Trusted Cyber Physical Systems

A solution for tamperproof authorization and non-repudiable auditing to control and monitor actions on cyber physical systems

Version 2.0 (April 2018)

Stefan Thom, Principal Software Developer
Torsten Stein, Senior Program Manager
Dave Thaler, Partner Software Developer

For feedback and question about this document please contact Microsoft at tcps@microsoft.com.

1 Executive summary

Attacks against critical infrastructure, like the Triton breach of critical safety systems of an energy plant, have become more frequent globally. While the financial toll of cyber-attacks has become an unfortunate norm, attacks that can damage connected systems, and put human lives and property at risk are emerging with new regularity. This document describes how cyber-physical systems (CPSs)[1], also known as Internet-of-Things (IoT) in an industrial context, can be securely controlled, monitored, and audited throughout the IoT infrastructure, including cloud services, compute devices, and microcontrollers (MCUs[2]), down to the pins that provide power to, e.g., open and close a valve in a water plant. The key to this approach is that all actions and messages to and from a CPS device, all the way down to the hardware I/O pin, are cryptographically secured. Even if the OS on a cyber-physical system itself is compromised, an attacker will not be able to operate the valve nor tamper with the activity log of the valve. Furthermore, even the OS vendor or ISV cannot access private data nor send unauthorized commands or software updates. This will allow a clear separation between the authorized operators of solutions and the software vendors, hardware vendors and solution providers.

[1] https://en.wikipedia.org/wiki/Cyber-physical_system

[2] Micro Controller Units, https://en.wikipedia.org/wiki/Microcontroller

2 Introduction

The credit card industry is embedding a Secure Element (SE)[3] in credit cards. The change from magnetic strip to Secure Element to access the customers' card data is one of the recent efforts to address spoofing, theft, and tampering with customers' credit card information. The SE-based solution establishes an end-to-end (E2E) trusted connection between the content on the credit card and the credit card's processing center. This makes any other system in the path merely a facilitator of this action with no access to confidential information or the ability to clone a card or replay the messages.

As the Internet of Things is gaining more momentum with millions of devices connecting to each other and to the cloud, it presents challenges in securing those devices and services. The issues related to unauthorized access to control such devices is similar to access to information on credit cards. However, the consequences of misuse of IoT devices can have far more severe consequences as our lives can be negatively impacted, potentially including loss of life. Thus, IoT warrants a solution at least as secure as credit cards use today.

Imagine if the same type of secure access that is used for the information on credit cards were used to control IoT devices. Instead of cryptographically protecting financial activities, a cryptographic element would protect the I/O pins on the MCU that controls IoT devices. And as with the bank's processing center, IoT operators would have a secure end-to-end communication to the MCU's I/O pins that control the physical world.

[3] Secure Element (SE): https://www.globalplatform.org/mediaguideSE.asp

3 Background

Recent surveys done by Microsoft with partners in the industrial and consumer IoT spaces show that their number one concern is security, with focus on system and data access. These concerns are justified by recent widely-publicized attacks on consumer devices such as cars[4] as well as manufacturing and infrastructure systems such as the uranium enrichment facility in Iran,[5] the Ukrainian power grid,[6] and other energy plants[7]. In comparison to attacks on data systems (e.g., credit cards[8]), attacks on cyber-physical systems (CPSs) can have a direct effect on our surroundings with potentially physically harmful and life-threatening consequences. Operators and providers of CPSs have negative financial and reputational impact on their business through these attacks.

The "air gap solution"

While most CPSs have security measures in place and even provide an "air gap" between the Internet and the local network in an attempt to protect their systems from unauthorized remote access, they often have insufficient measures against breaches due to devices carried into the secure environment (flash drives, personal phones, etc.), and still have no measures against breach of the transition point of the software command and the hardware pin that controls the physical system. Anyone with access to the PLC[9] or microcontroller, be this the system integrator or a hacker, can control the PLC to trigger actions or read data from it. IoT solution providers reported that trust just isn't there among customers that "someone else", including governments, cannot *potentially* access their information, so for many customers connecting outside of their on-premise solution is a big concern today.

Remote operation

Security is often even more important for CPSs than for more traditional computing systems, since interacting directly with the physical world can present greater dangers, and CPS devices often operate autonomously without any human interaction for a long-time period. When the CPS uses constrained devices, the problem is compounded by the fact that there are often fewer resources available to actually implement security.

---

[4] Nissan Leaf electric cars hack vulnerability disclosed

Hackers Remotely Kill a Jeep on the Highway

[5] Stuxnet computer virus

[6] Analysis of the Cyber Attack on the Ukrainian Power Grid

[7] Triton: Hackers take out safety systems in 'watershed' attack on energy plant

[8] Home Depot breach put 56 million payment cards at risk

[9] Programmable Logic Controller

Privacy

Privacy is another key concern, especially for CPSs that have access to personal information (e.g., in the health care industry), or are associated with a company's intellectual property (e.g., trade secrets, or systems designed to prevent industrial espionage), or a nation's defense industry (e.g., companies with defense contracts). Where such data is stored is important, e.g., due to laws requiring data to stay within national boundaries so that it is not subject to foreign subpoenas.

Operation

The picture below shows, at a high-level, how authorized access is enabled end-to-end.

Figure 1: High-level architecture

The actual details may vary depending on the use case. For example, many industrial environments look like the following today:

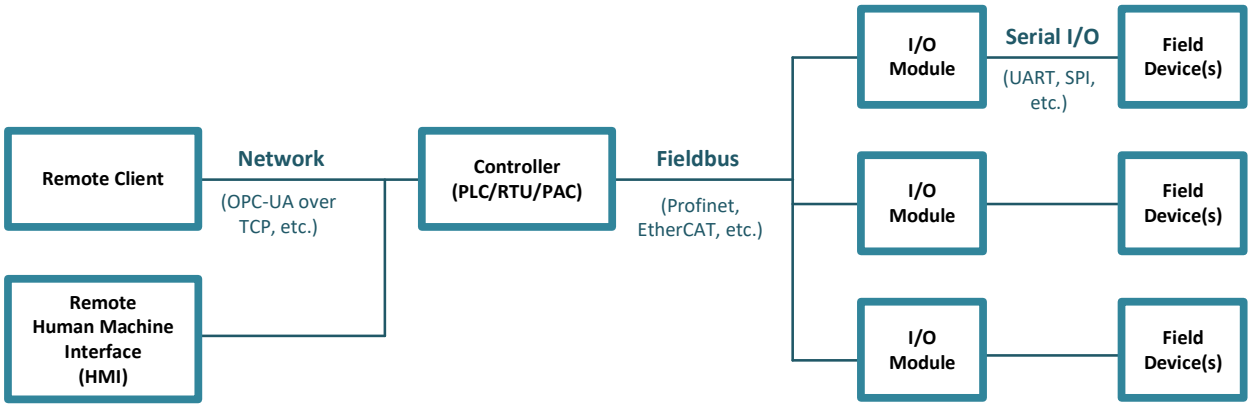


Figure 2: Sample industrial environment

Trusted Cyber Physical Systems

The key point of the high-level architecture is that devices that have access to unencrypted actuation commands or sensor data are most secure when they have a trusted execution environment, and any connection to devices that lack one but are instead physically secured are accessible only from within another device's trusted execution environment which can perform authorization. Authorization can also be delegated to an "edge compute" device (sometimes called a gateway, although as discussed below there are other roles as well) or even to the High Integrity CPS device (e.g., an I/O module). While the Operating System and applications running on it will facilitate passing commands back and forth, the authorization is always processed in a trusted execution environment (TEE)[10].

[10] https://en.wikipedia.org/wiki/Trusted_execution_environment

4 Example Customer Scenario

A utility company operates several water plants throughout the region. They remotely control and monitor their facilities, which provide drinking water to thousands of households, and may use automation and robotic controls as well. Providing a constant, high quality supply is essential for the region.

4.1 Customer challenge

A major concern for the company is that their facility might be compromised by unauthorized operations due to attacks against their cyber infrastructure. They have several measures in place to protect pieces of the system. But from recent industry attacks, they've learned that even systems on an isolated network can be compromised. These attacks are all targeted towards the PLCs that control the physical systems like their water valves and chemical systems.

4.2 Solving the customer's challenge

The utility company learned about the trusted cyber-physical systems solution. Their security review gave them confidence that any operation on the CPS device could only be authorized by their operation center, and they have the ability to securely delegate specific operations to trusted third parties as they need for their service crews. Furthermore, all operations are auditable events in tamperproof logs.

4.3 Customer benefit

The solution assures the integrity of control and monitoring for the CPS end-to-end. This is a key requirement for customers (CPS operators) to feel confident in mitigating the threats of unauthorized operation and tampering with operational data. They feel confident enough to lift their "air gap", which then allows them to more fully utilize the capabilities of IoT.

The TCPS solution will provide them with the following benefits:

- **Tamperproof authorization and non-repudiable auditing to control and monitor actions**
  - Neither a cloud service provider (e.g., Microsoft) nor a software provider will be able to execute actions on CPSs that are not authorized by the system operator
- **Data flow and storage throughout the infrastructure is integrity protected and encrypted, giving only entities authorized by the CPS operator access**
  - No system provider, cloud or on premise, will be able to decrypt, alter or replay any of the data processed without the CPS operator's explicit permission. Even if a subpoena, FISA order, etc., is given to the service providers they cannot give out the CPS's data since it is cryptographically protected.
- **Use of well proven industry standards provides transparency and trust in all security-related operations throughout the system**
  - There is no secret Microsoft sauce when it comes to security. Microsoft's advantage is in customer trust built up by security experience, end-to-end solutions, easy-to-use security policy management tools, and transparency of all trusted execution environment code, which allows independent verification by security analysts.

With the TCPS solution, the utility company management feels confident that cyber-attacks against their physical systems are significantly mitigated and that the data provided by their sensors will hold up to security audits. They can fulfill their responsibility of servicing the public with clean drinking water. They avoid bad headlines and potential law suits due to unauthorized operations. They can also improve their insurance and loss prevention costs[11].

The utility company can now also benefit from cost savings opportunities that their previous air-gapped approach wouldn't allow them to do. This includes scenarios that allow employees to work remotely or use their own devices (BYOD[12]), as well as scenarios using secure cloud resources rather than running their own internal datacenter.

Thus, potential benefits include, among others[13]:

- Tracking and auditing activity
- Data analytics
- Automation (e.g., autonomous rules)
- Fault detection
- Enhanced access control (e.g., time-of-day policies, immediate revocation, etc.)
- Loss prevention

[11] "10 Real-Life Examples of IoT in Insurance", https://internetofbusiness.com/10-examples-iot-insurance/; Insurance IoT Industry Survey 2017

[12] BYOD: Bring your own device, https://en.wikipedia.org/wiki/Bring_your_own_device

[13] See section 2.C of https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf for more details

5 TCPS Architecture

A TCPS solution covers the entire path end-to-end, including cloud services, edge compute devices, PLCs, etc.. Trusted Execution Environments in the cloud and in each device work in concert with secure protocols to enforce customer policy and protect the assets entrusted to it.

CPS operators can be assured that only they can authorize operations on the CPS, and that all data from the CPS is protected and meets regulatory compliance.

Key aspects of this approach include:

(1) using trusted execution environments at all points in the end-to-end path that need access to the data, including user devices, the cloud, PLC's, etc.,
(2) restricting access to the physical sensors and actuators to be *only* accessible from within a Trusted Execution Environment (TEE),
(3) keeping raw data accessible *only* from inside a trusted execution environment and only readable by the customer and those whom the customer explicitly authorizes,
(4) keeping the code inside the trusted execution environment as small as possible and having ways to vouch for its trustworthiness, and
(5) using tamperproof logging techniques to provide secure and non-repudiable auditing.

Performing actions on a CPS device, e.g., opening a water valve, will require a key to authenticate the action on the device and a policy that describes the usage of the key.

Data reported from the device will be signed with the identity of the device, and encrypted if this is required. This will ensure the integrity of the data throughout the IoT infrastructure.

5.1 Trusted Execution Environments (TEEs)

Some examples of TEEs include Secure Elements[14], SGX[15] enclaves, DICE-capable[16] MCUs, and TPMs[17]. Only signed and authorized code can run in a TEE. Key principles of TEE code include:

1) Code running in a TEE is to be kept as small as possible (thus with minimal attack surface area), and keep most code that is accessible over a network (e.g., protocol parsers) outside of the TEE.

2) Code running in a TEE must be able to be considered trusted by the customer. This can be achieved by making the code (both source and binary) public to all stakeholders, along with the expected hash that is matched against code running in the TEE.

3) Code, memory, and storage used by a *cloud* TEE must be encrypted so that the hoster cannot access them.

---

[14] A tamper-resistant platform capable of securely hosting apps and their data, such as is used on a credit card chip. https://www.globalplatform.org/mediaguideSE.asp

[15] Intel® Software Guard Extensions, http://software.intel.com/en-us/sgx. Blackhat overview slides at https://www.blackhat.com/docs/us-16/materials/us-16-Aumasson-SGX-Secure-Enclaves-In-Practice-Security-And-Crypto-Review.pdf

[16] A secure device identity standard produced by the Trusted Computing Group designed to scale down to MCUs where a larger trusted execution environment such as SGX (or even TPM) would be impractical.

[17] Trusted Platform Module, https://trustedcomputinggroup.org/tpm-main-specification

4) The fact that software running outside of a TEE cannot break into the TEE is guaranteed by the TEE hardware. The hardware vendor still needs to be trusted and customers can select their vendor of choice.

5.2 CPS Devices

This section covers two cases: new high-integrity CPS devices, and what to do if a customer has pre-existing low-integrity CPS devices that will take time to phase out.

5.2.1 High Integrity CPS (HI-CPS) device

A High-Integrity CPS (HI-CPS) device utilizes controllers with a trusted execution environment, so its code and operations policy is fully attestable. This is realized by MCUs, processors, or SoCs[18] that operate with a secure device identity. Any action of these devices is executed in the Trusted Execution Environment. The code in the TEE will require authentication for any action on the I/O pins controlling the physical system. Any actions or data provided to the devices' I/O pins will be logged by the TEE in a non-repudiable manner using blockchain technology.

The TEE in the HI-CPS device acts as the policy enforcement point (PEP) for its own operations, and the wires from the I/O pins that lead to the physical system being controlled are assumed to be physically secured.

Besides the actions normally associated with the function of the CPS, another important action is to be able to securely patch the software/firmware in the TEE itself. Patches must be securely authenticated and authorized, just as with any other action.

5.2.2 Low integrity CPS (LO-CPS) device

Although HI-CPS devices are the desire for end-to-end security, we expect that some customers will need a transition path in a "brownfield"[19] installation where cyber-physical systems might already be present that do not incorporate trusted I/O execution and either are extremely costly to replace or do not yet have high integrity processors available that meet their unique requirements. Today, such LO-CPS devices are often deployed without cloud connectivity (air gapped, as noted earlier).

An approach to providing them an intermediate solution is to place next to the LO-CPS device an intermediary device (e.g., a Windows IoT Core edge compute device, or any other High-Integrity CPS device) that securely provides access to it (i.e., all communication to the LO-CPS device must go through that gateway). The gateway must have a Trusted Execution Environment that is the only way to access the wires that lead to the LO-CPS device, and the wires that lead to the LO-CPS device are assumed to be physically secured, just as the wires from a HI-CPS device to the physical system must be physically secured. Such wires could even include a bus or a networking protocol for a more advanced LO-CPS device, but the key is that the bus/network connection must be isolated from the gateway's host OS and instead be accessible only to its Trusted Execution Environment. The TEE validates any request to send/receive a message to/from the LO-CPS device and only permits authorized requests.

The diagram below shows two options for how a brownfield installation could utilize a Trusted CPS solution. A key element in both options is that the communication behind the Trusted CPS gateway,

[18] System on Chip. https://en.wikipedia.org/wiki/System_on_a_chip

[19] Brownfield: https://en.wikipedia.org/wiki/Brownfield_(software_development)

towards the physical system, is physically protected. For example, control components such as PLCs with non-secure MCUs must not have exposed connectors that would allow insertion of malicious code.

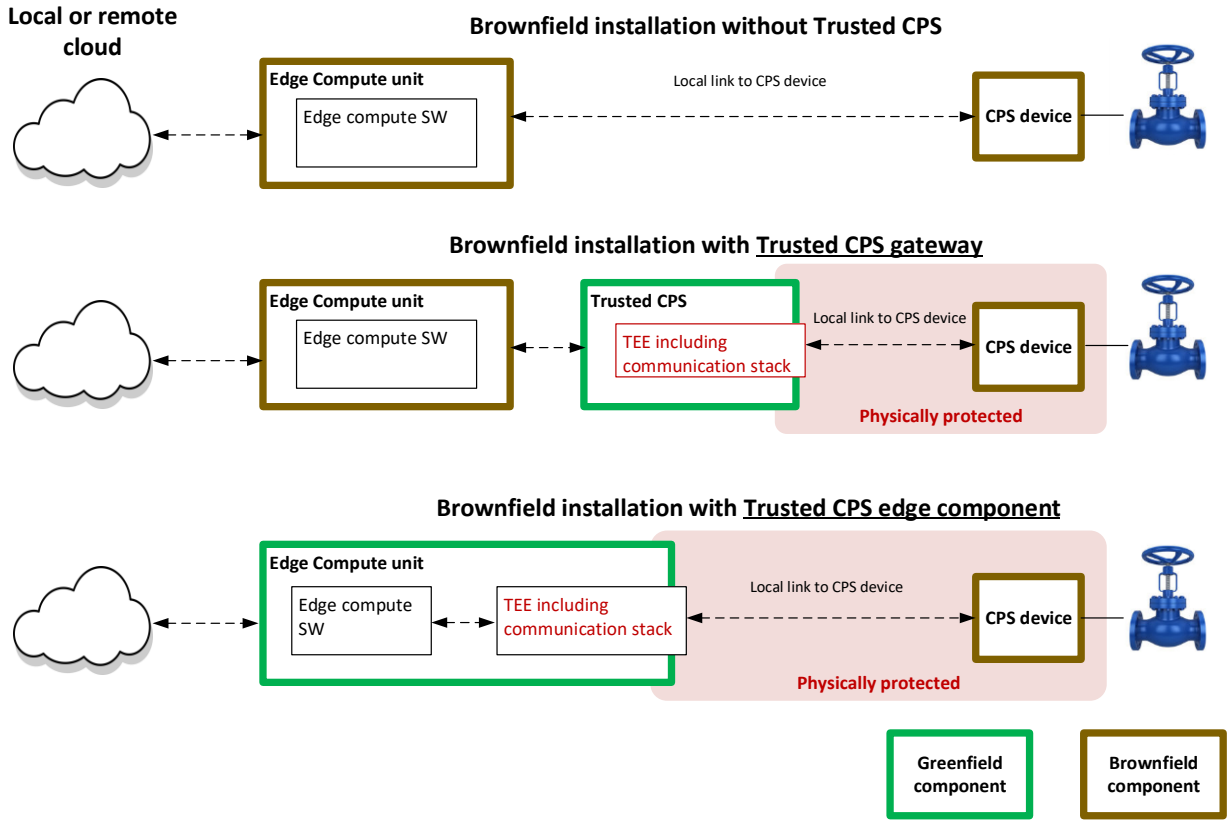


Figure 3: Brownfield alternatives

In the first option (middle row), a Trusted CPS bridge is added as a separate device in front of the LO-CPS device, such that all access to the MCU must go through the Trusted CPS gateway, code outside the TEE cannot access the local link to the CPS device, and physical access beyond the Trusted CPS gateway is protected. In the second option (bottom row), an edge compute device can be replaced by a Trusted CPS capable version.

If the LO-CPS device can be patched at all, it is also important to be able to secure patches, which again in some cases may require trusting an edge compute device to act as the gateway that checks any patches before passing them on to the LO-CPS device.

5.3 Edge compute device

The edge compute device is generally a less resource-constrained platform than the CPS device and so can provide additional features, many of which require a Trusted Execution Environment and secure protocols. It will provide cloud connectivity as well as a TEE, with capabilities to:

- Act as a **Policy Decision Point (PDP)** using more complex policies than an MCU could deal with itself, such as time-of-day based policies.
- Allow **configuration of autonomous rules/policie**s if desired, such as enforcing that a switch can only stay open for a maximum of 25 seconds. This would require it to be able to securely initiate an emergency close operation in such a case.

- **Store and manage secured logs**. If the CPS device encrypts the logs itself, an edge compute device without a TEE could potentially store opaque encrypted data, but could not necessarily protect against loss of that copy of the log.
- Act as a **secure gateway for a legacy LO-CPS** device as discussed above. If the LO-CPS device has firmware that can be upgraded, this also includes facilitating secure patch management of such devices.
- **Provide cloud connectivity**, including acting as a gateway to/from the protocol used by the CPS device. Trusted execution is required if such a gateway needs access to the unencrypted data in order to implement a gateway between two different enough protocols.
- Act as a **security gateway if a CPS device is not capable of using certificates**.
- Provide continuous operation within on premise systems even when an Internet outage is temporarily in effect

5.4 Cloud services

Cloud services allow for remote connectivity and offsite data maintenance (e.g., for security and disaster recovery), potentially using outsourced infrastructure for cost savings.

The service side of the solution thus contains several fundamental services that provide security guarantees:

- **Trusted Execution Environment** for CPS operation and data attestation.
- **CPS Patch Management**. Such patches might come from different vendors (the PLC manufacturer, the CPS operator, the edge compute device OS vendor, etc.) and only patches authorized by the CPS operator should be allowed.
- **Operations Log service**. Maintaining multiple copies of a log (whether on premise or in the cloud) allows tampering or corruption of a single copy to be detected and mitigated.
- **Customer Key Management and Escrow**. A key escrow[20] service allows scenarios such as backing up device keys and migrating them from one device to another (e.g., when replacing a broken device with a replacement), without the cloud service having access to the key itself or being able to use the key.
- Act as a **private Certificate Authority**, and a trusted root for certificates used by the Trusted CPS solution.
- Act as a **Policy Decision Point (PDP)** using more complex policies than an edge compute device might be capable of. For example, policies might involve a system of multiple actuators and sensors, which might be reached via different edge compute devices. As another example, execution of some policy might require manual confirmation by a human, for which the cloud might manage securely reaching out to one or more remote humans. Some particularly security-sensitive systems might even need confirmation from more than one human before being allowed.

[20] https://en.wikipedia.org/wiki/Key_escrow

This design will ensure that:

- any **privileged operation** is being conducted in a policy-protected and auditable way,
- any **escrowed key** is only stored and handled exclusively in an encrypted form that makes it unusable outside of the authorized devices
- **logging** is done in an infrastructure that uses forward progressing cryptographic validation and is maintained jointly by several entities

These cloud services may be run on Microsoft's cloud infrastructure or within a datacenter owned by the customer (e.g., using Azure Stack). Both are applicable to different customers; many customers benefit from the cost savings of using Microsoft's cloud, while customers with stricter requirements (e.g., national boundaries) can operate in an on-premise cloud.

It is also important that on premise systems can still be operated normally even in the event that connectivity to cloud infrastructure is temporarily unavailable. For example, if an external attacker can disrupt communication between a factory and the cloud infrastructure, the outage will not result in the inability of local devices to communicate with on premise systems. Thus, the availability of services in the cloud must not be strictly required for critical operations during stress events. Instead, edge compute devices provide continuous operation during such outages.

5.5 Trusting Hardware and Software

In the wake of the Snowden revelations, there was much industry discussion of potential vulnerabilities[21], including by major governments, via certificate authorities, software creators, hardware factories, network operators, etc. Thus, establishing trust in hardware or software can be difficult.

If a customer buys a piece of hardware, they must either perform an expensive security analysis of each piece of hardware or accept some risk and choose to trust the manufacturer. The same applies to software and services. A customer must either perform an extensive security analysis of each piece of software or accept some risk and choose to trust the software provider.

Hardware and software providers might also fall under jurisdiction of countries they are operating in. For such reasons, some countries choose to only buy from domestic factories using domestic designs and only use cloud data centers hosted domestically, and similar concerns may apply to non-governmental entities as well.

The TCPS design allows for mitigations that would allow others to trust code execution and key material without giving the service provider, ISV or government access. An objective of TCPS is to have any security-critical processing be done in a TEE that can provide a root of trust the solution operator can accept. For such customers, the following would likely be requirements (as evidenced by actual or potential attacks revealed by Snowden):

(1) Any trusted roots used by the TEE code are chosen by the customer, and Microsoft need not be one of them, even if the customer uses the Microsoft cloud and Microsoft code.
(2) The source code for TEE code is available, and small enough for a security lab to evaluate and certify. This is to mitigate attacks where the code contains a back door.

[21] See https://www.ietf.org/proceedings/88/slides/slides-88-perpass-6.pdf for a survey.

(3) The source code for the toolchain (e.g., compiler, linker, etc.) used to produce the TEE code from source is available, and small enough for a security lab to evaluate and certify. This is to mitigate attacks where the compiler inserts back doors.

5.6 Root of Trust

One of the key principals of a Trusted Cyber Physical System solution is, as the name says, trust. At any time, the operator of a TCPS solution must be able to follow a chain of trust for code operations as well as data. This chain will lead to a Root of Trust (RoT) that the operator ultimately accepts as trusted.

There are two types of information that should be secured with potentially different Roots of Trust:

- Code, to defend e.g. against malware
- Data, to defend e.g. against tampering or information disclosure

Depending on his business needs and security assessment, a TCPS operator can use a range of RoTs. Common RoTs are:

- **Customer/operator/device owner**
  - All customer-specific data and code uses a customer Root of Trust
- **Hardware vendor** (chip and/or device) as Root of Trust for hardware and firmware patches
  - Trust the hardware was made to be secure
  - Trust might be extended to firmware from the same HW manufacturer
  - A customer can also require hardware or firmware to be counter-signed by the customer Root of Trust if the customer has a vetting process
- **RoT vendors such as security companies**
  - RoT vendors providing security reviews and attestation for SW and HW
  - RoT vendors will sign SW, HW and data processed

There are several entities that are part of a TCPS solution and facilitate the date flow and processing but need **not be a RoT for any of the secure operations**. This includes:

- 3rd-party application provider
- Operating system provider
- Cloud service hosting provider
- Management system software provider
- Manufacturers of other hardware to facilitate operations, e.g., routers

It might also be in the interest of these parties not to have the possibility to access or change secure operations or data to avoid liabilities. In the water plant example above, the solution provider can assure the plant operator that none of his technicians can operate a valve without the consent of the operator.

5.7 Align with Industry standards

The industry has already well-established systems in place that provide communication via secured messages. As one example, the Industry 4.0[22] efforts utilize OPC-UA.[23,24] However, these solutions today

[22] https://en.wikipedia.org/wiki/Industry_4.0

[23] OPC foundation, https://opcfoundation.org/

[24] OPC Unified Architecture, https://opcfoundation.org/about/opc-technologies/opc-ua/

terminate the secure message exchange at software running in the PLC and not at the I/O pin of the MCU within the I/O module.

TCPS will utilize this infrastructure and extend the message protection to the TEE that controls the I/O pins. Cryptographically protected messages, such as commands carried by OPC-UA, are validated and processed in the TEE of the OPC server. The TEE in the OPC server is provisioned with credentials so it can authorize actions on the high integrity CPS device (e.g., a high integrity I/O module). It can also receive messages from the HI-PLC that are encrypted or attested, and translate them into authenticated OPC-UA messages.

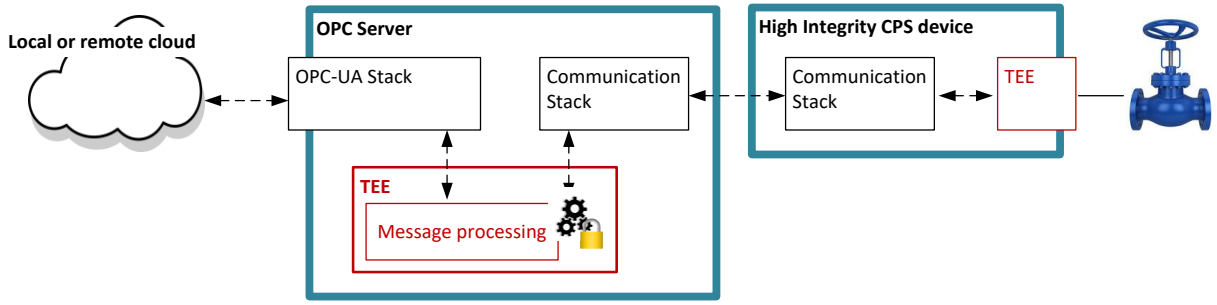


Figure 4: Relationship to OPC-UA

In some cases, the OPC Server and the HI-CPS device in the picture above might also be merged into one unit, where the OPC Server TEE can control the physical system.

5.8 Solution Lifecycle

A TCPS solution will go through a number of stages during its lifecycle. The architecture and scenarios for a TCPS design need to accommodate these stages, which are as follows:

Production:the HW and SW are created

Setup: The solution is deployed and provisioned and will be ready to use

Operation: The solution is doing what it is designed for, is maintained and might change ownership

End of Life: The solution is decommissioned

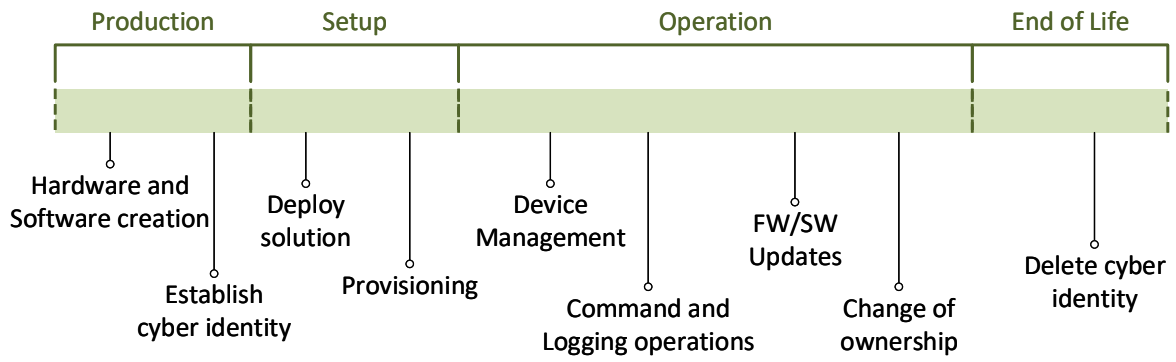


Figure 5: Solution lifecycle

5.8.1 Hardware and Software Creation

Building the HW and SW, including services, of a TCPS solution is a critical phase with regards to trust. This process must take place in a trusted manner, e.g., controlled design and manufacturing of MCUs or software with well-designed and reviewed security. Software is clearly separated into components that must run inside a TEE vs. those that do not run in a TEE, and TEE components undergo deep security vetting.

Any security breach in this phase is difficult to detect later and will have significant security impact to the whole solution.

5.8.2 Establishing Cyber Identity

All security relevant components, both hardware and software, will receive a manufacturer RoT used to sign updates. Any provisioning action on this system can use this RoT. This can include action such as adding a manufacturer certificate to a TEE or signing a piece of code. Hardware also receives a unique device identity from the manufacturer.

5.8.3 Deployment

All hardware and software components, including services, are put in place. At this time, the solution will be able to facilitate the processing of commands and data from/to the CPS device, even if the provisioning step has not yet occurred (deployment and provisioning can occur in either order, depending on the provisioning procedure used).

5.8.4 Provisioning

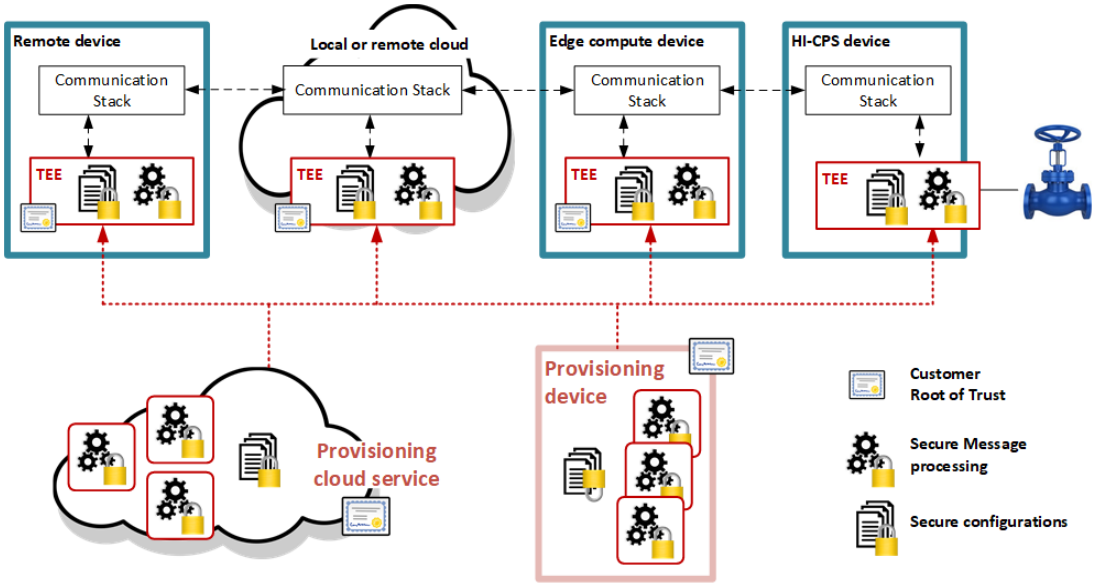
There are several systems that need to be provisioned with customer-specific credentials and software in the TEE.

Provisioning is one of the critical steps in the TCPS life cycle. Security-sensitive information is moved to all the involved systems, remote control devices, PLCs, cloud services and gateways/edge devices. Trusted operation of a TCPS solution will rely on the secure provisioning of all of those systems.

The graphic below shows two possible ways to provide subsequent customer-specific provisioning information once the customer RoT has already been provisioned:

Provisioning cloud service will provide secure configurations and processing code for any TEE in the graphic below. This will allow a remote configuration of the TCPS messaging chain.

Provisioning device is a device, such as a tablet or local machine, that will provide secure configurations (e.g., certificates) or code that will be processed by any TEE in the graphic below. These devices are used by local servicing personnel or on the manufacturing line.



Once provisioned, each device will have its own credentials that chain up to the customer's RoT (rather than the manufacturer's or the provisioning device's RoT), and the solution is then fully operable.

5.8.5 Device Management

Device management (DM) is a common task during operation to maintain the solution. A TCPS solution requires authenticating the DM commands as they could impact the physical system, e.g., restart a device.

5.8.6 Command and Logging – solution is doing its job

During the intended operation of a TCPS solution, the two major activities are sending commands to CPS devices and receiving data from CPS devices. Those operations will be authenticated and attested throughout the system. At any time, an operator can verify the correct operation of the solution. He is assured that he, and only he and authorized entities, have full control over the CPS.

5.8.7 Updating

A TCPS solution may need software/firmware updates over time, potentially including updates to code that runs inside a TEE. Compromised updates are a major entry point for malware. Therefore, it is essential that updates be deployed in a secure way. In a TCPS solution, updates are signed by the software/firmware manufacturer's RoT, and can be required to be counter-signed by the customer's RoT before they can be deployed in a TEE.

5.8.8 Change of Ownership

Change of ownership is often a common process in the physical world. When it comes to CPSs, such a change will also include the change of ownership in the cyber world, meaning the change of cryptographic information. This means that the device credentials used by the previous owner must be removed, and the new owner must establish new device credentials.

5.8.9 End of Life

If a CPS device reaches its end of life, it might be necessary to also destroy not only the customer-specific credentials of the device, but also the manufacturer's unique identity assigned to the device, to avoid misuse of the information in, e.g., refurbished devices.

6 Openness and Trust

Trust can only be achieved through means of a transparent auditable operation that has clearly defined principles that are in control for the operation of the solution. With Microsoft having a wide range of assets to define and build a secure IoT solution, it is essential that these developments can be shared and easily adopted by the rest of the industry, and can be analyzed by any security lab. The architecture allows for a variety of CPS platforms and vendors.

The approach described in this document will utilize well-established industry standards. Microsoft is already active in many of the relevant organizations. TCPS solutions need to be adoptable by a wide range of verticals, including manufacturing, facility operation, military and others.

Furthermore, any code that needs to run in a TEE will be available for security analysis.