White Paper

Building Secure IoT Endpoints and Edge Compute Architecture in Operations Technology Deployments

Sponsored by: Intel

Bill Rojas Hugh Ujhazy Emilie Ditton
December 2020

EXECUTIVE SUMMARY

The integration of IT and operations technology (OT) systems will mean the application of IT-related technology into OT architectures and capabilities. Such a change drives new investment requirements across industrial companies.

According to IDC's IT/OT Convergence and OT Security survey in May 2020, the top barriers to IT/OT integration for manufacturers globally are security, manageability, legacy applications, and lack of skills or expertise. Within the transformation, cloud is a fundamental required enabler despite industrial companies being cautious in the utilization of cloud to operational applications.

The requirement for trusted network security or provision of a chain of trust, from the endpoint to the gateway, to the edge compute node, and to the private/public cloud servers, means that all hardware and software must be founded in a root of trust. Trust can only be achieved if every key hardware, software, and firmware element participates in a chain of trust that follows the end-to-end data path — at rest, in execution, and in flight.

In this White Paper, we take a closer look at the key elements needed to build and manage a secure industrial Internet of Things (IIoT) network comprising intelligent endpoint devices (gateways, controllers, edge compute nodes) and the CPU chips/cores as well as hardware trust elements needed to construct trusted embedded intelligent systems.

We also discuss the challenges and digital frameworks that are being developed for utilities and manufacturing industries.

1. MAKING THE EDGE INFRASTRUCTURE SECURE

IDC decomposes edge infrastructure into four edges: enterprise, telco, operations, and endpoint device edge (see Figure 1).

Today, **enterprise edge** includes content distribution network (CDN) as well as storage and compute servers that might be sitting in a remote branch.

The **operations edge** is typically found in manufacturing, construction, energy, resources, transportation, retail, and Smart City.

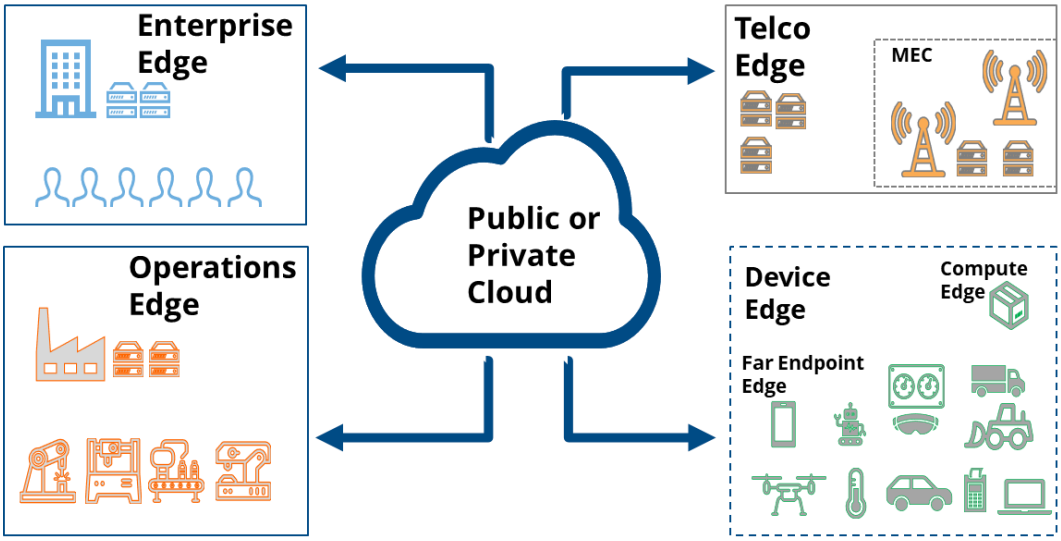
The **endpoint device edge** includes the far edge and the compute edge. The far edge are the sensors and actuators that transmit sensor data and receive control commands from the operations cloud, while the compute edge typically comprises secure concentrator gateways that collect data from sensors and transmit the aggregated data in a secure fashion via the telco network to the OT cloud. The OT cloud will comprise an Internet of Things (IoT) platform, storage, general compute, and analytics that can span more than one physical datacenter and more than one cloud domain (multi-cloud).

Finally, the **telco edge** includes the cellular radio access network (RAN), IP and optical aggregation sites, regional and central datacenters, and mobile edge computing hosts.

According to the IDC FutureScape: Worldwide IoT 2020 Predictions, 70% of enterprises will run varying levels of data processing at the IoT edge by 2023. While IDC FutureScape: Worldwide IT/OT Convergence 2020 Predictions states a 10% improvement in asset utilization will be enabled by a 50% increase in new industrial assets having some form of artificial intelligence (AI) deployed on edge devices by 2022.

FIGURE 1

The Four Major Types of Edge Infrastructure



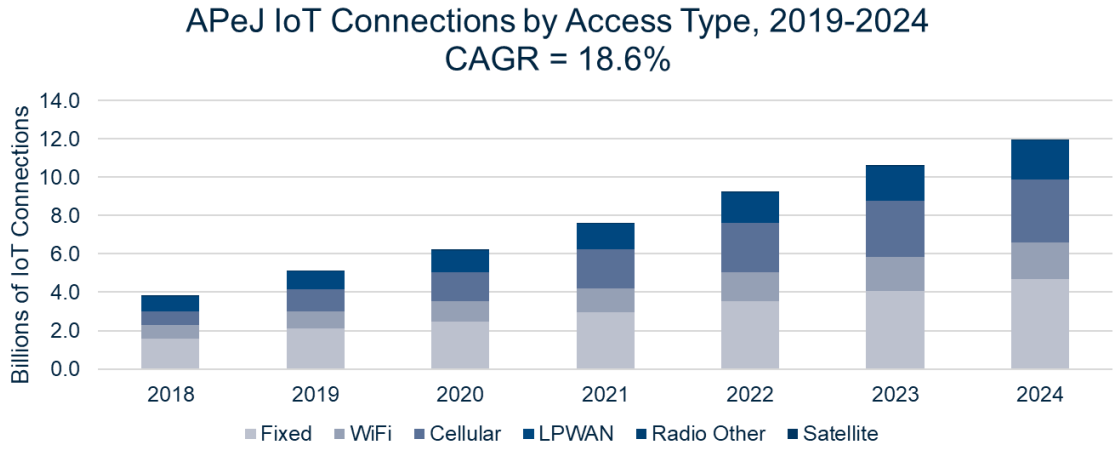
Source: IDC Directions 2020: Edge Strategies

IDC forecasts that a number of IoT connections will grow at double-digit growth rates of 18.6% from 2019-2024. To handle this growth, IoT onboarding, management, and the overall authentication life cycles will all need to automate significantly in order to scale.

Scaling of onboarding devices in the edge can only be efficiently and effectively implemented with a plug-and-play approach.

FIGURE 2

IDC's IoT Connections Forecast for APeJ, 2019-2024



Source: IDC APeJ IoT Access Model, 2020

The Operations Technology Edge

The high-level challenges of managing IoT endpoint devices in the IIoT include:

- Lower cost of managing the growing number of IoT devices
- Ease of management and security updates of IoT devices in hard to reach places
- Optimize productivity and driving efficiency by reducing IoT device downtime
- Protect IoT devices with security updates proactively

Figure 3 shows a general topology diagram of how a typical industrial company utilizes both wireless and fixed telco network infrastructure to connect endpoints, gateways, and edge compute nodes to the OT cloud and to each other.

The path for end-to-end data flow to the OT cloud involves collecting data from sensors, aggregating multiple streams of data, and securely transmitting it to/from the OT cloud platform and edge nodes. The role of the concentrator/gateway (referred to hereafter as "the gateway") is critical in terms of managing the data flow and transport as well as managing and implementing secure end-to-end transport.

For discrete and processing manufacturing factories, machine tools and production equipment will be increasingly connected wirelessly with Wi-Fi or cellular LTE/5G (indoor and outdoor). In other cases, the real-time raw data is fed to the cloud and in other cases an edge compute server in the factory premises will pre-process information before uploading to the OT's cloud network.

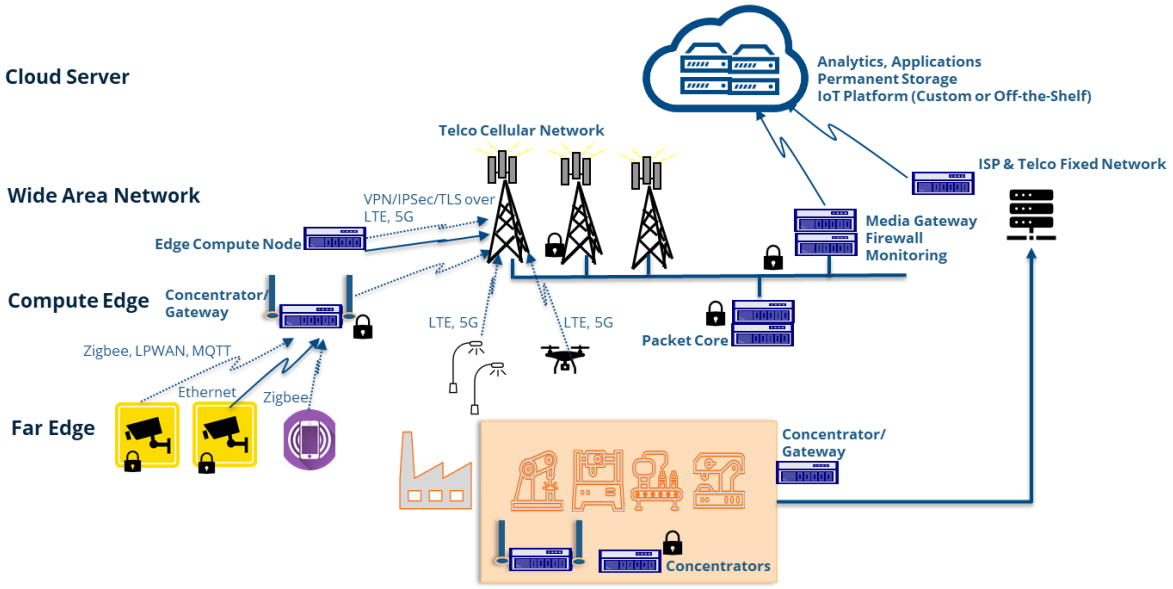
The edge compute node comprises server compute and storage capacity. Depending on the use case, the storage may be temporary or it could be longer term. In the past several years, different industries have examined the introduction of cloud technologies to replace parts of the traditional legacy infrastructure devices such as programmable logic controllers (PLC) and supervisory control and data acquisition (SCADA) equipment in industrial segments. However, this is a trend that will take time.

In all scenarios studied and developed by specific industries, the role of security and secure communications from the endpoint to the OT cloud has never been in question.

The rest of this paper addresses the different security requirements and best practices needed to implement IIoT in the industrial setting.

FIGURE 3

Typical Operations Technology Remote IoT Network Topology



Source: IDC, 2020

Edge-to-Cloud Aggregation

The challenge for industrial companies is to achieve mutual assurance between the cloud server and the endpoint device that both are what they say they are and that they have not been compromised.

There are a number of IoT and edge platforms for this purpose. Many of the solutions started out as "cloud" aggregation solutions but are rapidly evolving to include a distributed edge component.

Cloud vendors such as AWS, Google, IBM/Redhat and Microsoft are building platforms and actively working with telcos and industrial companies to develop OT edge connectivity. IT vendors such as VMware, Dell, HPE, Hitachi, Fujitsu and others are actively working with both telcos and industrial companies to introduce cloud-native technologies into the factory floor.

Software-defined networking and automated orchestration can be used to better secure the OT sub-networks at the edge devices.

Operations Technology and Industrial Internet of Things Ecosystem

Industrial companies have started the long journey of integrating heterogeneous IT and OT systems as part of their Industry 4.0 and digital transformation (DX). The relevant vendor community includes network equipment providers, IT hardware makers, system integrators (SIs), and software vendors.

The OT IIoT ecosystem is moving into this space and are exploring ways to converge these systems to mimic the legacy functionality of SCADA systems. The workhorse of the software stack of OT is still the PLC which (not surprisingly) was never intended or designed to deal with cybersecurity in a hyperconnected world. While the focus of this White Paper is to endpoint security and protection, we should mention that inputs do get corrupted or compromised despite the best of efforts. Sensor fusion techniques or parallel systems can be used to determine valid edge input and can highlight address level of checks for operating mission-critical systems.

IT companies such as Dell EMC, HPE, Oracle, VMware and others are looking at edge computing as a practical way to realize IT/OT integration and move industrial companies off the legacy SCADA and PLCs. The IT vendor community is wrestling with a number of IT/OT challenges including congestion or traffic management, latency, reliability and redundancy, and analytics.

In a recent IDC IT/OT Convergence Survey of 1,014 companies, 32.5% of companies said security concerns is the primary motivation for the use of edge computing, followed by 24.7% system resiliency and reliability, 19.7% deployment of analytics models, and 19.6% minimization of latency withing the industrial network (Source: *The Blurred Lines at the Edge of IoT*, IDC#US46826120, September 2020).

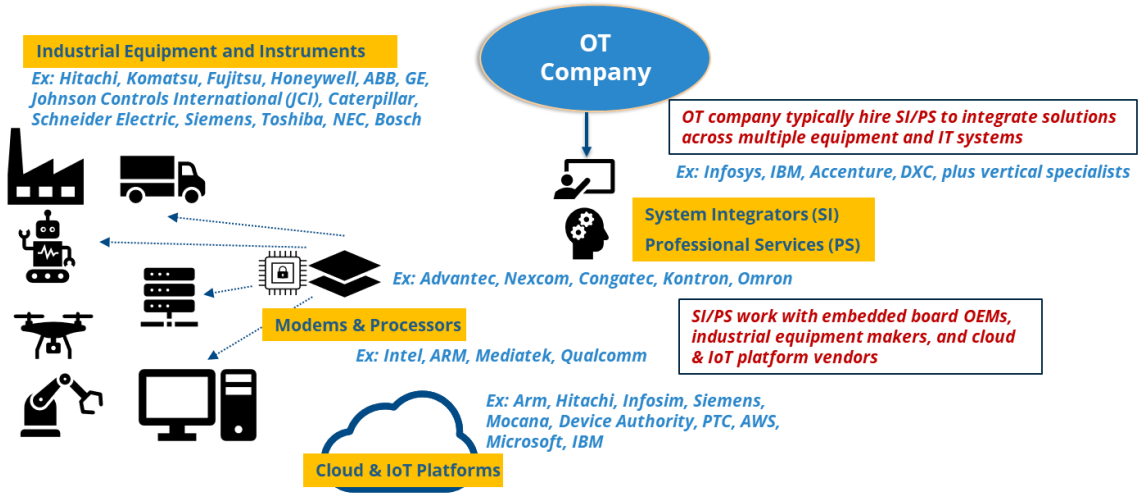
Figure 4 provides an overview of the ecosystem of software, hardware, and cloud vendors that typically are involved in IIoT. The industrial equipment and instruments companies produce equipment such as industrial-grade sensors, automated guided vehicles (AGV), autonomous trucks (for mining), trains with autonomous control, automated drilling equipment, digging equipment, phase measurement units (PMUs), and a wide range of SCADA systems, remote terminal units, and Human Interface/Control panels.

Each of these systems contain embedded boards and modules and require various types connectivity access such as an Ethernet port, fiber port, Wi-Fi modem, LTE and 5G modems or, in remote scenarios, a satellite modem.

There is a broad and robust ecosystem of suppliers of these boards and modules. Oftentimes, the large industrial companies will procure these in big quantities to use for different types of applications.

FIGURE 4

Ecosystem of IoT Solutions Providers for Operation Technology



Source: IDC, 2020

2. ENDPOINT SECURITY ATTRIBUTES AND BEST PRACTICES

Over the past few years, there have been a number of notorious endpoint device hacks. Table 1 summarizes the top 8 threats and four categories of vulnerabilities.

TABLE 1

Threats and Vulnerabilities

Threats	Types of Vulnerabilities			
	Data transport	Life cycle	Software	Physical hardware
Sensitive data protection	X	X	X	X
Credential/Provisioning	X	X	X	X
Escalation of privilege/ransom	X		X	X
Insecure key storage			X	X
Insecure data-in-flight	X		X	
Unsigned firmware/rootkit		X	X	X
Unauthorized basic input/output system (BIOS) write		X	X	X

Threats	Types of Vulnerabilities			
Hardware limitations				X

Source: IDC, 2020

Key Device Attack Surfaces

Table 2 provides a summary of the different attack surfaces and how security attributes can help address these vulnerabilities.

Firmware upgrade is a serious challenge for OT networks. For example, the automobile industry is racing toward realizing the vision of connected cars and autonomous vehicles. With hundreds of embedded controllers in a typical car today, it is not surprising that software and firmware upgrade constitute a serious challenge and require redundancy.

TABLE 2

Security Features Mapped Against Attack Surfaces

Security attributes	Effectiveness against these attack surfaces			
	Code modification	Key compromise	Password compromise	Man-in-the-middle
Anti-tamper	X			X
Temperature/Voltage protections	X			
Software integrity	X	X		
Data-at-rest and data-in-flight		X		X
Firmware upgrade/life-cycle management	X	X	X	X
Device cloud attestation and mutual authentication		X	X	X
User authentication and permission		X	X	X

Source: IDC, 2020

Edge Nodes (Gateway) — Containers and Encryption

IDC believes gateways could augment the baseline security of endpoints. Thus, the design of the gateway from both a hardware and software architecture perspective are critical to the success of the secure IIoT.

The OT will need to choose the security features that it must have in all CPUs and communications processors that are used to build gateways. Apart from the hardware security functionality, the software architecture of the gateway will also be strategic and will impact provisioning, firmware updates, and automated operations and management.

IDC believes the best way forward is for industrial companies to consider a mix of hypervisors and containers since real-time response or control are crucial. Moreover, the gateways may also be used as edge compute nodes which means that a common software stack would need to support bot containerization and hypervisors.

The OT will also need to decide on an encryption policy. Currently, IDC observes that more and more IIoT field applications are requiring AES-256 bit encryption to secure data streams from endpoints in the field. Wireless SD-WAN manufacturers, for example, have been offering AES-256 bit encryption in small form factors for mobility applications such as police motorcycle cameras, disaster response, and mobile video surveillance.

TABLE 3

Data Path Considerations

Data path	Security considerations and actions
Gateway-to-gateway	Strong encryption such as AES-256
Gateway/Edge node container and VM	Workload integrity, workload encryption, and workload partitioning
Gateway-to-edge compute node	Strong encryption, geotagging, authentication, and firewall and intrusion detection
Gateway-to-OT cloud	Audit of compliance, geotagging, and authentication
Gateway/Edge node-to-management and monitoring (on-premise or in cloud)	Encryption, geotagging, and workload integrity (server side), authentication and some form of non-repudiation control

Source: IDC, 2020

Edge to Cloud Connectivity — Audit Compliance

The edge (gateways and edge compute nodes) to cloud(s) connectivity must be secured and the integrity of the edge and cloud platform (BIOS, OS, hypervisor) must be verified against a known good state or whitelist at boot time.

Intel has developed a software suite called Intel Cloud Integrity Technology that is delivered as an Open Source via OpenStack or integrated into policy and compliance products (e.g., Hy Trust Cloud), which addresses this challenge by helping to create logical groupings (pools) of trusted systems isolating them from untrusted systems.

Compliance is an important issue for industrial companies especially those that operate in multiple jurisdictions. There are a number of government organizations and industry associations developing standards and auditing compliance with those standards. As a result, if the industrial company is using a cloud provider's infrastructure, compliance and audit will be important to manage.

Some of the issues arising from cloud audits (both public and private cloud) include the following:

- Is the provisioned infrastructure trusted or verified?
- Are the servers located where they say they are? This requires geotagging.
- What about data sovereignty requirements?
- How to prove compliance to industry bodies and national regulators

Automated Provisioning — Scalable Onboarding, Management and Retirement

The challenge in provisioning an IIoT network infrastructure then becomes how to secure endpoints and carry out a protected onboarding of IoT intelligent devices (including the gateways) throughout the life cycle of the devices.

In a typical OT operation (which could be local or across regional and global sites), there could be hundreds or even thousands of embedded controllers in machines, robotics, vehicles, and sensors.

A portion of these embedded boards and chipset modules will be involved in IoT processes collecting and transmitting data to cloud servers. Some IoT devices will also be actuators that would be controlled by edge servers or cloud applications and this would usually be done in real time.

Most large industrial companies procure intelligent embedded boards/modules from suppliers specializing in embedded board/module design. For example, the boards would be built with ARM-based, Intel processors, or others. The basic embedded boards with connectivity, compute, and storage capability can be custom built to order in large volumes.

However, without a flexible onboarding processes the embedded board makers will need to prepare separate SKUs for each customer because the cloud URLs need to be included at the time of manufacture. Intel has developed a solution called Secure Device Onboard (SDO) which solves this problem by enabling late binding (see Figure 5). Late binding is one of feature of SDO; SDO also allows complete provisioning of system at deployment time. OEMs can ship the system with bare minimum and at the time of deployment, after the secure verification of device in field platform can be provisioned and loaded with latest SW.

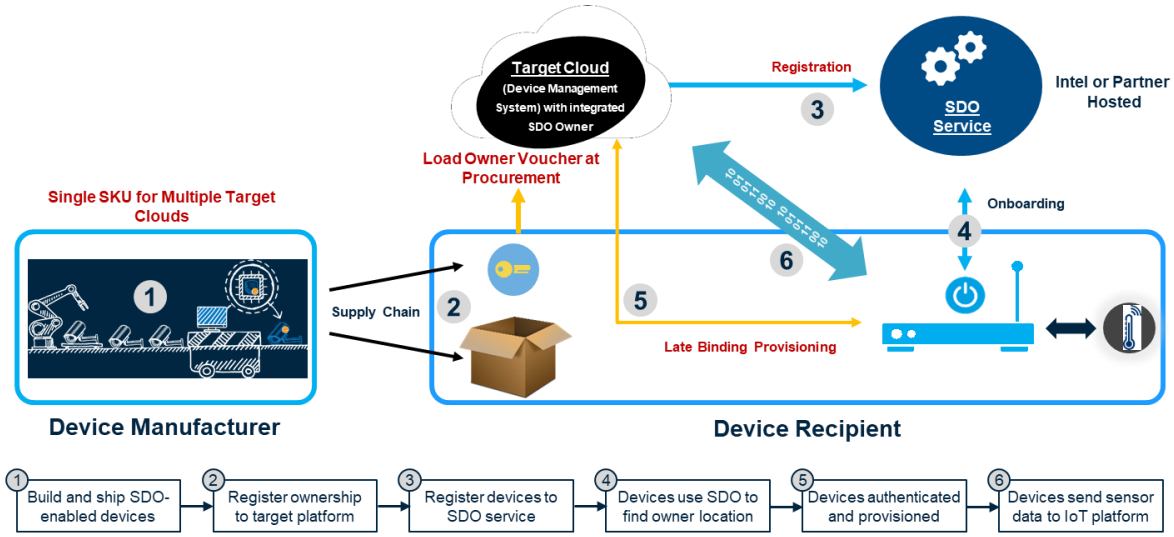
Intel and ARM have teamed up to establish SDO as an industry standard that helps to expand the ecosystem of partners. The Intel platforms with Trusted Execution Technology (TXT) [Xeon, Core, Atom] will support SDO Agent while a generic C-Software Development Kit (C-SDK) Agent is used for ARM processors. This is a major development for the embedded board/module industry because it means that manufacturers will be able to enable late binding and reduce the number of SKUs and the associated costs.

The OEM manufacturer will then use a Credential Tool to bind the ARM or Intel-based processor generating a certificate. Then, the certificate is authenticated via a Rendezvous Server running in the cloud or at the customer premise.

The use of the Rendezvous Server means that late binding becomes possible when the device is activated, then the binding to the correct target cloud/server address is performed and not at the time of manufacturer.

FIGURE 5

Provisioning with Intel's Secure Device Onboard



Source: Intel, 2020

There are several other standard groups that are relevant. One of them is Fast IDentity Online (FIDO) Alliance which is an open-industry association launched in February 2013 and has the mission of developing and promoting authentication standards that help reduce the world's over-reliance on passwords.

FIDO addresses the lack of interoperability among strong authentication devices and reduces the problems that users face in creating and remembering multiple usernames and passwords. Founding members were Agnittio, Infineon, Lenovo, Nok Labs, PayPal, and Validity Sensors. By 2016, there were 260 members including Apple, Samsung, Intel, IBM, Gemalto, ARM, Broadcom, NXP Semiconductors, and Qualcomm.

In June 2019, the FIDO Alliance announced that it was setting up an IoT Working Group (WG) with members including Intel, ARM, major CSPs, and others. The password replacement goal in internet applications is very similar to the challenges in IoT authentication.

Intel SDO is a foundational component of the FIDO Alliance standards.

3. A DIGITAL FRAMEWORK FOR OT VIA TRUSTED IOT ENDPOINTS

It is imperative that the IIoT operations can trust the data from endpoints as it gets aggregated in gateways and post-processed in edge compute nodes and then gets transported through the telco network out to multiple OT cloud domains.

In order for that process to be realized, all processes have to be part of a chain of trust starting with securing the intelligent endpoints, the links between the edge gateways and edge compute nodes must be secure using strong encryption.

It should be pointed out that while broadband fixed and cellular networks are fairly secure, there is always going to be the danger, however miniscule, that the data payload can be intercepted and that is the reason for the need that all data streams to servers and the cloud are encrypted. Moreover, it is important that the OT cloud can verify and authenticate the source of the data (i.e., gateway).

Recently, traffic congestion has become an increasing problem in IIoT networks and, as such, IDC believes that software-defined network (SDN) and SD-WAN technology embedded in the gateway edge would be the most effective way to automate traffic management.

There are seven key steps and guidelines needed to implement a secure IIoT framework, as follows:

1. Establish a secure device system architecture

All intelligent devices must utilize company approved root-of-trust hardware that would be specified when ordering embedded board solutions. Before the industrial company designs the embedded board specifications, it must choose a topology that provides redundancy and alternative paths to the cloud. Moreover, all CPU and communications controllers (Wi-Fi, ethernet and fiber interface ports, LTE, 5G modems) should be required to be built with Trusted Execution Environment (TEE) enabled. The OT will need to select a secure OS for the Secure World software and this would have to become a companywide standard. Intel offers Software Guard Extension (SGX) as a solution for the TEE for embedded applications.

Flexibility across different CPU makers. It is recommended to give SIs and OEMs/Original Device Manufacturer (ODMs) flexibility in choosing CPU makers, but it is imperative that the secure boot, root of trust, and boot loader policies be strictly adhere to.

2. Implement life-cycle management

a. **Enable fast, secure, and automated device provisioning.** This is zero-touch onboarding services that will take seconds at power on. Intel's SDO has been open sourced and utilizes unique privacy preserving hardware security model.

b. **Utilize open software APIs/standards for provisioning.** The benefit of Open APIs is that SIs will be able to deliver solutions better tailored to the IT needs of the OT.

c. **Create a device registry.** Based on our understanding of the current state of technology, most industrial companies do not have an online inventory of every embedded board in use. IDC believes that as a practical approach all embedded boards that interact with the corporate IIoT intranet would need to be registered in a device database, which would also maintain device security attributes and policies. This way, if a security vulnerability was discovered in the future, the OT engineering team would be able to identify which boards are exposed and take appropriate action. As a best practice, it is also important to keep a repository of all major Voucher Certificates used for onboarding.

d. **Establish a plan and policy for retrofitting of intelligent endpoints.** Most industrial companies have legacy PLCs, SCADA, and gateways with embedded boards that do not provide hardware-based trust. Although it is not an easy process, the industrial company will need to develop a migration and transition roadmap for gateways and edge compute nodes to be equipped with the required corporate security hardware and software.

3. Lay out a roadmap to cloud-native architecture

a. **Utilize a cloud-native software stack.** While more OT analytics and some management platforms run in the cloud, either private or public, most of these implementations have not been built with cloud-native concepts such as containers and SDN. IDC believes that implementing a secure IIoT network requires that the back-end software stack is secure and scalable. In a containerized architecture, it will be possible to provide additional level of security at the container level. IDC believes that containerizing the gateways and edge compute node is also in the long-term benefit of the OT so that a common SDN and orchestration architecture can be used for all software containers. However, it should also be pointed out that container deployments will be challenged to deliver real-time response and control.

b. **Incorporate SDN (for gateways and edge compute resources).** If SDN is incorporated in the gateway and edge compute node devices, it should be easier to automate the firmware update as a secure process similar to the way that vRAN is updated via Ethernet switches and SDN. IDC recommends that the industrial companies carry out periodic authentications of gateways and edge compute nodes using SDN.

4. Enhance the OT cloud and edge-to-cloud architecture

a. **Utilize trusted compute pools, resiliency, and multiple cloud instances.** It is important in virtualized and cloud environments that all of the underlying software modules are trusted, starting first with the hypervisor. Servers used in the cloud datacenter must have similar trust features including TEE and Trusted Platform Module (TPM) to ensure that the hardware can be reliable. If the software stack is implemented with containers, it will be imperative to build trusted compute pools. The OT team must also carry out audits of the important features of any public cloud system that is utilized. It is this dilemma that has made industrial companies slow to adopt public cloud for operations functions that are currently being done with PLCs and SCADA.

b. **Architect for network redundancy.** The ability for gateways to connect to the OT cloud via fixed and wireless links means that wireless can be used to provide better network resiliency. Also, wireless access is deployed in scenarios where digging up infrastructure is not practical or too costly. Another type of redundancy results from the containerization of gateways and edge compute nodes. The possibility of utilizing TEE secure mode to run real-time monitoring of critical links in the network is more intriguing. TEE can also be used to execute simulations for testing purposes.

c. **Support many-cloud (multiple providers).** Whether it is onboarding or analytics, the secure onboarding and other life-cycle functions can support multi-public environments. But we reiterate the importance of ensuring the server hardware meets the level of security audit from the server to the OS and hypervisor so that a chain of trust can be maintained.

5. Utilize AI and analytics in the cloud and edge cloud stacks

The software stack includes long-term data archiving and data analytics and when combined with analytics software. It will be possible to run analysis of near real-time data as well as archived data. Most OTs would utilize a mix of analytics tools including video and image analytics.

6. Automate security testing and simulation

The industrial company IIoT and OT cloud will always be undergoing changes and improvements, upgrades, and even migrations. All of these further open the door to vulnerabilities. Typically, industrial companies have an ecosystem of engineering services, construction, maintenance, and equipment contractors accessing applications – one of the biggest security vulnerabilities lie in managing the access rights and monitoring the access.

A new approach that is gaining interest in IT circles is the breach of attack simulation (BAS). Although this is a relatively new space, there is a lot to be said for the concept of automated software that runs in the background searching for security breaches, posing as fake gateways, and so on – taking validation to the next level beyond periodic authentication.

7. Expand the operations manageability framework

The manageability framework is a critical part of operating and maintaining an IIoT network as it scales and expands. The framework must also enable ecosystem partners to connect to any cloud of their choice. There are two basic scenarios for managing the endpoints in the edge. The first is a cloud-based end-to-end remote manageability model that provides dashboard and remote management of the user interface or console. The second is the on-premise end-to-end remote manageability model. A dashboard would also be used in this scenario but it would be connected to on-premise infrastructure.

a. **Support out of band management (OOB).** This includes system monitoring and control, software updates security patching, inventory management, troubleshooting and remediation, and retirement and de-commissioning. Intel's Active Management Technology (AMT) enables remote power control, remote BIOS access, hardware KVN, hardware alarm clock and alerting, and third-party data store.

b. **Implement an in-band manageability framework.** This includes Firmware over the Air (FOTA) and Software over the Air (SOTA) for a single system or multiple systems across every work site. Other features that would fall under this framework include TPM 2.0 base key and secret management, Secure MQTT with TLS, Access Control Lists (ACL) and end-to-end mutual authentication, and package signature verification.

OOB and in-band are available in remote or on-premise scenarios, OOB allows the admin to manage devices even when OS/VMM/BIOS is non-responsive. In-band requires BIOS/OS/VMM to remain active.

4. SECURING THE OPERATIONS TECNOLOGY EDGE WITH TRUSTED ENDPOINTS

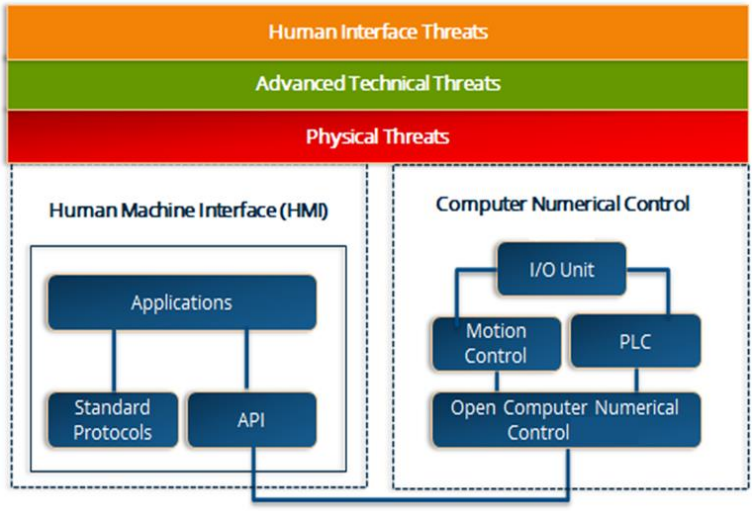
Smart Manufacturing

In May 2020, IDC Worldwide Semiannual IoT Spending Guide forecasts that global IoT spending in manufacturing (process and discrete) will grow 10.8% compound annual growth rate (CAGR) between 2020-2024 to reach US$289.7 billion. Manufacturing operations and production asset management will account for the largest portion of IoT spending in manufacturing as Industry 4.0-related initiatives continue to be the greatest driver for IIoT within manufacturing. Data-led intelligence, insight, and automation across manufacturing operations and supply chains will be required to enable increasing customization, personalization, and resilience.

Until recently, one area that has not received as much attention than it should is endpoint security in production computer numerical controlled (CNC) machinery monitoring. In order to enable CNC machine tools to participate in an IIoT process, they have to be retrofitted with diagnostic services and supplemented with additional sensors for both direct and indirect monitoring. In a factory that has hundreds or more CNC machine, tools connecting them into the factory WLAN introduces a new level of additional security and integrity risks. What makes the factory floor challenging in terms of security management is that most of the functionality in production environments is delivered by OT at the physical edge, which means that the endpoint security is the area that must be particularly fortified (i.e., the London casino fish tank hack). Figure 6 provides a simplified view of the security threats in production machinery monitoring. Manufacturing systems must preserve their physical and functional integrity and must use the available industry's best practice solutions for trust, identity, access control, and data protection mechanisms. Many clever techniques have been developed including cloning of tags, signal replaying, distributed denial of service (DDoS), worms (Stuxnet nuclear facility attack), and IoT device reverse engineering to allow attackers to gain access to critical data, services, and facilities; and in some cases, carry out data tampering. In the past, many of the countermeasures described in section 3 have not been deployed in production machinery monitoring due to resource constraints or other reasons. More advanced factory systems are combining IoT with SCADA and these also introduce new threats.

FIGURE 6

Diagrammatic View of Threats for Legacy Production Machinery Monitoring



Source: Cranfield University et al. *Sensors*, p. 2355, 2019

Smart Electric Grid

In May 2020, IDC forecasts that global IoT spending in utilities will grow 9.5% CAGR during the same period to reach $90.8 billion. Smart electric grid and smart gas distribution will account for the largest market size in IoT in utilities. Figure 7 provides a summary of the smart grid services which can utilize energy-oriented IoT processes (EIoT). The smart grid can be viewed as an evolution of the electricity distribution network to dynamically integrate the generation, distribution, and consumption of electricity.

The goal of smart grid is to economically and efficiently deliver sustainable, reliable, safe, and secure electricity supply to businesses, industry, and residences. The adoption of IoT processes is designed to automate the collection of data from devices (i.e., PMU, transformers, and smart meters) to dynamically manage the entire network in real time.

Smart grids will typically make use of multiple communications access technologies including Sigfox, LoRa, 3G/4G/5G cellular, Low Earth Orbit (LEO) satellites and fiber optic transmission. Wireless communications for the smart grid and micro-grid are a relatively new area that is receiving an increasing attention especially with the advent of the wide coverage of 4G LTE, the introduction of multi-access edge computing (MEC) and 5G networks. Another area where 4G/5G can play a role in smart grids is in the aggregation data from micro-grids such as building integrated photovoltaics (BIPV), rooftop photovoltaics, home battery energy storage, electric vehicle charging stations, and individual wind turbines and wind turbine farms. **Micro-grids** are essentially islands of consumers or a generating facility supplying a group of consumers that generate electricity and sell to the electricity companies or to other micro-grid members that will also benefit from the rapid deployment capabilities of multi-link WAN and cellular bonding.

Figure 7 depicts a typical intelligent power control system that shows an energy management system (EMS), which monitors and controls the whole power system safely and securely. The SCADA systems collect operational information and transfers this data between a constellation of Remote Terminal Units (RTUs) and/or PLCs to a centralized datacenter which may be in the private cloud or on a public cloud. The SCADA system transfers data. SCADA systems typically use several protocols including various International Electrotechnical Commission (EIC) standards, which address the data link and physical layers for application control, and Distributed Network Protocol 3 (DNP3). In the United States, the Energy Independence and Security Act of 2007 granted the responsibility of smart grid standards and guidelines to the Federal Energy Regulatory Commission (FERC) and the National Institute of Standards and Technology (NIST). The guidelines stipulate that the smart grid:

- Must be cybersecure
- Must be a national integrated grid with more than one command and control center, and not just local/regional
- Must manage distributed energy from solar and wind and store ad manage net metering and the production of renewable sources
- Must manage loads at the plug level
- Must be resilient and redundant rerouting and transmission in real time

The regional control center (RCC) SCADA operates the regional power systems, and the substation control center (SCC) provides the local feeder branch data. The role of the RTUs is to transfer status and information at remote sites to the central control system. The substation automation (SA) system controls the power system using data acquired through the Intelligent Electronic Devices (IEDs). In order to understand the important of a chain of trust in the power network, we only have to look at the five main communications links in the control system: EMS-RTU, EMS-SCADA, SCADA-SCADA, SCADA-SA and SA internal. DNP3 is used for most of those links.

Apart from the transmission systems, we note that many electricity companies are now looking at integrating their transmission SCADA systems with their Outage Management Systems (OMA) and Distribution Management Systems (DMS). A part of the reason for this trend is that in recent years OMA has become more automated and more integrated with Geographic Information Systems (GIS), Customer Information Systems (CIS), Work Management Systems (WMS), Mobile Workforce

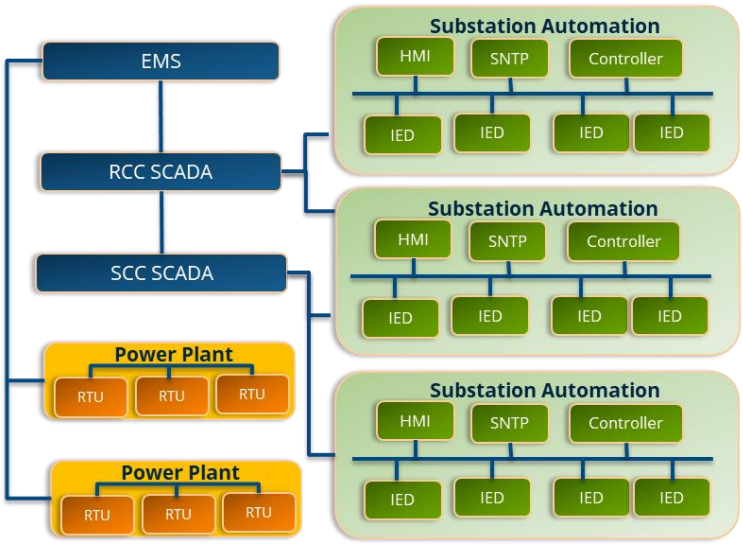
Management (MWM), SCADA, and Advanced Metering Infrastructure (AMI). Outage prediction is thus becoming more automated by using readings from AMI trouble orders, and SCADA RTU readings.

Cybersecurity in the power network is clearly of utmost and critical importance. The industry has studied various security vulnerabilities in power networks including DDos and data modification (such as data injection and command injection) of IoT devices particularly those that are connected via wireless access. The electricity industry has experienced a wide range of attacks on SCADA and PLC and is looking at using AI analytics and Intrusion Detection Systems (IDS) to determine network traffic that does not follow normal patterns of burst frequency, size, and noise.

The basic framework described in section 3 applies to the power control networks but every intelligent device such as RTUs including PLCs and SCADA and gateways must be built on a root of trust and encryption must be deployed throughout all major control links EMS-RTU, SCADA-SCADA, and SCADA-SA.

FIGURE 7

Topology of Typical Intelligent Power Control Systems



RTU = Remote Terminal Unit
EMS = Energy Management System
SCC = Substation Control Center

IED = Intelligent Electronic Device
HMI = Human-Machine Interface

Source: Mobile Network Applications, April 2018

5.CONCLUSION

Industrial company in OT must integrate security as an end-to-end solution with controls at each level – smart endpoints, gateways, edge compute nodes, edge-to-cloud connectivity, and cloud platforms which includes AI and analytics software. Industry 4.0 and DX is a journey that will necessarily require trusted pools of systems but eventually will need to secure all intelligent devices. Cloud-native technology will take time to assimilated in OT and proof of concepts (PoCs) will need to take place before commissioning live containerized cloud-enabled platforms.

Endpoint security begins with securing the hardware through Trusted Execution Environment (TEE) and Trusted Platform Module, and by using software such as SDO that is based on TEE primitives. Traditional intrusion detection systems (IDS) and intrusion prevention systems (IPS) are still needed but it must be augmented with automated security testing and simulations. The attack surface will not shrink at OT but will continue to expand, and this is the reason that a well-thought-out endpoint security framework is necessary to ensure the integrity, reliability, and availability of OT systems across a wide range of industries and tasks including energy generation, transmission and distribution, and manufacturing production logistics.

6. ESSENTIAL GUIDANCE FOR OPERATIONS TECHNOLOGY SYSTEM INTEGRATORS

SIs will typically fall into one of two categories of responsibilities when involved with industrial company OT and IIoT:

- **Responsible for total network architecture.** For SIs that are involved in affecting and implementing the total network topology and protocol architecture, the framework described above is a good guide to proceed in terms of network architecture, life-cycle management, manageability framework, edge server topology, and server/gateway to cloud.

  It is recommended that the SI work with the client's industrial company to formulate a roadmap to cloud-native technology which ultimately encompasses container management and security. By utilizing the open source Intel Cloud Integrity Technology, it will be possible to introduce over time virtual endpoint solutions that run as containers in the cloud or on edge servers.

  Automated security testing and BAS are critical to being able to operate and expand the network in a smooth manner as a way of continuous security fortification.

- **Responsible for some domains.** For SIs that are commissioned to provide networking and endpoint security for selected domains but not the entire network, it is recommended that the SI create logical groupings (pools) of trusted systems isolating them from untrusted systems.

  If the PLCs, SCADA, and RTUs do not have secure communications, the SI can look at encapsulation and tunneling to aggregate the upstream data flows through gateways that are trusted systems with TEE. In other words, unsecure devices should not be allowed to connect directly to the cloud platform and, instead, must all be routed through secure gateways.

  SIs can work with the client to test PoC of containerized and virtualized SCADA, PLCs, and RTUs. Hypervisors, container, and cloud-native technology (Kubernetes, Docker, Open Stack, etc.) are recommended as a way to implement the separation of trusted systems and untrusted systems.

  The path to the cloud needs to be secured but this might be challenging if other domains do not use the same edge-to-cloud solution. The industrial company will need to spell out the roadmap for the edge-to-cloud security.

  Life-cycle management and automated testing BAS are recommended for the domains for which the SI is responsible. Manageability framework needs to be integrated or interfaced with other manageability platforms that are being used in other domains.

Table 4 provides a how-to checklist for OTSIs:

TABLE 4

Checklist for Integrators

Focus Area	Consideration	Task	Importance/Timeframe
Device system architecture	Secure devices	Use embedded modules with CPUs that have Secure Boot (e.g., Intel Boot Guard) TEE (Intel TXT) and TPM as well as activated with SDO	Critical/Immediate
	Isolation	Isolate secure devices from those that are not secured into different physical edge/cloud network domains. This may include SCADA and PLC equipment that are unsecure but can be routed into gateways that are themselves secured	Critical/Immediate
	Redundancy	Choose a topology that provides redundancy between edge/compute nodes and the server cloud	Optional/Mid-term
		Engineer alternate paths to cloud	Optional/Mid-term
	Resilience	Ensure secure execution area onboard gateway or endpoints	Critical/Immediate
		Define architecture relationship between endpoints and gateways	High priority/Immediate
Life-cycle management	Device registry	Create a device registry that includes CPU/TEE, TPM, and other security attributes. Manageability using, for example, Intel's Active Management Technology (AMT) enables remote power control, remote BIOS access, hardware KVN, hardware alarm clock and alerting, and third-party data store	High priority/Immediate
	Automate device provisioning	Implement zero-touch onboarding with SDO	Critical/Immediate
	Develop plan for device retrofitting	For SCADA, PLC, and other embedded devices that need to be connected, develop a roadmap for either replacing the devices or routing their unsecure data streams into a gateway that encrypts the ingress flow into an encrypted data stream that is routed to the OT servers/cloud	Strategic/Mid-term

TABLE 4

Checklist for Integrators

Focus Area	Consideration	Task	Importance/Timeframe
Cloud-native migration/design	Incorporate SDN control for edge/compute nodes	Implement SDN control architecture for all gateways and edge nodes that connect to the server/cloud. The SDN controller can be on-premise or in the OT server/cloud	High priority/Immediate to mid-term
	Develop roadmap for introduction of containerization and cloud-native software stack	Containerization of increasingly important components can be migrated from current legacy systems but this will take time and needs to be a strategic direction of the OT company	Strategic/Mid- to long-term
Cloud architecture	Establish trusted compute pools	All virtualize/cloud environments must be trusted compute pools meaning that the underlying servers and cloud-enabling software including hypervisors are trusted	Critical/Immediate
		Audits need to be carried out on a regular basis to ensure that all datacenter and cloud servers are trusted entities	High priority/Mid-term

MESSAGE FROM THE SPONSOR

As IoT and edge technologies evolve, information, operational, and communications technology (IT/OT/CT) convergence becomes more complex.

At Intel, we're ready to take your business needs to collaborate in new ways to deliver the fully integrated stacks that customers need now. Open new doors when you access a vibrant ecosystem of vetted IoT technologies and partners, such as Intel® IoT Solution Aggregators who can help with solution sourcing and creation. Use your growing expertise to pump up your portfolio of IoT offerings and break the siloes separating IT and OT. Leverage vetted solution stacks and Intel® technology, expertise, and training to help your customers integrate new technologies into legacy infrastructure. Intel® IoT Market Ready Solutions and Intel® IoT RFP Ready Kits, along with Intel® IoT Solution Aggregators and other ecosystem partners, enable access to advanced use cases such as automation, edge compute, predictive maintenance, and more. The future is approaching fast, so don't miss out. Add the powerful dimension of Intel connections to sharpen your competitive advantage and thrive in IoT.

For more information, please go to www.intel.com/iot.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Asia/Pacific

80 Anson Road
#38-00 Fuji Xerox Tower
Singapore 079907
T: +65 6226 0330
Twitter @IDCAP
www.idc.com/ap