Introduction

1. Overview

Industrial automation refers to the integration of control systems and advanced technologies to automate industrial processes, thereby enhancing efficiency and productivity while minimizing the need for human intervention. This approach leverages a variety of control systems such as programmable logic controllers (PLCs), industrial robots, IoT devices, and other automation tools, to manage and operate processes autonomously, leading to significant improvements in operational efficiency and overall productivity.

2. Importance of Cybersecurity

A cyberattack on industrial automation systems targets the disruption or incapacitation of critical industrial control systems, such as SCADA (Supervisory Control and Data Acquisition) systems or other industrial control mechanisms. These attacks can result in severe consequences, including operational disruptions, data loss, and potential risks to human safety and environmental security.

Problem Statement

According to ABI Research and Palo Alto Networks report, OT environments have become very attractive targets, as they have immense financial potential. This explains why in the past year 2023, 70% of industrial organizations fell victim to cyber attacks and 26% face attacks weekly or more. Beyond the immediate consequences of data and revenue loss, these attacks disrupt the continuity of business operations.

Threats are evolving

Beyond the existing threats, owners and operators of industrial assets are increasingly aware of emerging technologies and their associated risks. The study highlights that AI is a significant concern, with 74% of respondents identifying AI-based attacks as a critical threat to their operational technology (OT) infrastructure.
Similarly, the adoption of 5G technology introduces new vulnerabilities. While organizations are integrating 5G to enhance connectivity, efficiency, and transmission speeds, nearly 70% of respondents recognize it as an escalating threat vector.
Industry professionals surveyed emphasize that securing industrial devices against emerging technologies such as AI, 5G, and remote access will be the primary cybersecurity challenge for their organizations over the next two years.

TECHNOLOGY

How a major oil pipeline got held for ransom

The largest petroleum pipeline in the country was reportedly breached by a single leaked password.

by **Sara Morrison**
Updated Jun 8, 2021, 10:20 PM GMT+5:30

Colonial Pipeline shut down its massive oil pipeline after a ransomware attack took some of its systems offline. Above, a Colonial facility in 2016. Luke Sharrett/Bloomberg/Getty Images

BBC

Home News Sport Business Innovation Culture Travel Earth Video Live

Meat giant JBS pays $11m in ransom to resolve cyber-attack

10 June 2021

Share

The world's largest meat processing company has paid the equivalent of $11m (£7.8m) in ransom to put an end to a major cyber-attack.

IT-OT Convergence

According to the survey, over 60% of respondents identified the complexity of OT security solutions as a significant barrier when purchasing software and equipment, underscoring the urgent need for more simplified and streamlined approaches. Furthermore, 40% reported conflicts between OT and IT teams, highlighting a critical misalignment that poses a serious risk to security efforts, especially since IT remains the primary attack vector. This concern is driving 70% of respondents to consolidate IT and OT solutions under a single cybersecurity provider. Notably, executives are 33% less likely than frontline operational staff to recognize industrial disruptions, revealing a concerning disconnect that hampers informed decision-making and effective investment in security solutions.

Analysis

Industrial automation systems are categorized as Fixed (Hard), Programmable, Flexible (Soft), and Totally Integrated Automation (TIA) systems. These systems are primarily used in high-volume manufacturing with specialized equipment that can be adjusted for different product designs. Programmable automation relies on instruction programs to direct production processes, while flexible automation uses a central computer to control system components. Key terms in this context include OT Networks, SCADA systems, DLCs, PLCs and IIOT. OT, or Operational Technology, refers to hardware and software that monitor and control industrial processes, distinguishing it from traditional IT systems.

1. **SCADA**(SupervisoryControlandDataAcquisition)systemsmonitorandcontrolindustrial processes through a combination of computers, networked data transfers and graphical user interfaces. These systems are crucial in industries like manufacturing, power generation, and infrastructure management.

2. A **Distributed Control System (DCS)** is another critical system, featuring autonomous controllers throughout a manufacturing plant. This decentralized approach enhances control stability, process quality and productivity. DCS, along with PLCs, forms the backbone of industrial automation, but they are also susceptible to cyber threats.

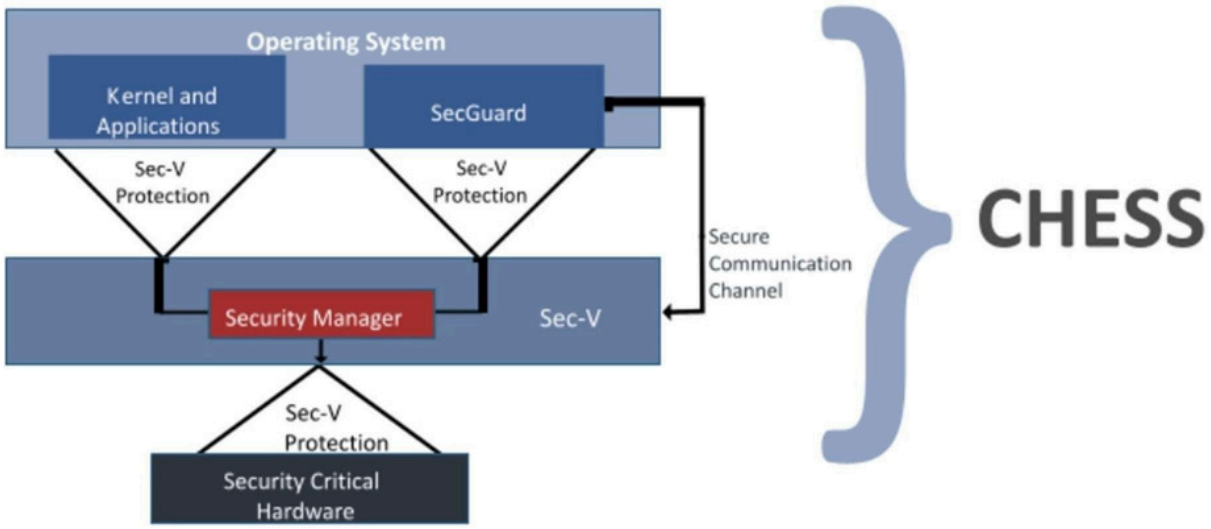
3. **PLCs or Programmable Logic Controllers**,automate processes by continuously monitoring inputs and controlling outputs based on specific programs. However, PLCs can be vulnerable to cyberattacks, which may target them to gain deeper access to OT networks.

4. Attackers can weaponize PLCs, compromising engineers' workstations and accessing critical systems. The complexity of these systems, combined with their integration into essential infrastructure, makes them attractive targets for cyber espionage and attacks.

5. Given the complexity and diversity of **Industrial Internet of Things (IIoT)** systems—including heterogeneous devices, a mix of legacy and modern connectivity protocols, and distributed networks—sophisticated attacks such as ransomware pose significant challenges.

Solution and Implementation

In Industrial automation, safeguarding systems from increasingly sophisticated cyber threats is paramount. A highly effective strategy for this is implementing a defense-in-depth (DiD) approach, which uses multiple layers of protection to secure critical assets. SecurWeave's CHESS solution is designed to enhance this strategy by addressing critical and zero-day cyberattacks, particularly in robotic and industrial systems.



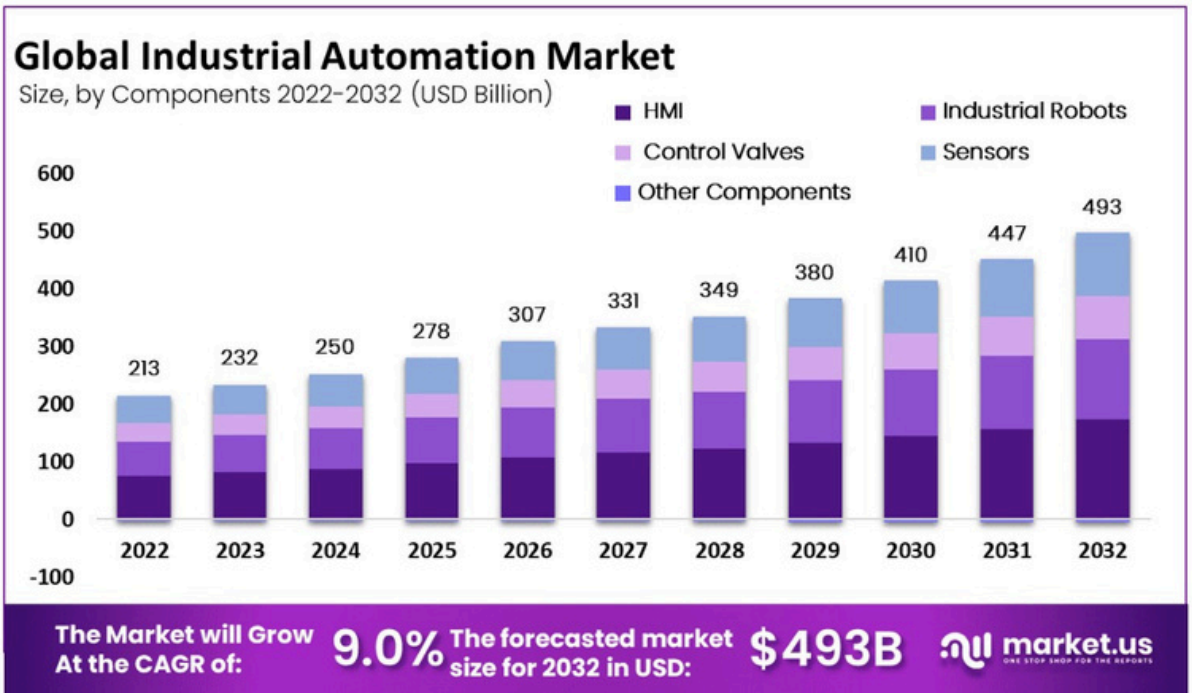
CHESS is built around a secure hypervisor that protects these systems from advanced threats like Advanced Persistent Threats (APTs) and rootkits, which are notoriously difficult to detect and mitigate. This solution is crucial in an industrial automation environment, where the integrity of robotic systems directly impacts operational safety and efficiency.
Key Components of CHESS:

1. SecGuard: This is CHESS's user interface, which provides tools for alerting, policy configuration, and secure updates. It is equipped with RESTful APIs, enabling seamless configuration and management, thus ensuring that system administrators have real-time control and oversight over the security measures in place.

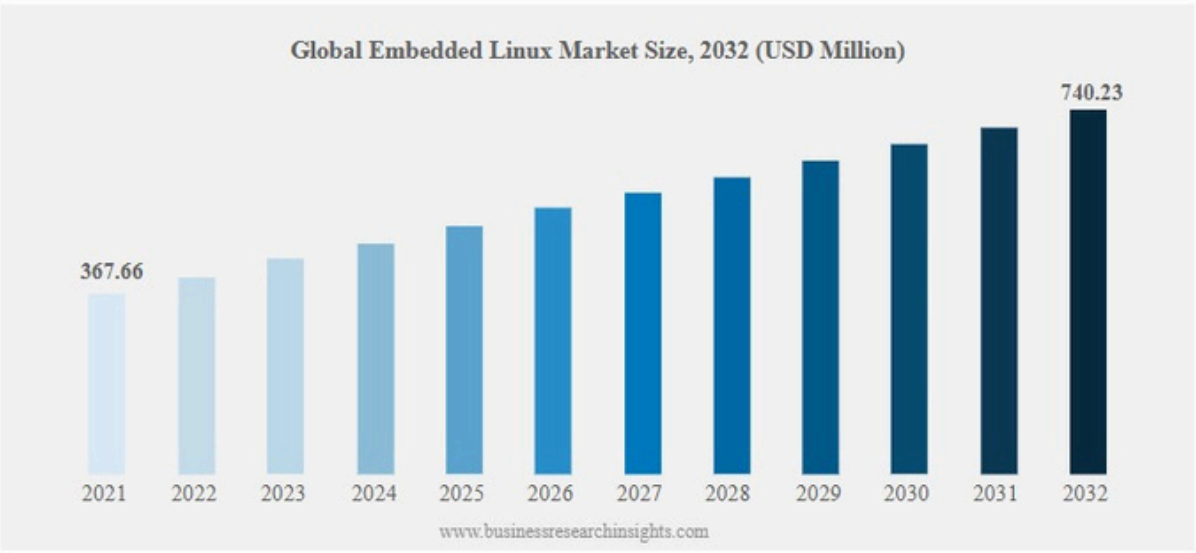
2. Sec-V (Security Hypervisor): Sec-V is a purpose-built security hypervisor specifically designed to detect, contain, and analyze kernel-mode APTs. Given the rise in APTs targeting the kernel, Sec-V's ability to operate at a higher privilege level than the OS kernel is critical. This elevated privilege grants it a strategic advantage in monitoring and managing systemactivities, enabling it to identify and neutralize threats that originate from within the kernel or from I/O devices—both common vectors for security breaches in Industrial systems.

By leveraging this elevated position, CHESS ensures that even if the operating system or peripheral devices are compromised, the core security and functionality of the industrial systems remain intact and secure. This robust defense mechanism is vital in maintaining the continuous, safe, and efficient operation of automated industrial environments.

Market Size

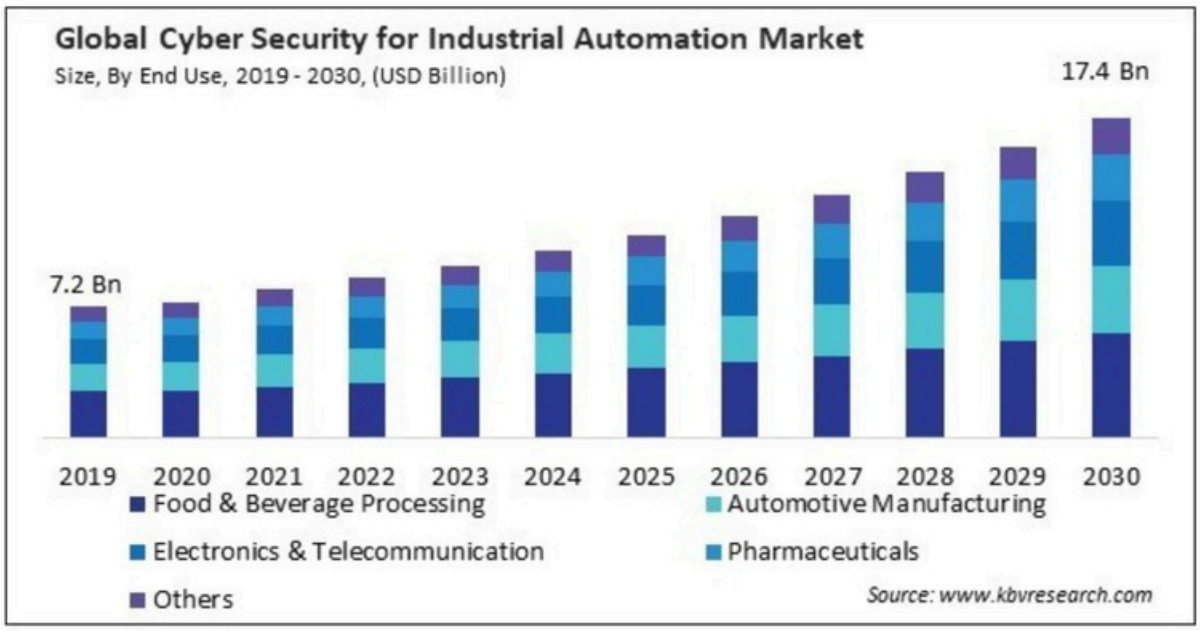


Embedded Linux denotes the deployment of the Linux operating system within embedded systems, which are specialized computing devices engineered for dedicated functions. Unlike general-purpose computers, embedded systems are tailored to perform specific tasks and typically operate under resource constraints, including limited processing power, memory, and storage. Linux is widely adopted in embedded systems because of its open-source nature, flexibility, and reliable networking capabilities.



Industrial Automation & Embedded Linux markets are growing at a CAGR of 9% and 6.57% respectively.

Global Cyber Security For Industrial Automation



Cyber Security For Industrial Automation market is growing at CAGR of 9.2% from 2023 to 2030

Key Players

- Cisco Systems Inc.
- Schneider Electric SE
- Dell Technologies, Inc.
- Rockwell Automation, Inc.
- Honeywell International, Inc
- IBM Corporation
- ABB Ltd.
- Microsoft Corporation
- Siemens AG
- Palo Alto Networks, Inc.

Addressable Market

Intel Technology and Linux are extensively utilized across a broad spectrum of industrial systems in various sectors. For example, Red Hat, Inc., a global leader in open-source solutions, recently announced a new industrial edge platform developed in collaboration with Intel. This platform introduces a contemporary approach to the design and operation of industrial control systems.

Automation and Control of Products

- PLC
- HMI
- RTU
- Edge Gateway

Market Leaders

- Schneider Electric S.E.
- Siemens AG
- Rockwell Automation Inc.
- ABB Ltd.
- Honeywell International Inc.
- Emerson Electric Co.
- Hitachi Ltd.
- IBM Corporation
- Mitsubishi Electric Corporation
- Yokogawa Electric Corporation
- Omron Corporation
- Advantech
- Dell Technologies
- Moxa

Conclusion

After thoroughly analyzing the challenges and implementing solutions in industrial automation. We have also evaluated the market size and potential for CHESS within industrial systems. It is clear that SecurWeave's CHESS is well-aligned with market demands, offering a robust and secure solution specifically suited for Industrial Automation

SECURWEAVE

securweave.com
info@securweave.com
+91-8790532463

Plot No 13/A, Laxmi Nagar Colony, Manikonda,
Rangareddy Telangana,
India 500089