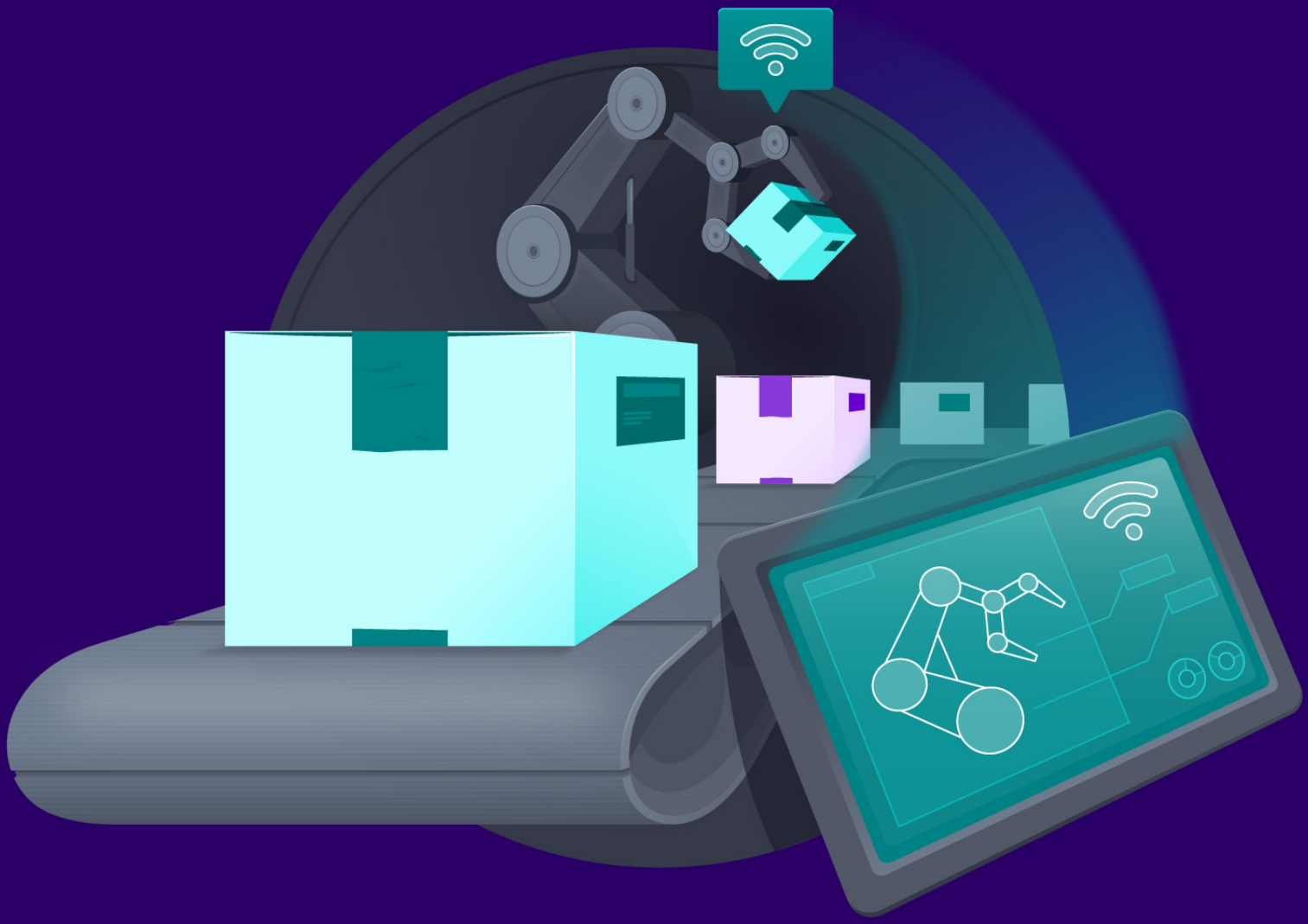
# State of ICS Security in the Age of Cloud



cloud security alliance®

The permanent and official location for Industrial Control Systems Security WG is at:
https://cloudsecurityalliance.org/research/working-groups/industrial-control-systems-ics-security/

# Acknowledgments


## Lead Authors

William Ho
Sabri Khemissa
Darnell Washington

## CSA Global Staff

Hillary Baron
Frank Guanco
Claire Lehnert
Stephen Lumpe
Ekta Mishra


**About the Industrial Control Systems (ICS) Security Working Group:**

As ICS advances from communicating with networks within the enterprise to interacting externally via IoT platforms and the cloud, efficiency, effectiveness and scalability have improved. However, these advances' additional complexity and larger attack surface have increased the opportunity for cyber-attacks. The ICS Security Working Group (WG) aims to develop security guidance to encourage cloud providers, asset owners and device manufacturers towards adopting best practices to secure ICS.

# Table of Contents

# Introduction

## Goal

This document aims to create awareness and share insights on the benefits of leveraging cloud computing for Industrial Control Systems (ICS) and Operational Technology (OT). It also attempts to stimulate discussion within the industry to communicate, exchange thoughts, debate, conclude, and share the outcomes with the ICS Working Group community.

## Audience

The intended audience includes the critical infrastructure sector, commercial organizations, ICS suppliers, and service providers. This includes cloud service providers, cybersecurity service providers, and managed security service providers, who apply and use ICS in their crucial business processes.

# Overview

Critical infrastructure protection involves activities that enhance the cybersecurity and physical security of public and private infrastructures that are critical to national and economic security, and public health and safety. Because a large percentage of the world's critical infrastructures is owned and operated by the private sector, and public/private partnerships are crucial for successful critical infrastructure protection.

ICS owners face threats from highly sophisticated global adversaries with intent to disrupt critical functions, and have increasingly become more agile and persistent. Ransomware against ICS systems has become prevalent as well as the exploitation of data through intelligence collection using spyware and injection of malicious code into vulnerable systems.

These critical infrastructures leveraging OT systems, especially ICS, are an increasingly attractive target for highly-sophisticated, bad cyber actors around the world. A more worrying trend has developed with the increased connectivity between IT and ICS (IT-OT convergent). This creates a potential opportunity for adversaries who are now able to compromise IT systems connected to the internet, secure their footholds, and move to the ICS to disrupt industrial processes.

A cyberattack resulting in disruption or failure of ICS may cause service disruptions and/or a safety risk to people and essential services, as well as hefty financial losses. Therefore, the cybersecurity and resilience of ICS are of utmost importance to society as a whole, utilities and other critical infrastructure operators, and organizations and industries using ICS.

Building a more stable structure for ICS security could mean significant alterations in how global systems work and are integrated. The current state of ICS security has great opportunities for modernization, efficiency, and shared services.

The COVID-19 global pandemic underscored the need for scalable off-premise (yet accessible) solutions. Most ICS systems define risk-based performance standards that chemical facilities must comply with if they present a high risk, and are managed by onsite security processes and protocols.

These ICSs did not have plans inplace for a pandemic included in site security plans, and implemented cloud-based, risk-based measures designed to deter cyber sabotage, including preventing unauthorized onsite or remote access to critical process controls.

# High-risk environments

One of the current effects and impacts is that little risk mitigation and remediation efforts are possible with limited human resources. The need for human involvement to maintain security, patching, hard-to-test production environments, and low visibility of assets, analytics, and operational data creates a higher risk.

In practice, legacy and unpatched systems are exposed to the public-facing internet, inviting remote attacks.

# Recent  Cyber incidents against ICS

According to *Infosecurity Magazine*, approximately one in three ICS systems were targeted by malicious activity in the first half of 2021, with spyware a growing threat. The Russian security vendor Kaspersky claimed its solutions blocked over 20,000 malware variants from more than 5,000 families during this period.

- April 2021 - Colonial pipeline hackers infiltrated the company's system that transports roughly 2.5 million barrels of fuel daily from the Gulf Coast to the Eastern Seaboard. The outage led to long lines at gas stations, many of which ran out, and higher fuel prices.
- April 2020 - Israel successfully defended against a cyberattack targeting the command and control systems of water treatment plants, pumping stations, and sewage in the country.
- April 2020 - U.S. officials reported seeing a surge of attacks by Chinese hackers against healthcare providers, pharmaceutical manufacturers, and the U.S. Department of Health and Human Services amidst the COVID-19 pandemic.
- April 2020 - Government and energy sector entities in Azerbaijan were targeted by an unknown group focused on the Supervisory Control and Data Acquisition (SCADA) systems of wind turbines.
- January 2020 - A Russian hacking group infiltrated a Ukrainian energy company.
- December 2019 - Iranian wiper malware was deployed against the network of Bapco, the national oil company of Bahrain.
- October 2019 - India announced that North Korean malware designed for data extraction had been identified in the networks of a nuclear power plant.
- June 2019 - U.S. officials reveal ongoing efforts to deploy hacking tools against Russian grid systems as a deterrent and warning to Russia.

## Some Notable Breaches against ICS (2014-2021)

| Year | Attack Type |
|---|---|
| 2021 | Colonial Pipeline attack: Took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast and was the result of a single compromised password |
| 2019 | Ransomware attack: Norway's Norsk Hydro experienced production stoppages |
| 2019 | Unknown virus: Thailand experienced a partial shutdown of the eyeglass lens manufacturer Hoya |
| 2018 | Wannacry ransomware: A Taiwanese chip maker, TSMC, shut down several plants |
| 2017 | Triton malware: A Saudi Arabian petrochemical plant experienced disruption to an oil refinery |
| 2017 | NotPetya ransomware: Starting from a Ukrainian software firm, it spread to the pharmaceutical company Merck, the snack company Mondelez and some other big industries worldwide, leading to a combined financial loss of over $10B USD |
| 2016 | Industroyer malware: The Ukraine's capital, Kyiv, was attacked which caused 20% of their power grid to be offline for between 1 and 6 hours, impacting 230,000 customers. |
| 2015 | Spear phishing/BlackEnergy3 malware: Ukraine Power grid experienced an attack which remotely switched off substations, resulting in widespread loss of electricity supply during winter |
| 2015 | SQL injection and phishing: US Kemuri Water treatment plant - Personal information of 2.5 million customers leaked |
| 2014 | Havex malware: Attackers compromised a number of strategically important US and European organizations such as energy grid operators, major electricity generation companies, petroleum pipeline operators for spying purposes, and had capacity to disrupt the energy supplies in affected countries |
| 2014 | Unknown: An attacker compromised control system components of a US Utility using remote access |
| 2014 | Email phishing/malware: A German steel mill was compromised and blast furnaces were inappropriately shut down leading to loss of control for the plant operators, which caused physical damage to the system and process interruption |

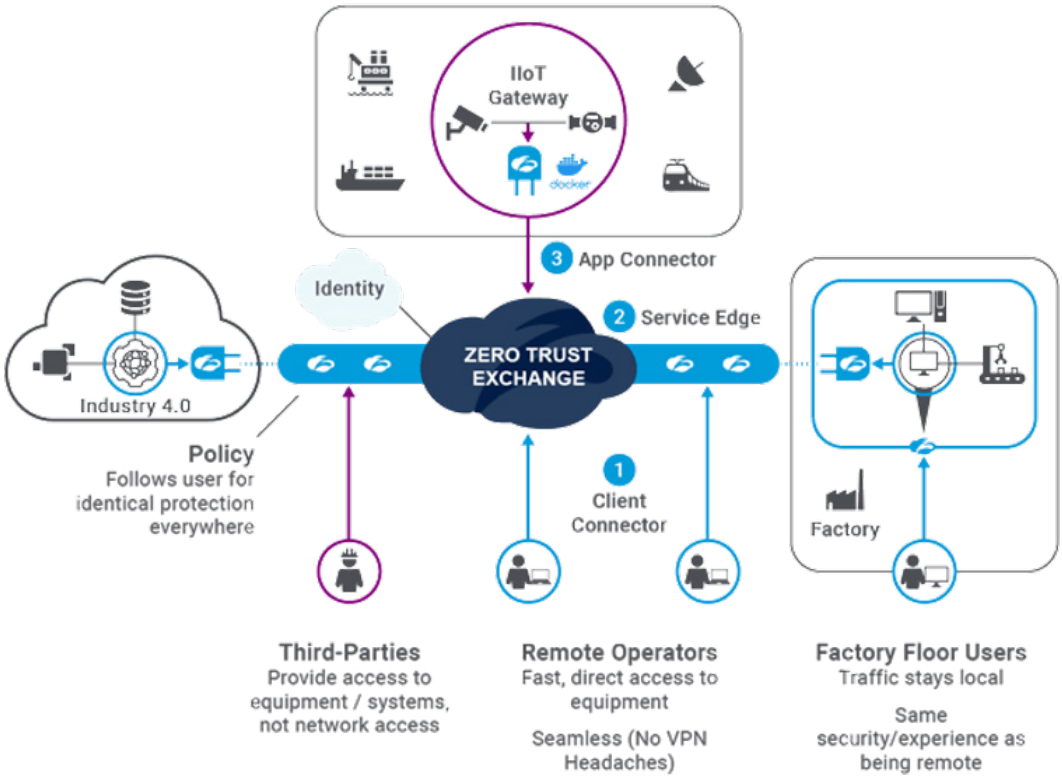
# Industry Trends

Visibility is commonly the biggest hurdle when it comes to protecting ICS environments from cyberattacks. ICS environments can gain visibility of their OT networks without disrupting their processes by following methods that meet the unique needs and requirements of OT devices. This includes active and passive monitoring of network traffic to identify assets, baselining normal activity to spot anomalies, and analyzing log data for indications of cyber events. With that visibility, organizations can effectively implement additional protective controls, such as industrial firewalls to segment critical assets and establish secure conduits.

Technical advancements that include high-performance microprocessors and Artificial Intelligence (AI) platform evolution provided new capabilities that managed fault and pre-failure notification, and deterministic and predictive models that provided insight to build robust ICS system environments.

Some of the prevalent changes include:

- Zero Trust Networks: Products and services that create an identity-based logical boundary that is hidden from discovery, and access is restricted using a trust model to protect named entities.




- Network zoning and conducting (ISA/IEC 62443):- Compartmentalizing a group of interfaces to a specific security policy to protect others without explicit mission-based requirements to perform required tasks.

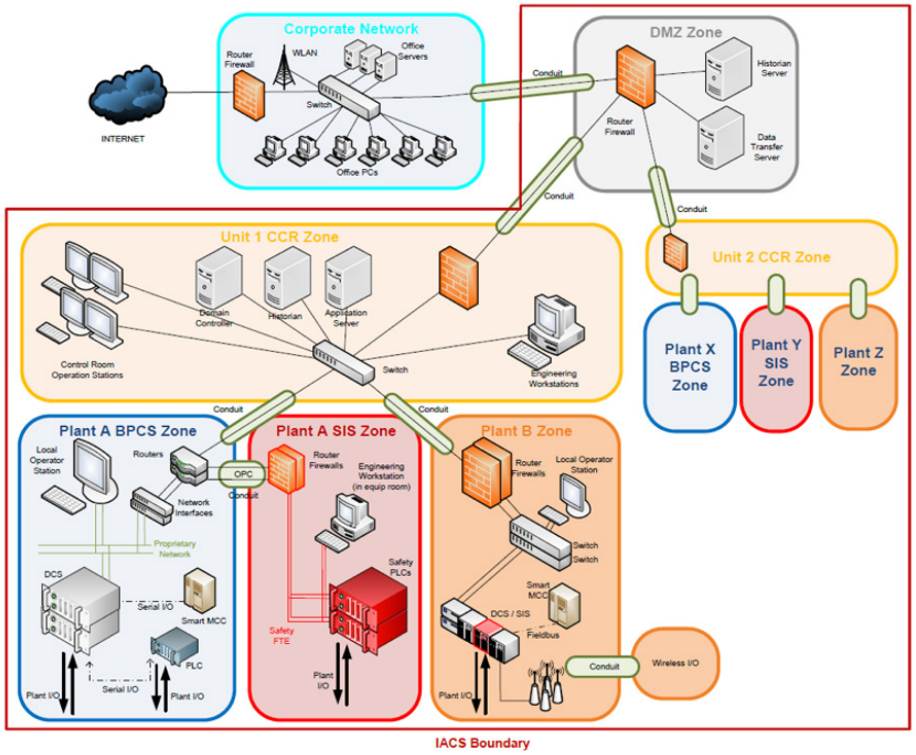



*Image courtesy of Asset Guardian*

- Web-configurable device firewalls: Products and/or services that manage and protect dataflows internal to ICS systems.

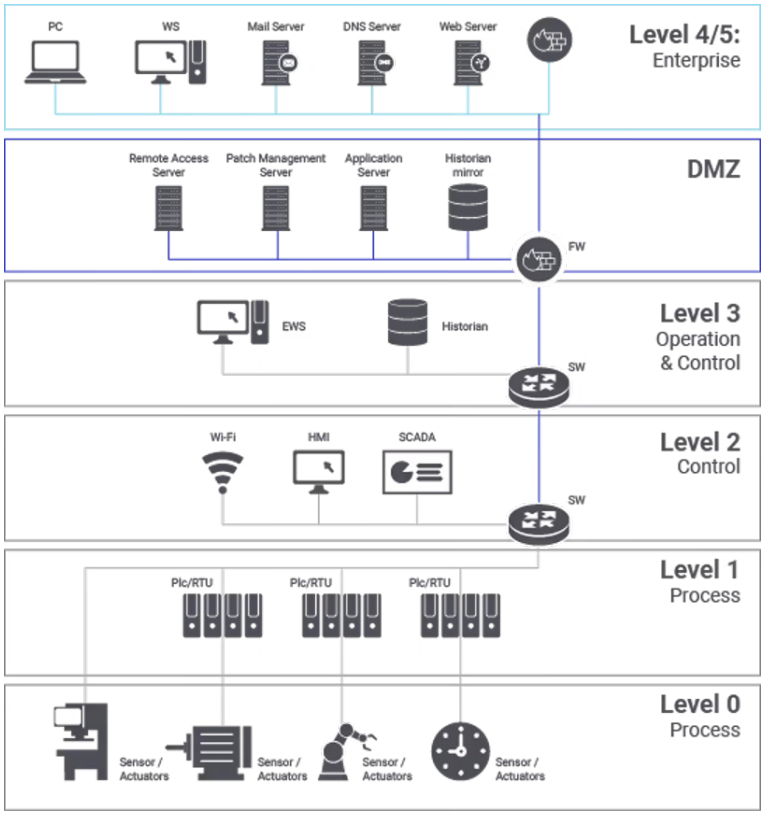



*Image of the Purdue model courtesy of Zscaler*

- Centralized user account management: Allowing IT administrator visibility and monitoring over every device, application, or network access across the organization, and having central control over users and ICS devices to ensure that traffic stays within the organization.

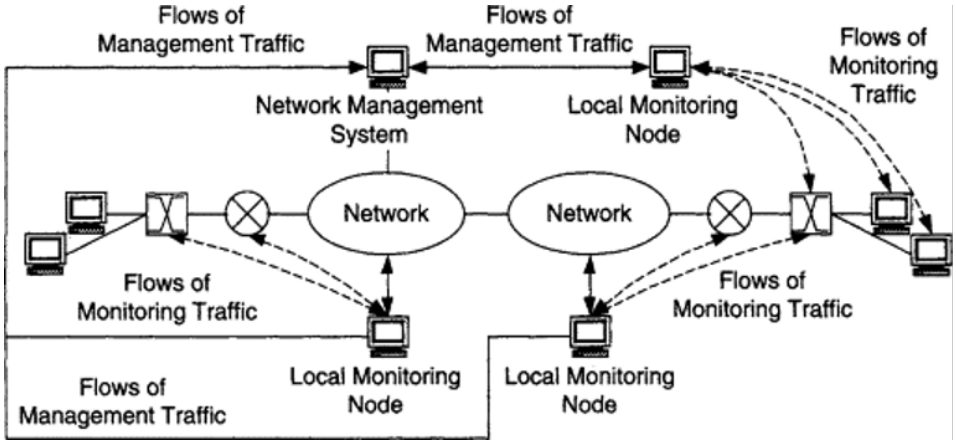



*Image courtesy of Sciencedirect.com*

- Embedded VPN: Enabling devices that can communicate to other devices through external servers avoiding firewall configuration and proxy rules.

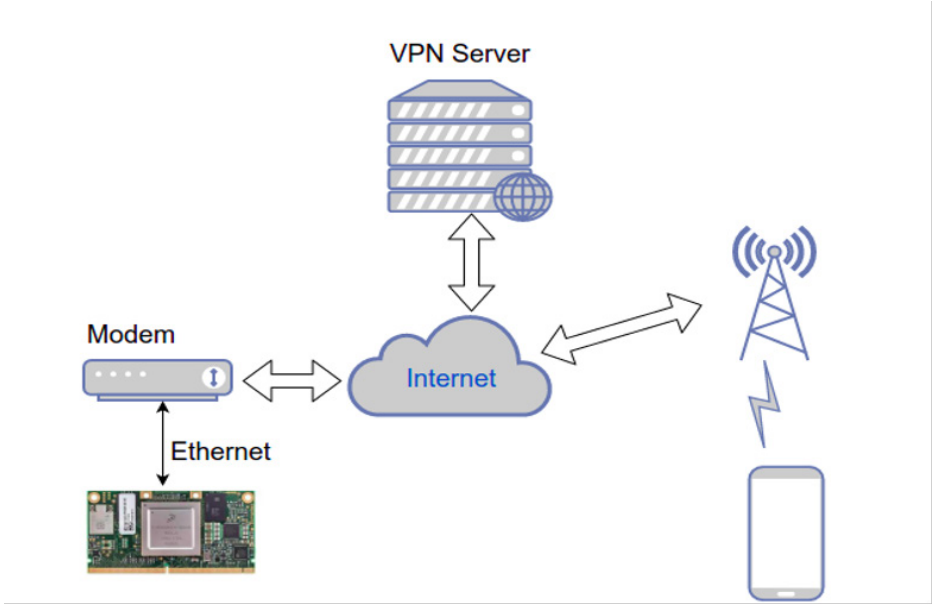
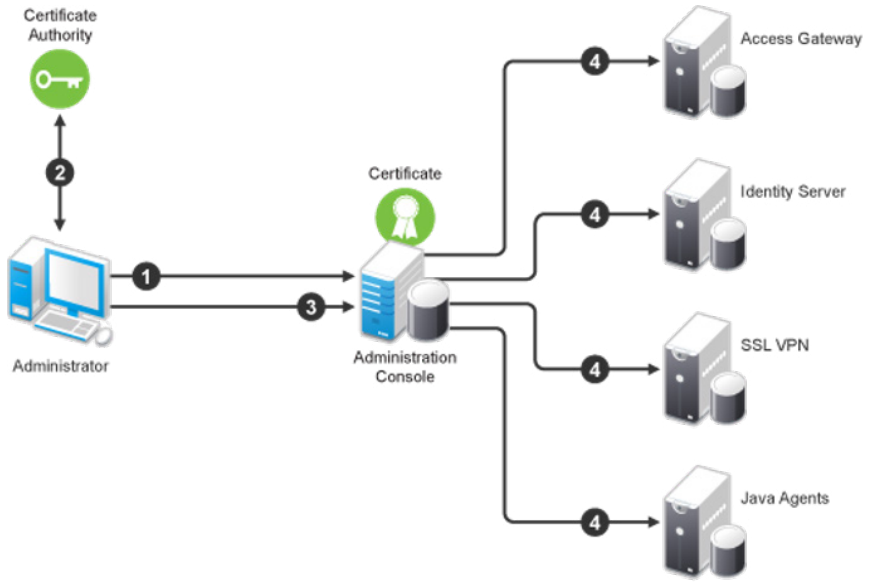



*Image courtesy of Toradex*

- SSL/TLS certificate management: Web-enabled applications that create secure transactional layers between clients and web services.




- Encrypted HTTPS and MQTT comms: Secure lightweight messaging platforms for ICS devices.

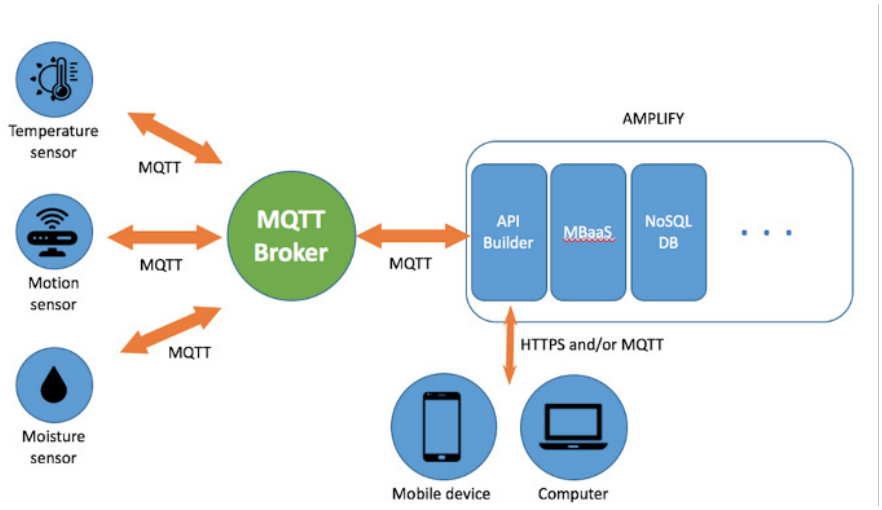



*Image courtesy of Ashiq KS*

# Artificial Intelligence in the Cloud

AI is probably one of the most interesting industry trends within ICS environments. Models are being developed that integrate ICS and Software as a Service (SaaS) models for resource allocation, predictive modeling, and in some cases, increasing or decreasing production or flows based on supply, inventory, price, or peak usage conditions.


*Image courtesy of Control Global*

AI in the cloud can also be used to detect fraudulent use or misuse of resources by establishing baseline, trend analysis, and performing system auditing without human intervention.
AI in the cloud can also provide decentralized security through the implementation of blockchain ledgers for supply chain security and the integrity of transactions at an enterprise level.

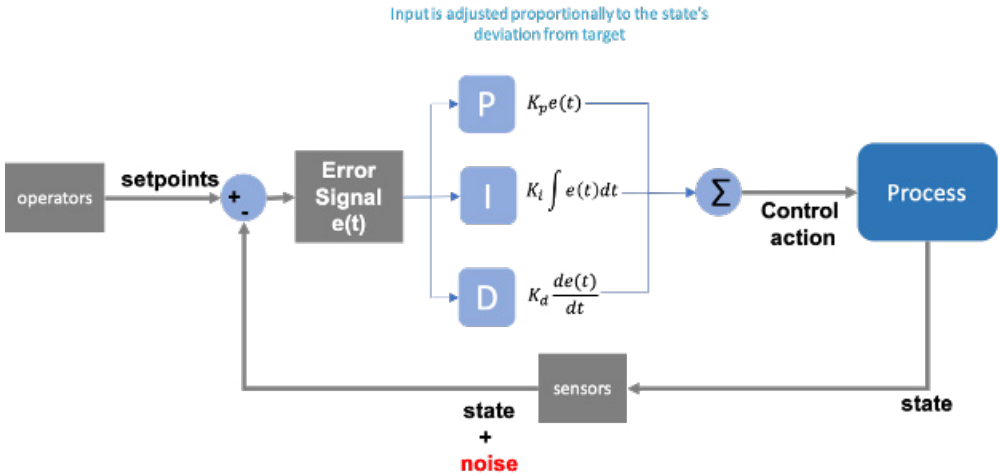



*Image Courtesy of Towards Data Science*

# Multifactor authentication

Recent implementations of multifactor authentication have been adopted where the phone is used, as the alternative device has proven to be a successful alternative (including callback) and has been successfully implemented to eliminate the use of legacy username/password combinations, especially when used from remote locations.

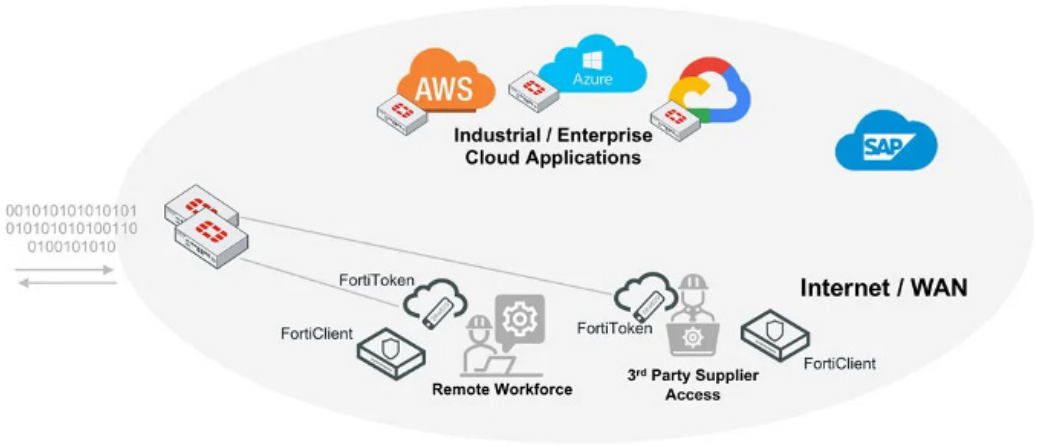



*Image courtesy of Fortinet*

# Data Localization

Not all data needs to be made available to all systems for appropriate input, processing, transmission, and storage of ICS data. Data localization stores data on premise until needed by other subsystems used for production, manufacturing, and reporting.

## Edge computing devices

Edge computing devices and sensors have evolved significantly over the past few years providing intelligence and support for sensors that can detect heat and temperature variations as well as physical security for ICS environments. CCTV and IP cameras with AI-based analytics can perform many ICS tasks with limited degradation of resources such as bandwidth and compute power within these environments.

## Containers

Containers in the ICS world are lightweight standalone executable packages that can run in a specific environment and perform functions that can easily be ingested by other platforms or applications.

As containers make their way into ICS environments, we will see more robust applications and performance improvements when collecting, disseminating, and distributing information to local and remote computing resources.

## Online Training and Education

Organizations worldwide have transformed distance learning and remote training to support the safety and well-being of employees and their communities. Use of virtual training and simulation tools have now been proven to be robust and effective, and have equivalent competency qualifications as on-site training.

Future trends in augmented reality and virtual reality training and education solutions are expected to train individuals in production and ICS environments, complemented by online collaboration tools integrating voice, video, and chat.

## Off Premise Cloud Administration

Remote workforces will provide off-premise cloud administration and monitoring of ICS controls. These will include remote diagnostics and even high-availability failover and switching based on specific ICS needs. Off-premise cloud administration will be supported by digital diagnostic tools, sensors, and actuators that will increase bandwidth and software requirements needed for data and event visualization.

# State of ICS Security in the Age of Cloud

If we had treated the many global ICS issues relative to the COVID-19 pandemic we would have a referenceable model relevant to best practices, information sharing, and the sense of urgency to ensure appropriate resources, collaboration, and development lifecycles, we would probably be further along. Public health and safety concerns over COVID-19 uncovered weakness in our worldwide governments to have effective collaboration, reporting, and information systems in place to contain the spread of infectious disease. If public health and public safety concerns even without COVID that (dependent on ICS technology) were considered at the magnitude as a pandemic disease, more significant allocations of resources and effort would be in placed of ICS and cybersecurity.

Comparison and Contrast of Pre-Covid and Post COVID Response (How rapidly transformation occurred and security implications of choices required to establish or maintain continuity)

*Image courtesy of NIST ICS*

# Future Work

Future work should include on and off-premise continuous stateful monitoring of ICS systems and should be managed through the use of digital certificates issued by a trusted certificate authority for security using multi-factor authentication – prohibiting the use of legacy username and password combinations and requiring the use of smart cards or other biometric credentials that uniquely identify an individual responsible for configuring and using the assets within ICS environments. This will allow for certificate revocation of compromised devices and users that transmit data and information within critical ICS systems.