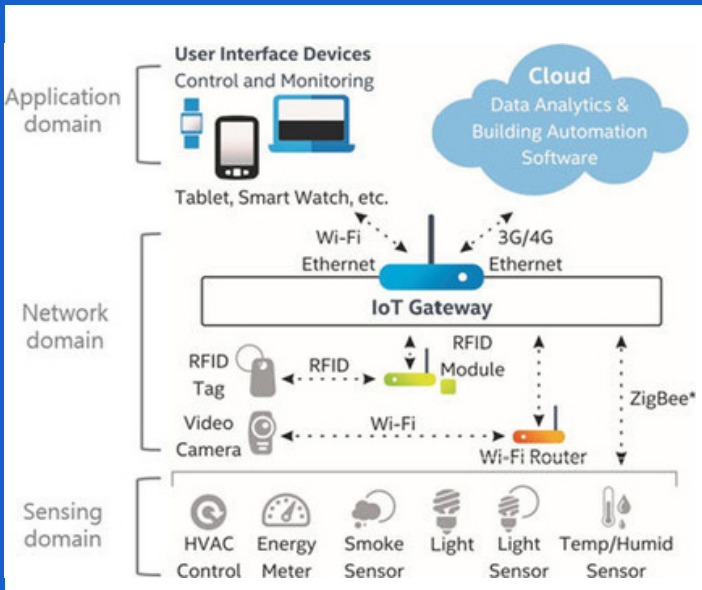
Introduction

With the emerging revolution of Industry 4.0, the relevance and application of Industrial Internet of Things is growing exponentially in a wide spectrum of industries ranging from small factories to energy infrastructure and process automation. The role of edge devices is naturally broadening with heavy emphasis on in-premise analytics, distributed supervisory control, massive real time data collection and storage etc. being offloaded to edge. The envisioned trend is to move control, communication, computation and decision making closer to the location where data is generated i.e. to the edge nodes.

SECURWEAVE

The Evolution of Edge Nodes

With the aforementioned premise, edge nodes need to evolve to meet stringent requirements such as performance, scalability, interoperability, agility and reconfigurability for efficient deployment, safety, mixed criticality etc. These requirements are beyond the reach of traditional PLCs, currently used in industrial environments and this is driving adoption of MultiProcessor based hardware in industrial scenarios.



Security Challenges

The evolution of IoT in industry also brings security challenges. Apart from the strict isolation needs of multiple applications that execute in the edge devices there is also the need to have security between IT & OT networks. Few points to consider here are:

- Fragmentation between the IT (cyber) and OT (physical/operations) networks
- Porousness across domains where IT/OT networks converge, a high potential exists for data leakage
- Lack of security in preventing attack penetration of the IT network from the OT network or vice versa, and malicious activity emanating from one and damaging the other.

SECURWEAVE

Virtualization in Edge Platforms

With mixed-criticality workloads at the edge level and the need for stringent security, virtualization becomes a crucial need for providing secure, safe and flexible execution environments on next generation IIoT edge nodes.

A conventional virtualization solution involving a general purpose hypervisor will not scale with the specific needs of IIoT segment and the hypervisor used should be able to address the specific needs of IIoT world, especially the security.

Note: An example of a recent adoption of virtualization in IoT edge device is TTTech's open edge computing platform 'Nerve', which has integrated ACRN hypervisor for real time performance benefits. More details available at https://www.tttech-industrial.com/real-time-virtualization-nerve-acrn-intel-tcc/

SECURWEAVE

Security Hypervisor

According to Section 8 of IISF Report
To achieve the security objectives of IoT System i.e. Availability, Integrity and Confidentiality, one of the suggested technique to be implemented is Isolation Techniques for Endpoints

Isolation refers to the technique used to shield a component of a system from unwanted effects where an element of the endpoint cannot be affected by other elements of the endpoint, thus shielding its functionality from failures and malicious activity.

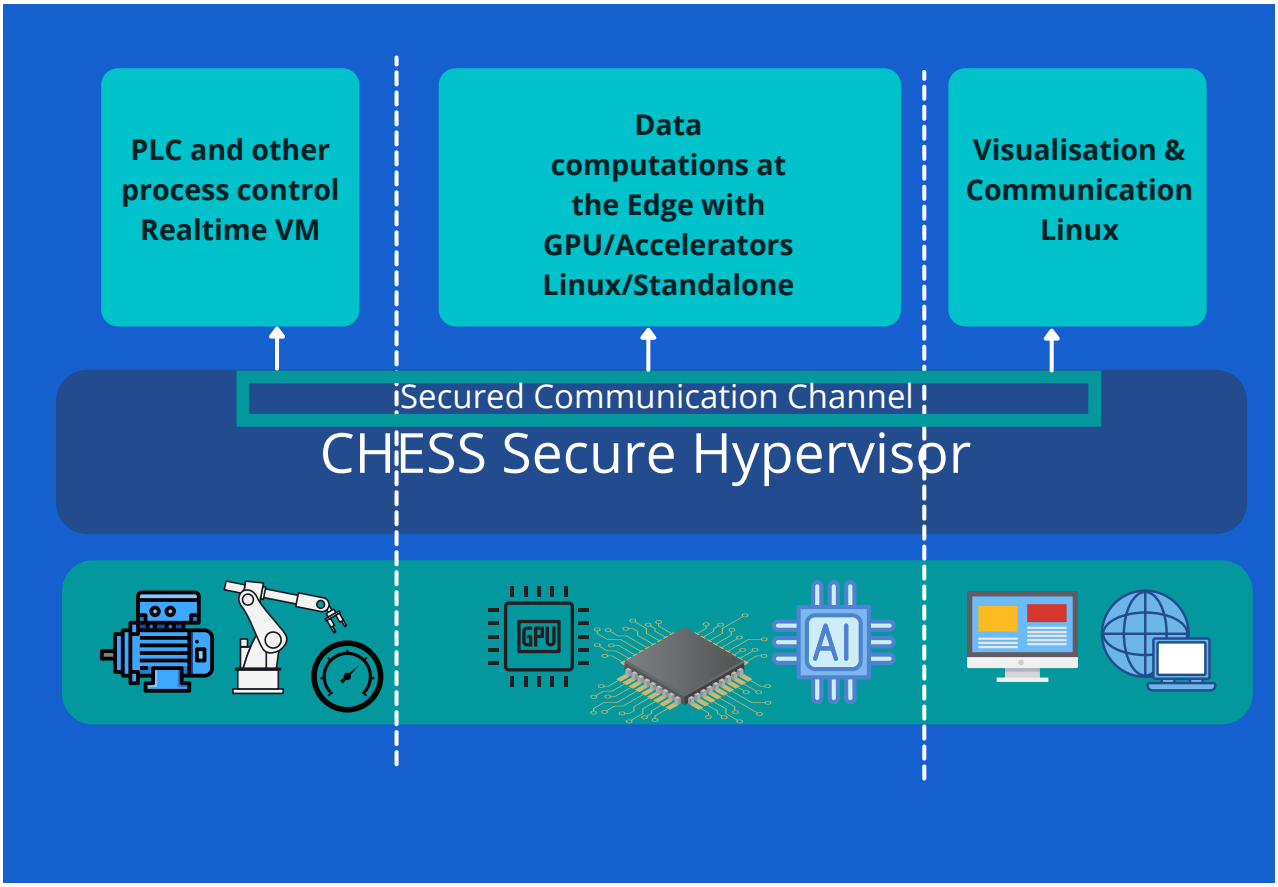
The virtual isolation model sometimes referred to as hypervisor isolation uses a hypervisor to implement isolation between each virtual instance running on the device. In addition to isolating components from each other, they also enable communication control between components and devices according to a security policy.

MILS Architectural Approach also recommends and defines Separation kernel component in its architecture for Isolation

Virtual isolation enables the same economies of scale that have driven the growth in cloud adoption. On the edge, virtualization enables OT components to function without change in their existing operating system, while allowing security functions to run independently in its own OS. As the security OS is on the same physical device as the OT operating system, it can provide many controls such as embedded identity, secure boot attestation and communication interceptor pattern, all below the OT operating environment.

CHESS Deep Isolator: Secure Hypervisor based Platform For IIoT Edge

SECURWEAVE



Configurable Hardware Enforced Security Solution (CHESS) is SecurWeave's security platform for embedded applications. The key component of CHESS is the homegrown security hypervisor that is designed and developed by following secure practices. The security hypervisor module of CHESS is currently being enhanced to function as a secure hypervisor for IIoT edge platforms.

Key Features

- Determinism
- Safety
- Security
- Flexibility

Apart from security via strict isolation an additional capability of CHESS secure hypervisor is the ability to detect, prevent and report malware attacks that target the kernel of the Operating System.

SECURWEAVE

Conclusion

SecurWeave is looking forward to collaborating with industry leaders in the IIoT segment to develop secure platforms for the next generation IIoT. SecurWeave's decades of experience in developing security solutions and hypervisors gives us a unique edge in developing customized hypervisor based platforms for IIoT edge systems.