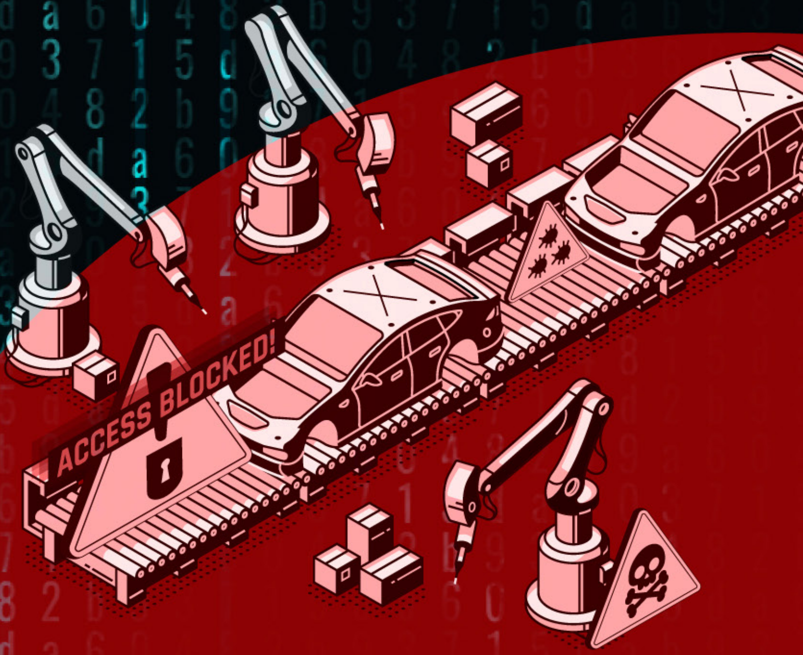
TXOne Networks

2023 /Q2



In-Depth Analysis of Cyber Threats to Automotive Factories

txOne networks

TXOne Networks

In-Depth Analysis of Cyber Threats to Automotive Factories

txOne networks

In-Depth Analysis of Cyber Threats to Automotive Factories

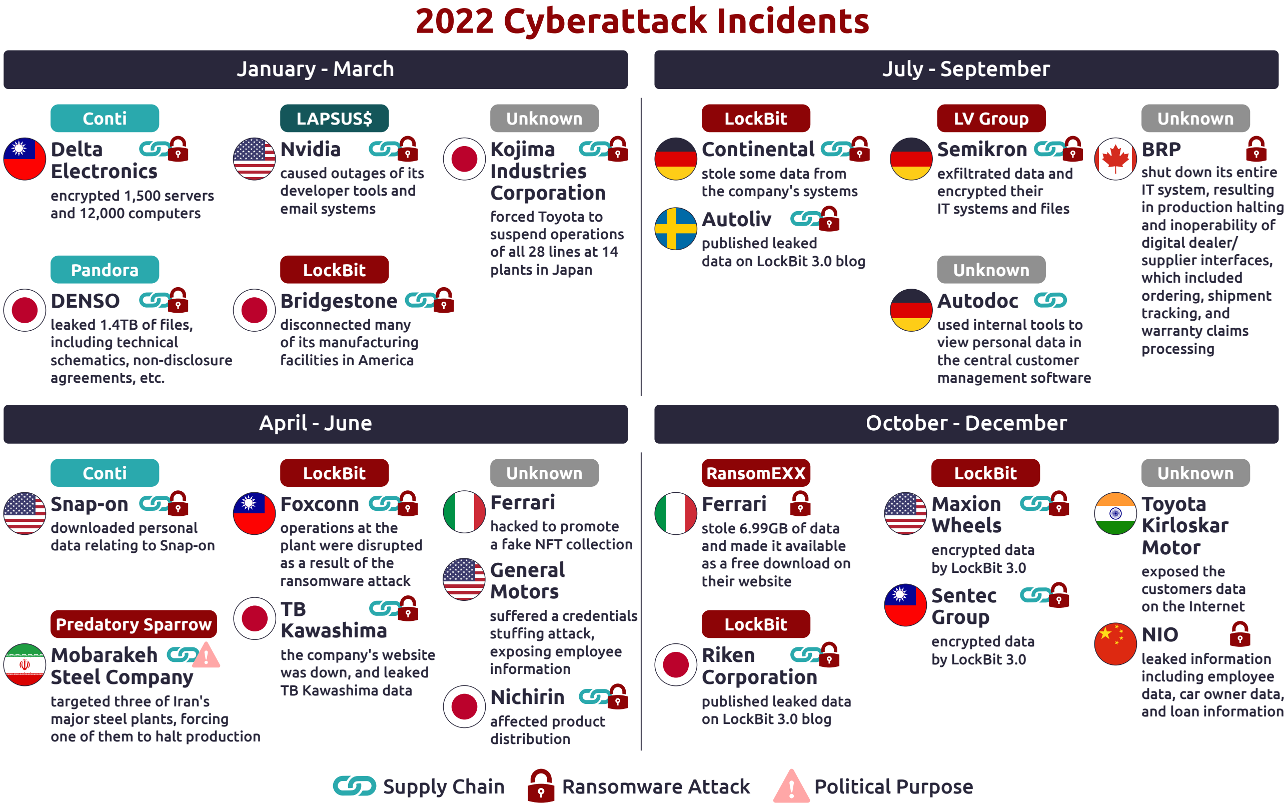
Table of Contents

Introduction

The year 2022 was turbulent, with threat groups zeroing in on critical infrastructure and numerous attackers continuing to carry out cyberattacks against industrial control systems. Based on cybersecurity incident intelligence investigating critical manufacturing in 2022, the automotive industry chain suffered the most severe attacks (as shown in Figure 1). We discovered that these were mostly financially motivated ransomware attacks. This is consistent with the findings of the 2022 SANS ICS/OT Cybersecurity survey results which revealed that the majority of industries are most concerned about threats from ransomware or other financially motivated crimes (accounting for 40%).[1] Therefore, the economically driven automotive industry is particularly compelled to pay close attention to the threats of cyberattacks.

Utilizing the MITRE ATT&CK for ICS framework can help companies understand and track their threats. Most enterprises are adopting this for ongoing assessments as the mainstream approach, and technology vendors are gradually integrating this framework into their ICS dashboards.

Generally, only a small number of companies have comprehensive countermeasures against attackers' tactics. Given this fact, this article will delve into the automotive industry's architecture and reference relevant threat research. This will enable automobile manufacturers to assess the specific consequences of these attacks.



2022 Cyberattack Incidents

January - March

Conti
Delta Electronics
encrypted 1,500 servers and 12,000 computers

LAPSUS$
Nvidia
caused outages of its developer tools and email systems

Unknown
Kojima Industries Corporation
forced Toyota to suspend operations of all 28 lines at 14 plants in Japan

Pandora
DENSO
leaked 1.4TB of files, including technical schematics, non-disclosure agreements, etc.

LockBit
Bridgestone
disconnected many of its manufacturing facilities in America

July - September

LockBit
Continental
stole some data from the company's systems

Autoliv
published leaked data on LockBit 3.0 blog

LV Group
Semikron
exfiltrated data and encrypted their IT systems and files

Unknown
Autodoc
used internal tools to view personal data in the central customer management software

Unknown
BRP
shut down its entire IT system, resulting in production halting and inoperability of digital dealer/ supplier interfaces, which included ordering, shipment tracking, and warranty claims processing

April - June

Conti
Snap-on
downloaded personal data relating to Snap-on

Predatory Sparrow
Mobarakeh Steel Company
targeted three of Iran's major steel plants, forcing one of them to halt production

LockBit
Foxconn
operations at the plant were disrupted as a result of the ransomware attack

TB Kawashima
the company's website was down, and leaked TB Kawashima data

Unknown
Ferrari
hacked to promote a fake NFT collection

General Motors
suffered a credentials stuffing attack, exposing employee information

Nichirin
affected product distribution

October - December

RansomEXX
Ferrari
stole 6.99GB of data and made it available as a free download on their website

LockBit
Riken Corporation
published leaked data on LockBit 3.0 blog

LockBit
Maxion Wheels
encrypted data by LockBit 3.0

Sentec Group
encrypted data by LockBit 3.0

Unknown
Toyota Kirloskar Motor
exposed the customers data on the Internet

NIO
leaked information including employee data, car owner data, and loan information

Supply Chain · Ransomware Attack · Political Purpose

Figure 1: 2022 Cyberattack Landscape for Automotive Industry

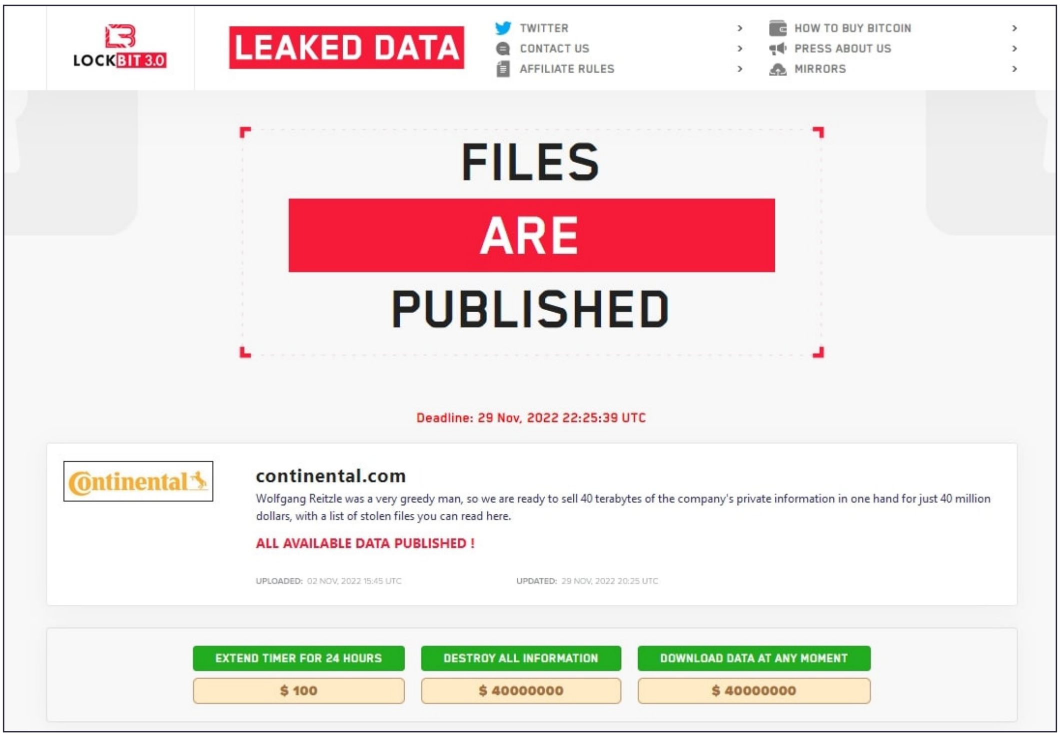
[1] *Nozomi Networks, "SANS 2022 Survey: The State of OT/ICS Cybersecurity in 2022 and Beyond", Nozomi Networks, 2022.*

Massive Cyberattacks on the Automotive Industry

In February 2022, Kojima Industries Corporation (a supplier of automotive interior and exterior components) fell victim to a ransomware attack on its file server, forcing the world's largest automotive manufacturer to temporarily shut down all 14 factories in Japan, comprising 28 production lines. Although the automaker resumed factory operations within a day, they stated in an announcement that the incident had impacted the production of about 13,000 vehicles, causing significant financial losses. This incident prompted automakers to reassess their supply chain threat management.

Active Ransomware-as-a-Service (RaaS)

We found that Ransomware-as-a-Service (RaaS) operations, such as Conti and LockBit, are active in the automotive industry. These are characterized by stealing confidential data from within the target organization before encrypting their systems, forcing automakers to face threats of halted factory operations and public exposure of intellectual property (IP). For example, Continental (a major automotive parts manufacturer) was attacked in August, with some IT systems accessed. They immediately took response measures, restoring normal operations and cooperating with external cybersecurity experts to investigate the incident. However, in November, LockBit took to its data leak website and claimed to have 40TB of Continental's data, offering to return the data for a ransom of $40 million.



Deadline: 29 Nov, 2022 22:25:39 UTC

continental.com

Wolfgang Reitzle was a very greedy man, so we are ready to sell 40 terabytes of the company's private information in one hand for just 40 million dollars, with a list of stolen files you can read here.

ALL AVAILABLE DATA PUBLISHED !

UPLOADED: 02 NOV, 2022 15:45 UTC

UPDATED: 29 NOV, 2022 20:25 UTC

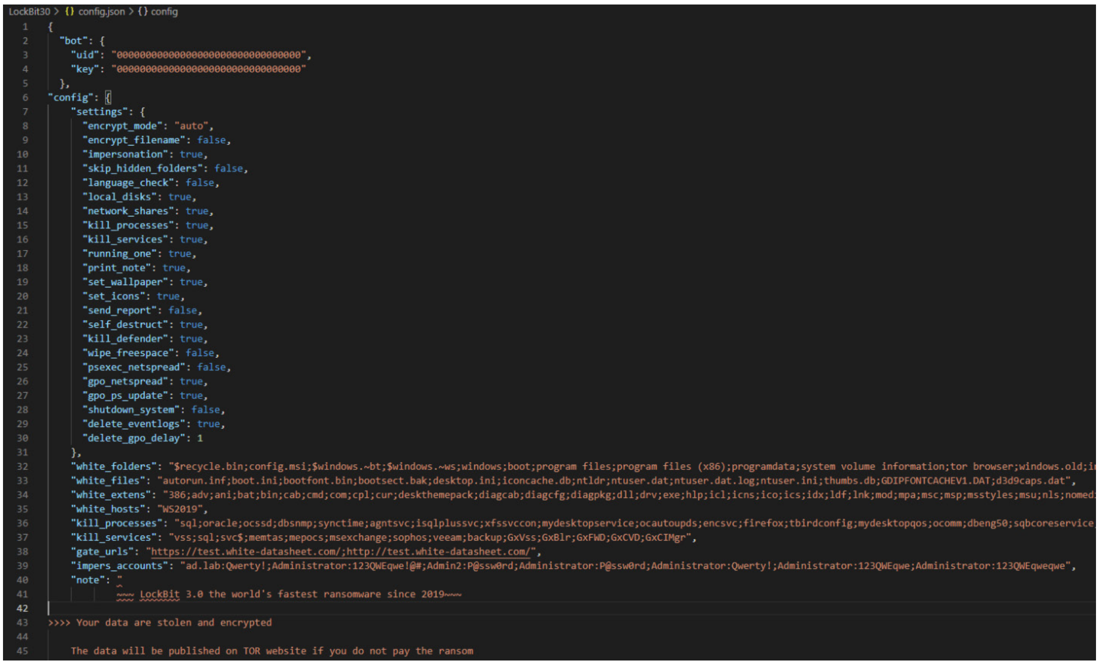
$ 100

$ 40000000

$ 40000000

Figure 2: LockBit Publicly Extorts $40 Million Ransom from Continental to Restore its Data

In recent years, LockBit has been popular not only for its high-profile social media activities but also for its configuration profiles, allowing threat actors to customize the encryptor for more flexible options. In September 2022, the LockBit 3.0 builder was leaked and published on GitHub. We can see that when LockBit 3.0 is activated, it follows the settings configured by a JSON file to execute customized actions (e.g., killed services/processes list, ransom note, files and folders' trust list, etc.).



```
LockBit30 > {} config.json > {} config
{
  "bot": {
    "uid": "00000000000000000000000000000000",
    "key": "00000000000000000000000000000000"
  },
"config": {
    "settings": {
      "encrypt_mode": "auto",
      "encrypt_filename": false,
      "impersonation": true,
      "skip_hidden_folders": false,
      "language_check": false,
      "local_disks": true,
      "network_shares": true,
      "kill_processes": true,
      "kill_services": true,
      "running_one": true,
      "print_note": true,
      "set_wallpaper": true,
      "set_icons": true,
      "send_report": false,
      "self_destruct": true,
      "kill_defender": true,
      "wipe_freespace": false,
      "psexec_netspread": false,
      "gpo_netspread": true,
      "gpo_ps_update": true,
      "shutdown_system": false,
      "delete_eventlogs": true,
      "delete_gpo_delay": 1
    },
    "white_folders": "$recycle.bin;config.msi;$windows.~bt;$windows.~ws;windows;boot;program files;program files (x86);programdata;system volume information;tor browser;windows.old;i
    "white_files": "autorun.inf;boot.ini;bootfont.bin;bootsect.bak;desktop.ini;iconcache.db;ntldr;ntuser.dat;ntuser.dat.log;ntuser.ini;thumbs.db;GDIPFONTCACHEV1.DAT;d3d9caps.dat",
    "white_extens": "386;adv;ani;bat;bin;cab;cmd;com;cpl;cur;deskthemepack;diagcab;diagcfg;diagpkg;dll;drv;exe;hlp;icl;icns;ico;ics;idx;ldf;lnk;mod;mpa;msc;msp;msstyles;msu;nls;nomed
    "white_hosts": "WS2019",
    "kill_processes": "sql;oracle;ocssd;dbsnmp;synctime;agntsvc;isqlplussvc;xfssvccon;mydesktopservice;ocautoupds;encsvc;firefox;tbirdconfig;mydesktopqos;ocomm;dbeng50;sqbcoreservice
    "kill_services": "vss;sql;svc$;memtas;mepocs;msexchange;sophos;veeam;backup;GxVss;GxBlr;GxFWD;GxCVD;GxCIMgr",
    "gate_urls": "https://test.white-datasheet.com/;http://test.white-datasheet.com/",
    "impers_accounts": "ad.lab:Qwerty!;Administrator:123QWEqwe!@#;Admin2:P@ssw0rd;Administrator:P@ssw0rd;Administrator:Qwerty!;Administrator:123QWEqwe;Administrator:123QWEqweqwe",
    "note": "
            ~~~ LockBit 3.0 the world's fastest ransomware since 2019~~~

>>>> Your data are stolen and encrypted

    The data will be published on TOR website if you do not pay the ransom
```

Figure 3: Configuration of LockBit 3.0

Exploring the Infrastructure and Architecture of Automotive Manufacturing Plants

The global automotive industry has become the largest spender on digital transformation, with a predicted expenditure of nearly $130 billion by 2023.[2] Various automakers are gradually increasing the digitalization level of their factories to gain competitive advantages and new opportunities. Nowadays, automotive manufacturing not only needs to meet performance requirements but also prove its uniqueness and worth to consumers. For example, Tesla invested $5 billion to build a factory to produce lithium battery packs for electric vehicles, which will enable Tesla to reduce its battery costs by about 30%, making their car models affordable for the mass market.

We collected several automotive factory architectures and their plans, consolidating common digital transformation applications as shown in Figure 4 below. These include industrial robots (as indicated in yellow), industrial cloud (as indicated in blue and orange), digital twins (as indicated in purple), transportation (as indicated in gray at the top left), and renewable energy technologies (as indicated in green). The explanation is as follows:

[2] *ABI research "4 Key Industries Embracing Industry 4.0", ABI research, November 22, 2022.*

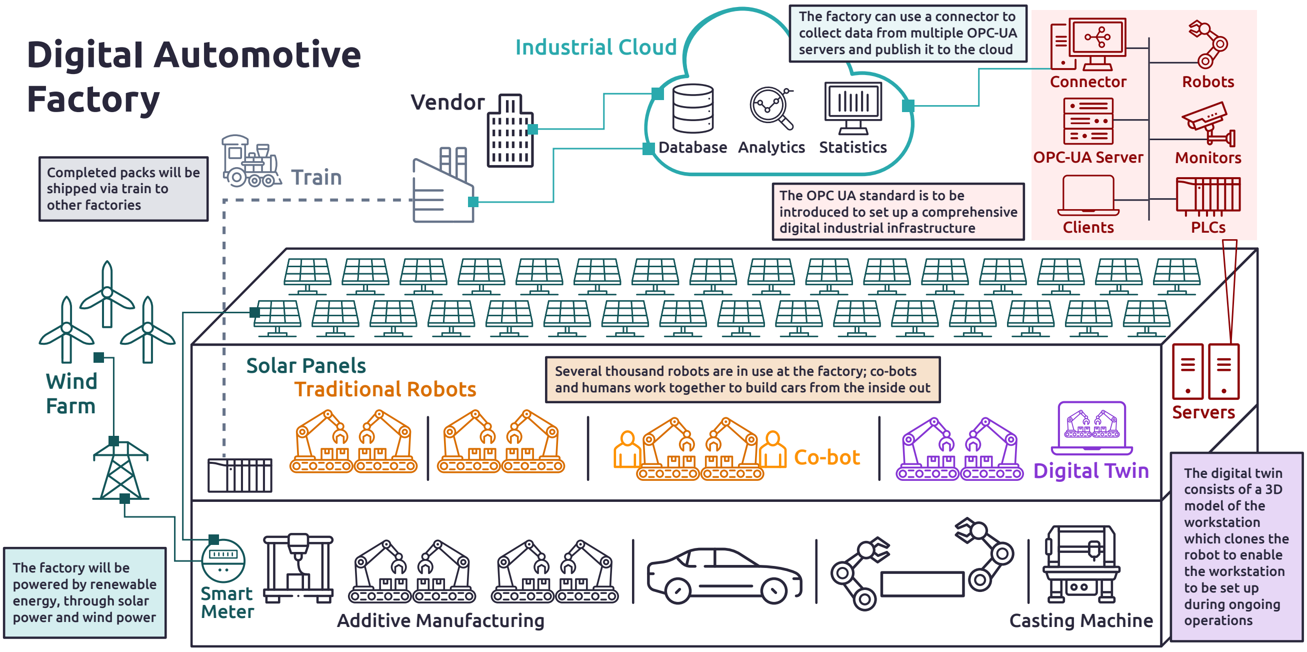

Digital Automotive Factory
Industrial Cloud
The factory can use a connector to collect data from multiple OPC-UA servers and publish it to the cloud
Vendor
Database
Analytics
Statistics
Connector
Robots
OPC-UA Server
Monitors
Clients
PLCs
The OPC UA standard is to be introduced to set up a comprehensive digital industrial infrastructure
Train
Completed packs will be shipped via train to other factories
Wind Farm
Solar Panels
Traditional Robots
Several thousand robots are in use at the factory; co-bots and humans work together to build cars from the inside out
Co-bot
Digital Twin
Servers
The digital twin consists of a 3D model of the workstation which clones the robot to enable the workstation to be set up during ongoing operations
The factory will be powered by renewable energy, through solar power and wind power
Smart Meter
Additive Manufacturing
Casting Machine

Figure 4: Digital Transformation to Automotive Factory

Industrial Robots

Using industrial robots to help manufacturing complete highly repetitive and easily programmable tasks is one of the most common strategies in digital transformation. This holds true especially in automotive manufacturing, where high-risk metal casting or defect inspections difficult for the human eye to catch are often required. These tasks are well-suited for assistance from industrial robots. For example, Volkswagen has deployed over 5,000 robots in its Wolfsburg factory alone, including the use of FANUC robots to assist in body production. Additionally, Tesla uses a large number of robots in its production lines. In the body shop, they use more than 600 robots to perform stamped parts & chassis castings tasks, followed by a giant robot lifting the entire body to the paint shop. In the paint shop, Tesla also employs robots to enable multi-layer painting for depth, dimension, and a hand-painted look.[3] The architecture of industrial robots not only includes the most prominent arms and end effectors (e.g., pliers, a cutter, or a laser beam welder) but also some important components described below:

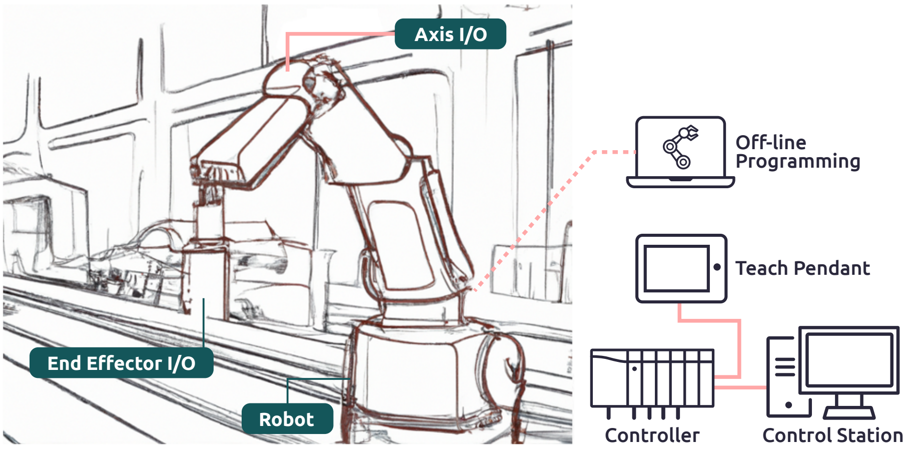


Figure 5: Industrial Robot Architecture

[3] Tesla, "Giga Berlin is the machine that builds the machine", Tesla Twitter, February 14, 2023.

1. **Controller:** The robot controller is composed of multiple subsystems and computers, usually enclosed in a chassis. Controllers typically offer automatic or manual work modes. In automatic mode, the controller loads programs from the teach pendant or its own memory to execute tasks. In manual mode, the controller executes corresponding actions based on commands input by the operator through the user interface. In this mode, the controller allows the use of reduced speed modes for programming the robot or high-speed modes for testing.

2. **Teach Pendant:** The teach pendant is a handheld device that provides operators with remote control of the robot, usually containing multiple buttons, switches, or a touch-sensitive display. In addition to displaying the commands the robot is currently executing, the display allows operators to edit these commands. The teach pendant also has an emergency stop button to immediately halt the robot's operation, ensuring the safety of surrounding personnel in case of a malfunction. To overcome issues with movement paths and cable positions, more and more manufacturers are adopting Wireless Teach Pendant (WiTP) technology, allowing simultaneous operation of multiple robots.

3. **Control Station:** This refers to a computer with installed robot-specific software, enabling remote operation and programming of the robot via a network. With the development of the Robot Operating System (ROS), its framework is widely applied in autonomous control fields such as drones, industrial robotic arms, unmanned transport vehicles, and self-driving cars. ROS 2 adopts the Data Distribution Service (DDS) as the standard for data exchange, features reliability, high performance, real-time, and interoperability, and is thus becoming one of the main application trends in factories. For example, in May 2022, Universal Robots released ROS 2 drivers compatible with their products, and PSA Group (Europe's automotive manufacturer, with brands that include Citroën, DS, Peugeot, Vauxhall, and Opel) used their robots to create a production line to improve factory efficiency and reduce costs.

4. **Off-Line Programming (OLP):** OLP is a method of robot program compilation, where programmers can use their EWS to write programs through 3D models in the simulator while offline, and then upload the program to the actual robot for execution. In addition to not interfering with the automotive manufacturing process, the benefits of compiling this way include helping programmers create optimal paths for executing specific tasks through the simulator's analysis tools.

Renewable Energy

Automotive assembly and automotive parts manufacturing are energy-intensive processes that used to result in massive carbon dioxide emissions due to the huge power loads it demands. In deference to government regulations, consumer demands, and brand reputation, adopting renewable energy has become a core business strategy for automotive manufacturers. For example, Mercedes-Benz collaborated with energy suppliers Enovos and Statkraft, and began purchasing electricity entirely from renewable sources in Germany in 2022. The electricity mainly comes from solar, wind, and hydropower plants, making a significant contribution to the expansion of renewable energy and energy transition in Germany. BMW Group also uses renewable energy in all its European manufacturing plants, prioritizing self-production of energy. If a plant cannot self-produce energy due to technical or economic reasons, they will purchase renewable energy electricity from local sources instead.

Furthermore, BMW Group utilizes the Carbon Disclosure Project (CDP), requiring suppliers to provide information on carbon dioxide emissions and agreeing with them to increase the share of renewable energy used. The most common power generation methods currently used in automotive manufacturing plants are solar and wind power, as described below.

1. **Solar Power:** This power generation method requires a large area, with endpoint devices dispersed across various regions. Automotive manufacturing plants that self-produce electricity have solar panels covering the entire roof and surrounding the building to generate most of their power needs. In addition to solar panels, the exposed equipment includes inverters with networking capabilities. Inverters in different regions can transmit power generation status to the controller through the internet, which then provides the information to the backend SCADA system. Similarly, inverters can also receive control commands to execute corresponding actions.

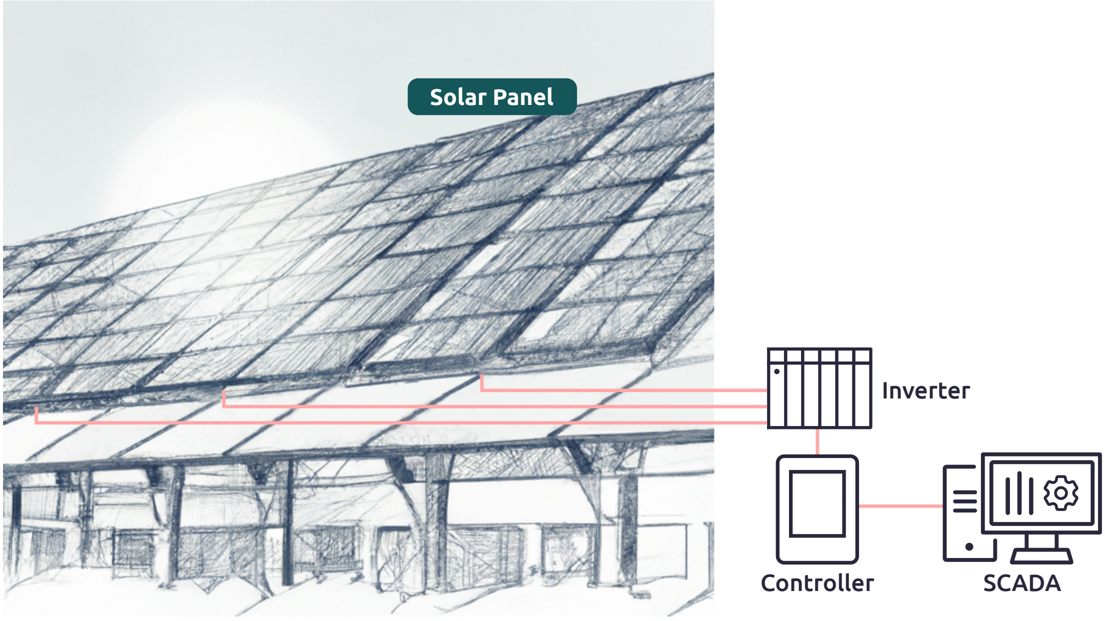


Figure 6: Solar Power Architecture

2. **Wind Power:** Similar to solar power, it requires cooperation with natural environmental factors, establishing wind turbine units in external environments. In addition to the blades, gearbox, and generator at the top of the wind turbine unit, there is also a networked control panel at the bottom. Depending on the implementation method, this control panel may consist of an HMI, controller, inverter, etc. During the power generation process, wind turbine units also provide power generation information to the backend SCADA system through a ring structure.

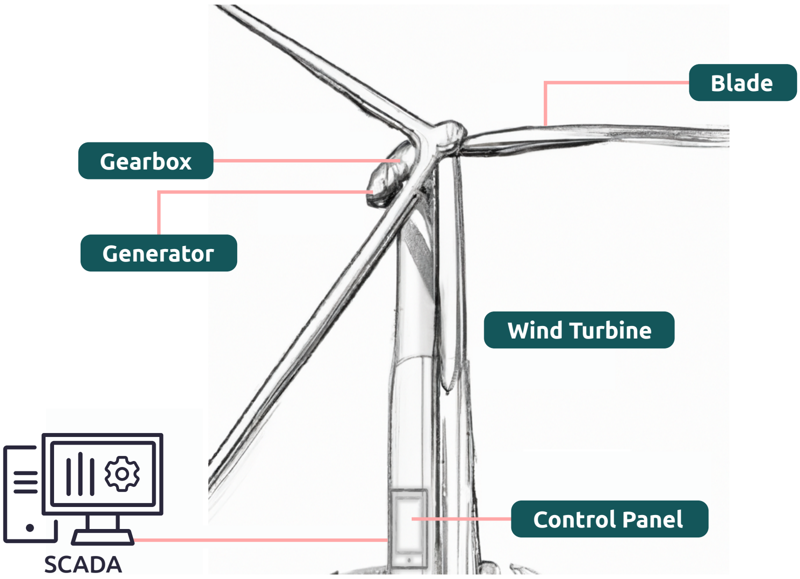


Figure 7: Wind Turbine Architecture

Industry Cloud

Adopting cloud technology for data analysis is nothing new for automotive manufacturing plants. Volkswagen collects data from all machines, equipment, and systems in their manufacturing plants and sends it to the cloud, allowing them to effectively analyze their manufacturing processes and improve productivity. They are also continuously integrating their global supply chain into the cloud, allowing them to comprehensively assess and control all critical data in production and logistics.

Specifically, Volkswagen and AWS collaborated to develop an industry cloud. Its architecture allows automotive manufacturing plants to publish data collected from multiple OPC-UA servers to this cloud through AWS's IoT SiteWise technology. This data can then be processed and used for machine learning through AWS IoT Analytics, Amazon QuickSight, S3, and Amazon SageMaker, providing visualization of analysis results for authorized users. Volkswagen estimates that by 2025, they can increase plant productivity by 30% and save 1 billion euros in costs by using this technology. Here are some introductions to a few AWS cloud technologies:

1. **AWS IoT Analytics:** Since IoT data often comes from devices that measure temperature, motion, or sound, these devices can easily transmit noise and corrupted or misread information. If this information is not preprocessed beforehand, it renders the data meaningless. AWS IoT Analytics provides automated filtering, transformation, and adjustment of IoT data, storing it in a time-series data repository for analysis. Users can then use the built-in SQL engine to analyze the data or perform more complex machine learning tasks.

2. **Amazon SageMaker:** A cloud-based machine learning platform that allows users to create, train, and deploy machine learning models in the cloud. SageMaker also provides managed instances for TensorFlow, allowing users to compile TensorFlow code and run it in the cloud. According to Amazon, in addition to the automotive industry, well-known brands in transportation, energy, pharmaceuticals, and healthcare are also using this service.

Cloud Architecture Overview

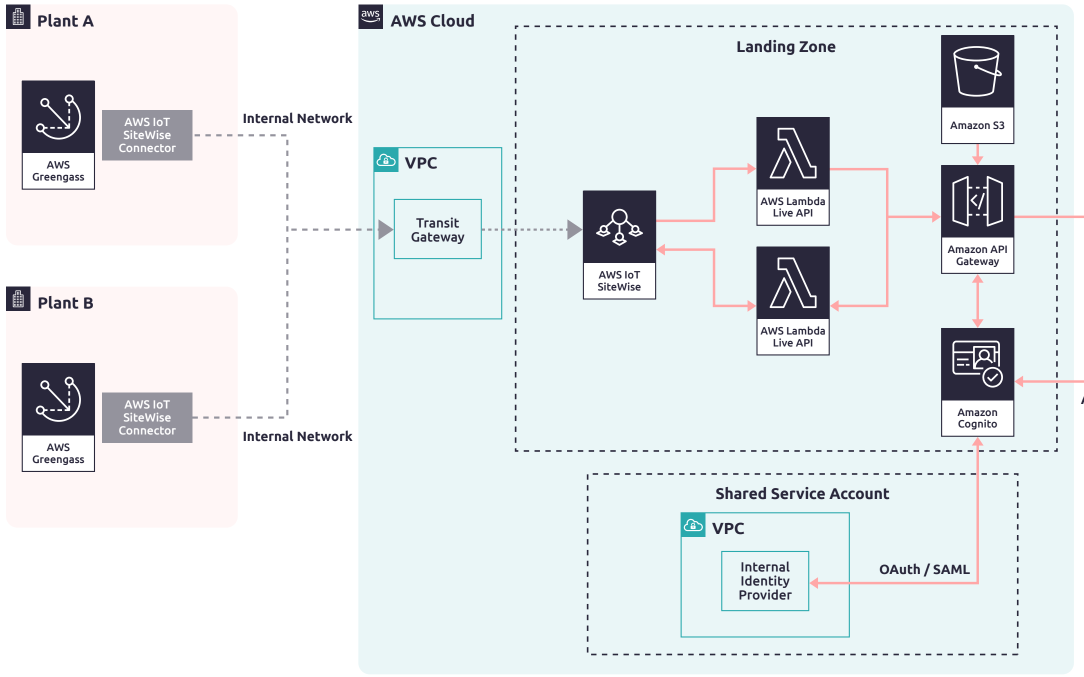


Figure 8: Solar Power Architecture[4]

It is worth mentioning that in 2022, Volkswagen introduced the OPC-UA standard (a standard specifically developed for inter-machine communication) in its manufacturing plants. This standard can help manufacturing plants almost automatically connect with the system when introducing new robots, eliminating the need for constant reconfiguration. In environments where up to 12 different machine languages are used worldwide, operators only need to master OPC-UA to handle most automakers' machine operations.

OPC-UA uses a publish and subscribe mechanism, enabling it to handle a large number of connections between servers and clients. It also uses the HTTP connection mode, allowing users to easily connect OPC servers and clients in different system environments remotely. The OPC server serves as a bridge between hardware and software, with software including automakers’ SCADA, MES, and Database systems, and hardware including PLCs, industrial robots, smart meters, sensors, and actuators. Under the industry cloud architecture, the more protocols the OPC server can support, the more extensive the collection of automaker data in the cloud, providing analysts with a more comprehensive analytical archive to draw from.

[4] *Pascal Hahn, Dr. Uwe Wieland, “Transforming automotive manufacturing with Volkswagen”, AWS re:Invent, 2019.*

If we take a closer look at the communication process of OPC-UA, we can find that when the client attempts to send a connection request to the server, there are specified Security Modes, Security Policies, and User Identity Tokens for the endpoint devices owned by that server. After the client sends a secure request to the endpoint device according to the specified method, the server will also record relevant connection information to protect the factory from communication protocol attacks by intruders.

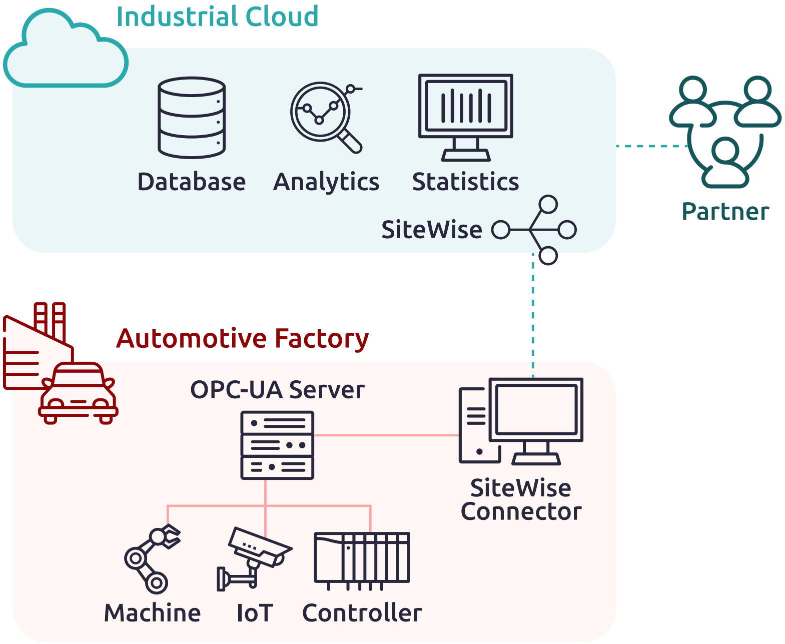


Figure 9: OPC-UA at Automotive Factory Sample [5]

Transportation

With the growth in demand for automobiles, the railway sector has designed trains specifically for transporting automobiles to increase cargo capacity. Trains are actually involved in all stages of automobile manufacturing, including transporting iron ore and coke required for steelmaking, transporting semi-finished products between manufacturing plants, and transporting finished products to dealerships. For example, Tesla manufactures battery packs for electric vehicles at its Gigafactory and subsequently transports them by train to the Fremont factory, about 250 miles away, where the battery packs are installed in the vehicle chassis. This shows that transportation is an indispensable link of the automotive supply chain.

Since trains carry a huge amount of cargo weight, it is difficult for them to stop when they encounter obstacles. To avoid collisions between trains, maintaining distance between trains through railway signaling is one of the most important safety systems. Some common railway signaling systems include Automatic Train Protection (ATP) and Communications-Based Train Control (CBTC), explained as follows:

[5] *Volkswagen, "Volkswagen brings additional partners to Industrial Cloud", Volkswagen, July 23, 2020.*

1. **ATP:** Trains can automatically receive ground speed limit information, process it in a series of steps, and compare it with the actual train speed. When the train's actual speed exceeds the speed limit, the braking device controls the train to stop before the stopping point or have an actual speed lower than the speed limit before the speed limit point. To achieve this effect, ground devices should include functions to detect train location, calculate the speed limit for subsequent trains based on the preceding train, and transmit speed limit information to the train. The train should include a system to receive and display speed limit information and automatic braking.

2. **CBTC:** The main objective is to increase the number of trains that can operate on railways by reducing the time intervals between trains. Specifically, trains continuously calculate and transmit their exact position, speed, direction of travel, and braking distance required to roadside equipment along the route via radio. This way, the required area for the train on the railway can be determined, and this area must not be passed by other trains on the same railway, ensuring the basic safety and comfort requirements between trains. This application can also be used to implement ATP functionality. The wireless networks used by CBTC mostly adopt WLAN devices based on IEEE 802.11 to enable trains to transmit large amounts of data in real-time. To meet high availability requirements, a redundant structure is also used. When one network cannot function properly due to equipment failure, the system can still send and receive data through another network.

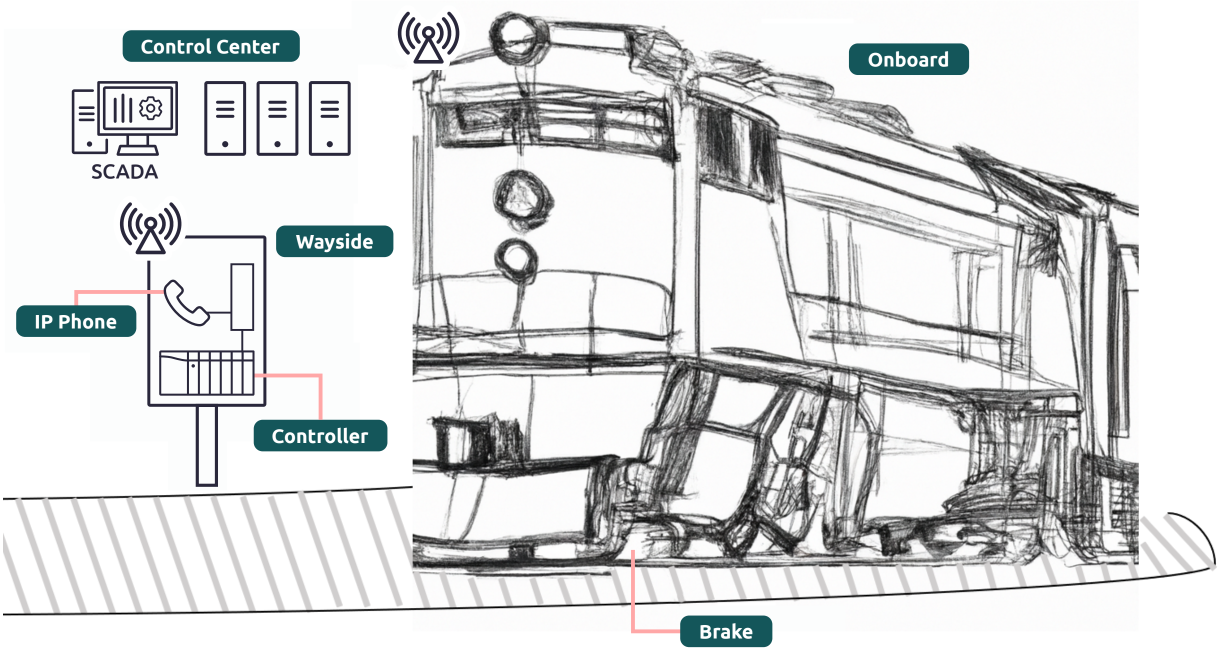


Figure 10: Train Architecture

Digital Twin

The main concept behind digital twin is to receive real-time data from the physical environment and present it to the user in a virtual but realistic simulation, helping users quickly understand, learn, and analyze the state of the physical environment. Driven by digital transformation in automotive factories, several manufacturers are now adopting digital twin technology to increase productivity or manage product quality. For example, Tesla creates a digital twin for each car they sell and continuously transmits data to the factory simulation through sensors. Through this simulation, they can understand whether each car is working as expected or if further maintenance is required. SKODA also uses digital twin technology to simulate the steps of automobile manufacturing, optimizing the efficiency of the car manufacturing process through detailed virtual factory images and simulating all mechanical motion processes.

In essence, digital twin technology is similar to Cyber-Physical Systems (CPS). CPS combines computer computations with sensors and actuators, closely integrating the various components of the physical environment with networks so that personnel can analyze and control the physical environment virtually, effectively improving the efficiency of automobile manufacturing. Another example is Ford's use of Digital Twin technology to simulate the actual operation of light beams in the physical world when building their headlight system (which helps drivers know in advance about approaching curves in the dark). When the operator wants to adjust the actual light beam in the physical environment to test the real vehicle, they can issue operation commands to the CPS to control the actuator to perform the corresponding functions. Through this method, Ford engineers can quickly test their systems under countless scenarios and lighting conditions, meaning they can gain an edge in the fiercely competitive automotive industry.

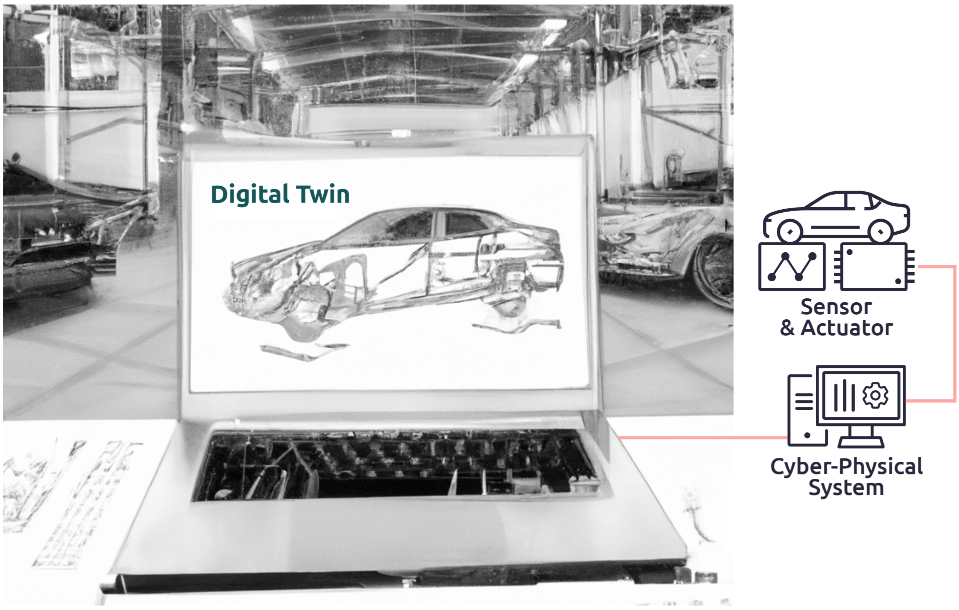


Figure 11: Digital Twin Architecture

In-Depth Threat Analysis of Automotive Factories

As automotive factories embrace digitalization, they often bring more threats into the factory environment. When attackers have the opportunity to exploit these threats and launch network attacks on the factory, it can cause significant losses to the enterprise. As noted in the 2022 Cyberattack Landscape, attackers with financial motives not only attempt to disrupt the operations of automobile manufacturers, but also target intellectual property (IP), which is one of the most valuable assets owned by these manufacturers. If attackers successfully breach the factory's critical systems and steal their data, it may compromise the manufacturer's past research efforts. Israeli network security solution provider, Upstream Security, predicts that, on average, network attacks will cause automobile manufacturers to lose $23 billion by 2023.[6]

Previous studies on automotive factories mainly focus on the general issues in the OT/ICS environment, such as difficulty in executing security updates, knowledge gaps among OT personnel regarding security, and weak vulnerability management. In light of this, TXOne Networks has conducted a detailed analysis of common automotive factory digital transformation applications to explain how attackers can gain initial access and link different threats together into a multi-pronged attack to cause significant damage to automotive factories.

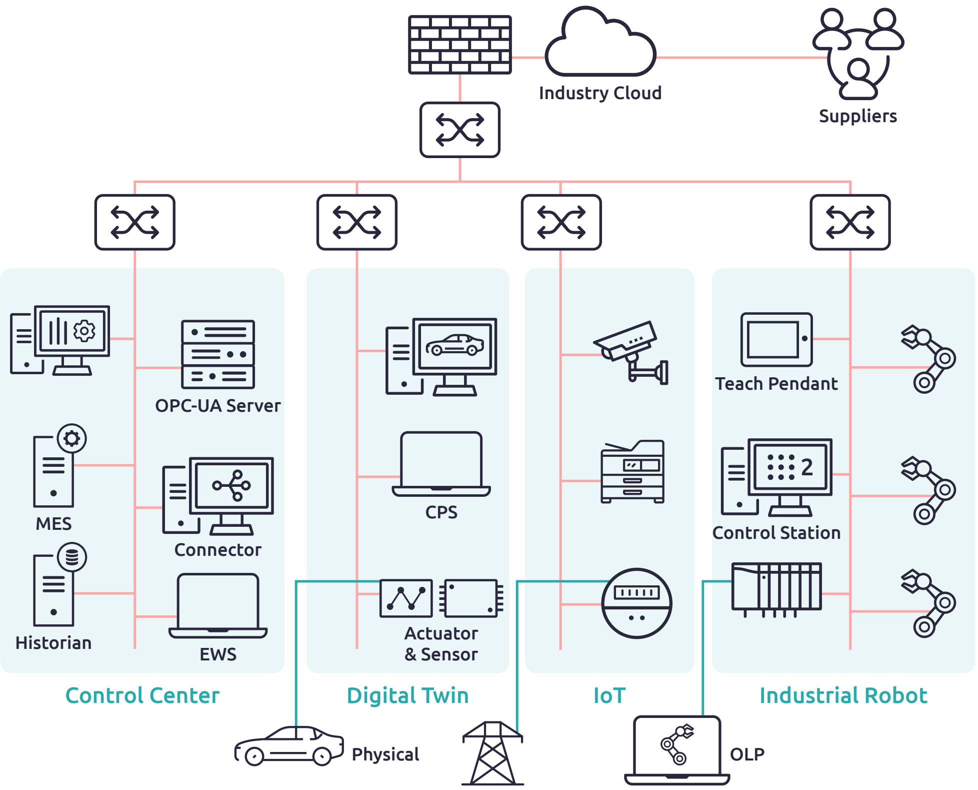


Figure 12: Digital Automotive Factory

[6] *Goud, N., "Auto Industry could lose $24 billion to Cyber Attacks - Cybersecurity Insiders", Cybersecurity Insiders, December 18, 2018.*

Takeover Automotive Factory

Without assuming the presence of remote services exposed to the internet, it is not easy for external attackers to gain initial access to a car factory. In most cases, attackers need to exploit the technical characteristics of the factory and the cooperation of personnel to have a chance at infiltrating the industrial control environment. In our analysis of common digital applications in car factories, we found that industrial robots, which are heavily deployed, could be potential elements for initial access.

In an operating car manufacturing factory, engineers would not want to pause the manufacturing process to test robot programs. This is especially true for manufacturers with clear production division, as delays in the delivery of parts can significantly affect the production outcome of the entire vehicle. Therefore, engineers will use the technology of offline programming (OLP) to simulate the manufacturing tasks of their robots using 3D models, write and test the code without physically contacting the robot, and upload it to the actual robot to execute after testing.

Depending on the robot supplier, they may have their own OLP program, which they may only provide to customers who actually purchase their products. We found that, since robot suppliers vary in how seriously they take cybersecurity issues or how they prioritize these issues during development, engineers installing OLP programs on their computers can expose them to many risky services. For example, some OLPs can open services for remote users to simulate the teaching function to operate the robot when simulating robot manufacturing tasks, and these operations often do not have any authentication mechanism. Among them, OLPs are given higher execution privileges in the computer. When there are issues such as path traversal access in OLP, attackers can install malicious software on the engineer's computer, and wait for the engineer to carry the computer into the factory environment for updating the actual robot program, so that the attacker can infiltrate the industrial control environment.

Another example of the engineer's computer is that some vendors provide online software extension platforms to enable engineers to quickly write programs by uploading or downloading relevant extension packages according to their needs. In previous studies, researchers found that attackers could bypass the review mechanism of the program and upload extension packages, which could also be successfully downloaded and executed by other users. In such cases, if the program also supports dynamic code loading, attackers can also install malicious software on the engineer's computer.

Another entry point for initial access is the cloud service of automotive suppliers. Ideally, suppliers would upload data from all of the factory's machines to the cloud and also upload machines in their supply chain for more comprehensive analysis. However, as more personnel from different companies have credentials to access cloud data, attackers have more opportunities to steal these credentials through common IT environment methods such as phishing and use cloud technology to execute operational behavior on machines in the factory. Compared to other computing systems, cloud computing has greater potential for critical damage because it does not have a physical counterpart. Once credentials are stolen, attackers can completely replace the original user's identity and easily interact with APIs and cloud services. For example, at Black Hat USA 2022, researchers found that in past Azure ADs, if attackers could obtain non-redeemed invite serial numbers in advance through social engineering methods, they could allow any external account to join the enterprise domain without verification.[7]

[7] *Dirk-Jan Mollema, "Backdooring and Hijacking Azure Ad Accounts by Abusing External Identities", November 10, 2022.*

The above explains how attackers can use Transient Cyber Asset and External Remote Services technology to obtain initial access to automotive factories. Next, we will analyze how attackers continue to impact the factory. Generally, since the industrial control environment has actuators connected to the network and manipulates the behavior of machines in the physical environment, when machine behavior is interfered with by attackers, the harm done to the factory is often acute. For example, when a robot intentionally produces a small defect that is difficult for an operator to detect during the car manufacturing process, the automaker may discover the problem too late and need to recall a large number of already sold cars. In addition to bearing the basic repair costs, this also sorely damages the intangible corporate reputation. If the automaker is developing a new system using digital twin technology, when the CPS cannot execute the correct command according to the engineer's requirements, it may lead to system development failure and the inability to gain a market advantage.

In the study of industrial robots, controllers sometimes enable universal remote connection services (such as FTP or Web) or APIs defined by the manufacturer to provide operators with convenient robot operation through the Control Station. However, we found that most robot controllers do not enable any authentication mechanism by default and cannot even use it. This allows attackers lurking in the factory to directly execute any operation on robots through tools released by robot manufacturers. In the case of Digital Twin applications, attackers lurking in the factory can also use vulnerabilities in simulation devices to execute malicious code attacks on their models. When a Digital Twin's model is attacked, it means that the generated simulation environment cannot maintain congruency with the physical environment. This entails that, after the model is tampered with, there may not necessarily be obvious malicious behavior which is a serious problem because of how long this can go unchecked and unfixed. This makes it easy for engineers to continue using the damaged Digital Twin in unknown circumstances, leading to inaccurate research and development or incorrect decisions made by the factory based on false information, which can result in greater financial losses than ransomware attacks.

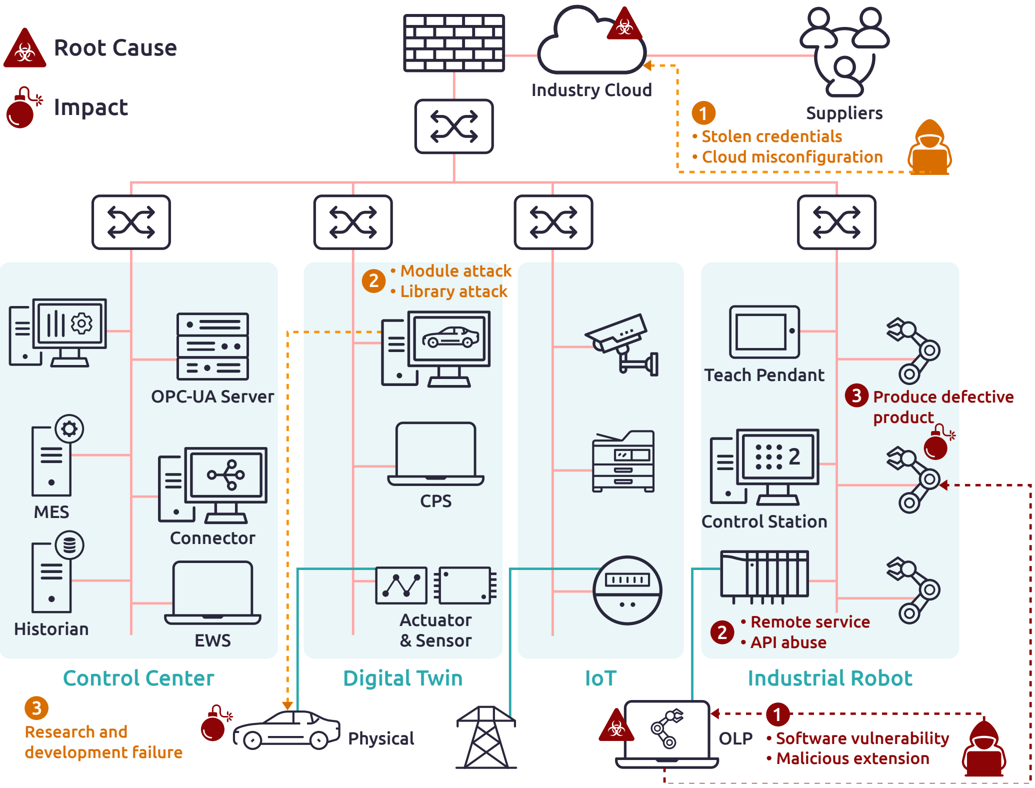


Figure 13: Takeover Automotive Factory

Obstructions to the Automotive Product Line

For car manufacturers with a core focus on profits, the losses are always enormous when a disruption attack occurs that affects the factory assembly line. Let's start by looking at OPC-UA, which is expected to become the communication core of digital factories. Currently, the mainstream OPC-UA package is built on the .NET Runtime (.NET Framework/.NET Core). However, the default memory stack size of .NET Runtime is limited, and when an attacker recursively exceeds a certain depth, there is a chance of causing a stack overflow issue. For example, in CVE-2018-12086, it was shown that an attacker only needed to send an ExtensionObject structure with a size of 64KB to cause the OPC Server to crash. Specifically, due to performance considerations, the OPC Server APIs frequently used, such as OpenSecureChannel, GetEndpoints, and FindServers, do not undergo whitelist authentication. Therefore, in CVE-2021-27432, an attacker could make a forgery of itself as an OPC Client and initiate a FindServersRequest to the server without whitelist restrictions, while enclosing nested OPC variables in the request. This would cause the server's .NET Runtime to call the function too many times, eventually causing a stack overflow and actively shutting down the OPC Server. The OPC Server is the communication bridge between various pieces of factory equipment, and its shutdown would stymie the operation of the factory assembly line.

Another example is the control station of industrial robots. The Robot Operating System (ROS) is an application development framework designed for robots, and many robot suppliers provide drivers for this framework. However, the past design of ROS did not consider security, and previous studies found that an attacker lurking in the factory could easily execute FIN-ACK DoS attacks against the control station. Even with the ROS 2 framework (such as Universal Robots), it is still plagued by disruption attacks. The main reason is that ROS 2 uses Data Distribution Service (DDS) as the standard for data exchange (which adopts the publish-subscribe communication model). Through our joint research with other teams, we found that this standard has vulnerabilities for amplification attacks [Multiple Data Distribution Service (DDS) Implementations (Update A) | CISA], which can cause denial of service attacks against robots on the production line. Specifically, an attacker laying low inside the factory can disguise itself as a client and make a packet with an erroneous source based on the DDS architecture. When the control station provides this packet content to the endpoint devices it controls, these endpoint devices will respond with data to the affected robot to achieve an effective amplification attack.

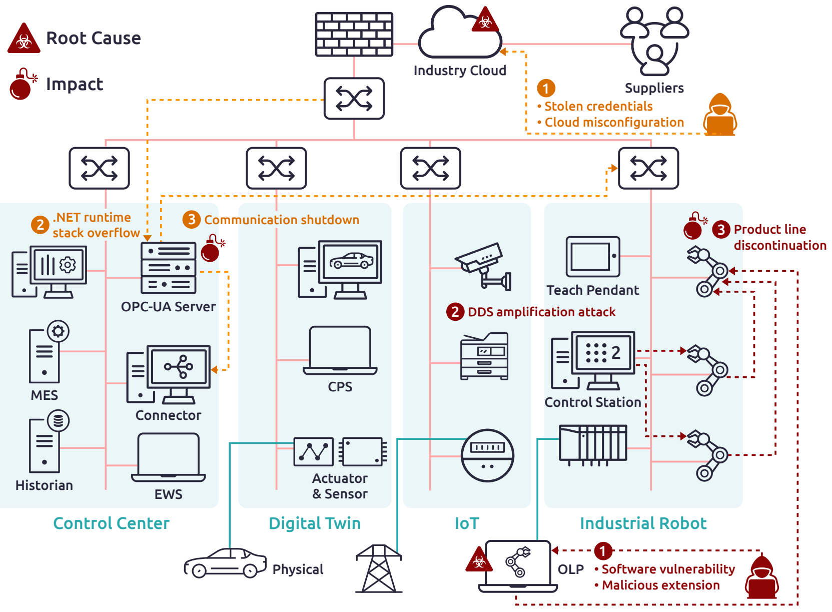


Figure 14: Obstructions to the Automotive Product Line

Corrupting the Automotive Supply Network

In March 2023, Tesla CEO Elon Musk unveiled the third part of his Master Plan at Investor Day, announcing a goal to transition the global economy to 100% renewable energy by 2050. In light of this, we examined numerous car manufacturing plants that use renewable energy and found that most of these plants rely on solar or wind power, which can be sourced through on-site generation or purchasing from local power plants. Therefore, these power technologies are essential components of the automotive supply network. However, we observed that the solar and wind power networks are mostly located in remote areas due to their inherent environmental limitations and lack of personnel management. For instance, in wind turbines, attackers can easily break physical locks to gain access to the control room. In addition, the control panel of wind turbines, which includes HMIs, controllers, and inverters, is connected to the backend SCADA system to provide power information. Attackers can exploit this connection to initiate a remote services attack and issue stop commands to all other wind turbines. Similarly, solar power devices, such as inverters, are also connected to the backend SCADA system to receive power information and control commands. If there are no proper security measures or data source restrictions in place, attackers can exploit the compromised inverters to issue control commands to other inverters and cause a widespread power outage.

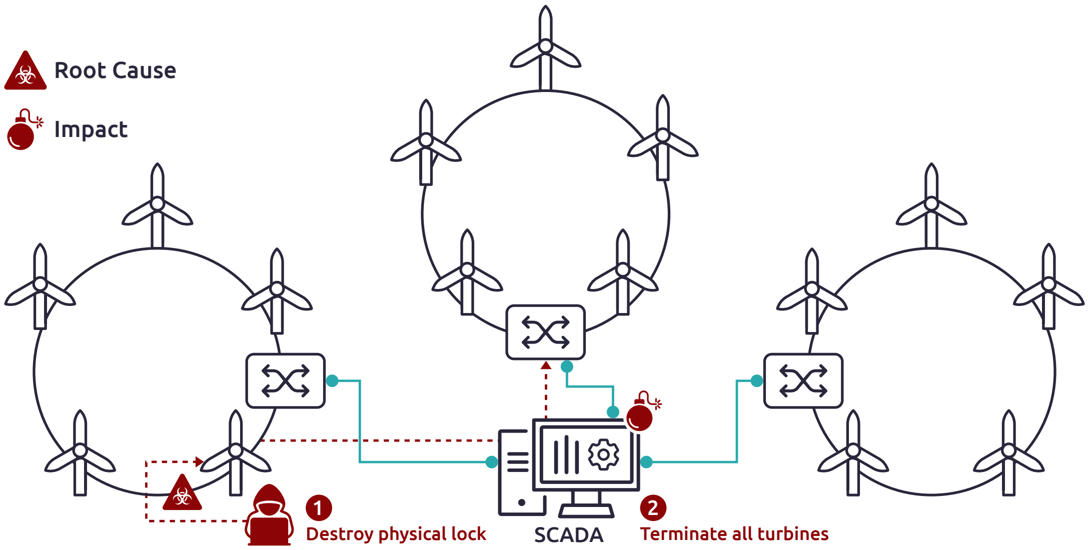


Figure 15: Wind Turbine Attack, Affecting Automotive Factory

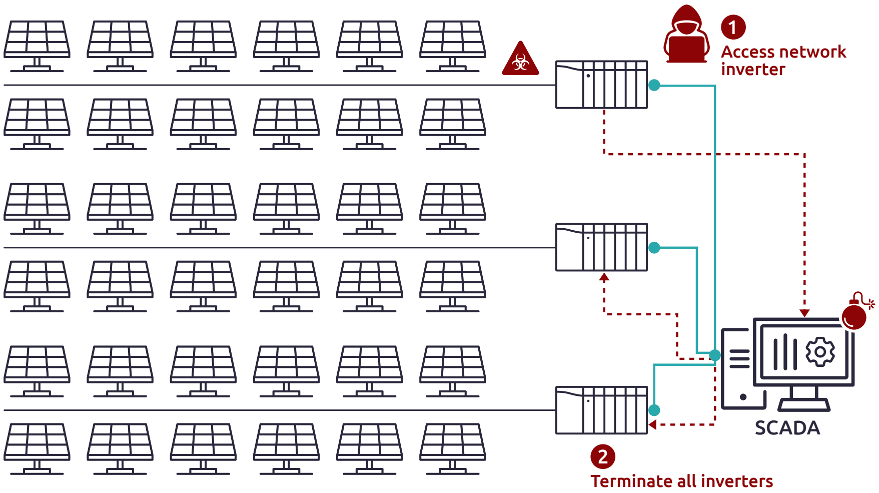


Figure 16: Solar Power Attack, Affecting Automotive Factory

Furthermore, after car manufacturing plants produce a large output of products, they transport them to other plants or dealerships via trains to increase efficiency and safety. The global market size of CBTC is expected to reach 2.76 billion USD by 2028, with a compound annual growth rate of 5.47% over the next five years.[8] However, the use of wireless network technology (IEEE 802.11) in CBTC makes it vulnerable to wireless compromise attacks, which is a possible initial contact point for attackers to access train systems. Attackers can use basic DoS attacks to severely impact the entire train system, which is responsible for train safety. Here we describe some DoS attack methods targeting IEEE 802.11:

1. **Management Frame Attacks:** Many management frames are not authenticated, allowing attackers to send deauthentication frames with forged MAC addresses, causing other clients to lose connectivity.

2. **Teardrop Attack:** A fragment packet can indicate an offset, allowing the receiving device to reassemble the entire packet. Attackers can design an offset value after the IP to cause the system to crash when unable to process the packet.

3. **WPA 802.1i Attack:** 802.11i is used to protect wireless networks, and its measures include closing a session for 1 minute if the WLAN AP receives more than 1 invalid MIC checksum and generating a new session key. Attackers can repeatedly send forged MIC checksums to freeze wireless services.

As a critical component of the automotive supply network, trains' suspension of operation due to security concerns may cause delays in the production process for car factories unable to obtain raw materials on time.

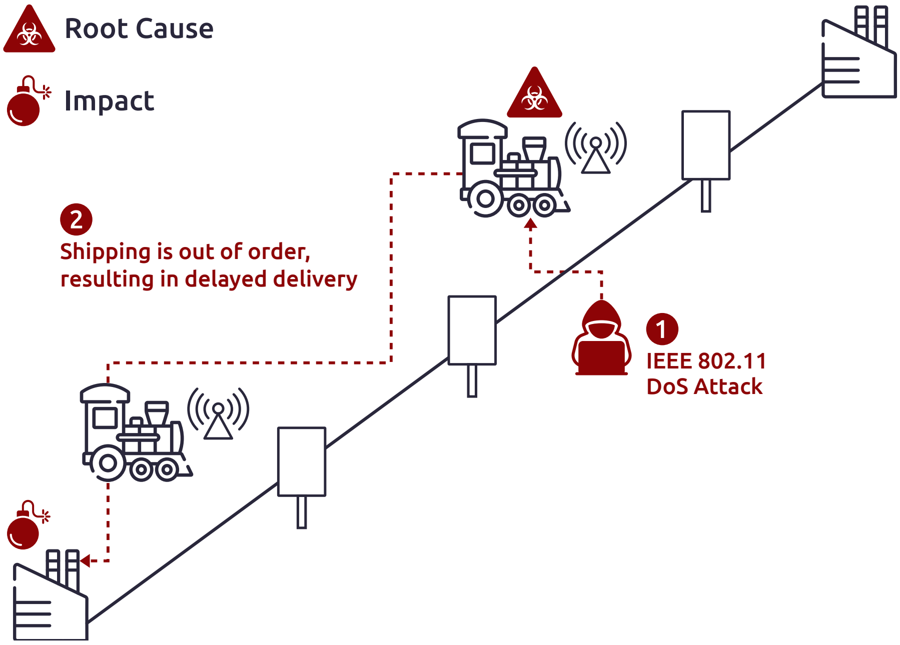


Figure 17: Train Attack, Affecting Automotive Factory

[8] MarketResearch, "Global Communications-Based Train Control (CBTC) Market Insights Forecast to 2028", MarketResearch, July, 2022.

An OT Zero Trust Approach for Automotive Factories

Cybersecurity is a new metric by which enterprises' quality is judged. In a manufacturing plant, you need to be able to adapt your system to current circumstances. Collaborative robots or interconnected robots that were trustworthy yesterday or five minutes ago may be compromised at any given moment. The OT zero trust approach can track and grant access based on the current situation and your security policies, providing complete protection for automotive factories. The four cornerstones of OT zero trust are as follows:

Inspect

Inspection is an essential step before integrating any asset into an automotive production line. The factory manager should proactively test and periodically audit each asset to create a record of OT health that proves the equipment is free of malware and has proper vulnerability mitigation. Attackers have previously launched cyberattacks and exploited the supply chain by compromising assets prior to shipment or during system maintenance.

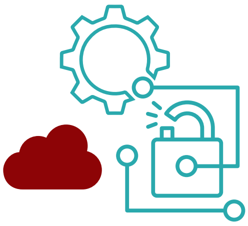
Proactive inspection and auditing involve taking a detailed inventory of all applications, firmware, operating systems, computer information, version numbers, and patch levels. This inventory is used for threat modeling to determine the likelihood of a known vulnerability being exploited and the potential consequences if it were. Even legacy equipment like standalone PCs running Windows XP, Windows 7, or Linux can be inspected, and air-gapped systems that were previously impossible to examine can also be inspected. Devices like TXOne Networks' Portable Inspector can run native scans or boot scans, depending on the asset's operating system.

Lock Down

Lockdown is crucial for providing lifetime protection of critical assets in automotive factories. Trust lists, also known as allow lists, are automatically generated from the inventory collected during the security inspection. This makes locking down endpoints easy because the security scan contains a list of all the files that are allowed to execute on the device. These trust lists are automatically updated during patching or maintenance to stay current and minimize downtime. For fixed-use assets like ticketing stations and on-board computers, Stellar is the ideal solution. Stellar's trust list based 4-in-1 lockdown excludes all unlisted applications from executing and all unlisted users from making changes to data or configurations, locking down applications, configurations, data, and USB devices. Only administrator-approved USB devices can connect to the device, and only an administrator can grant a device one-time approval to connect.

Endpoint protection solutions can enhance and ensure the integrity of computing devices, thereby protecting computing devices within critical OT systems from targeted attacks like APTs. Stellar monitors legitimate processes that are vulnerable to attacks under the control of least privilege by learning and authorizing normal operational behaviors. This gives Stellar the ability to detect abnormal operational behaviors and prevent malware attacks.

Segment



TXOne Networks recommends building segmented networks into the network architecture of automotive factories, as it greatly improves visibility and makes the system more resilient to network attacks. Network segmentation is set up on OT firewalls and OT IPS within the network and creates segments via carefully designed rules or policy sets. By routing network traffic through these segments, protection is increased without affecting workflow. OT-specific intrusion prevention systems (IPS) can analyze network traffic and prevent malicious packets from entering, moving laterally, or collecting information needed for an attack. In summary, using next-generation OT IPS technology can help automotive factories establish network segmentation strategies and controls designed with OT zero trust. For example:

- **Network segmentation strategy and access control:** In an automotive factory, OT IPS can check all traffic entering and exiting the factory network with excellent protocol sensitivity. Its minimal delay ensures optimal speed for data transmission while maintaining protection. These rules can filter files or segments based on protocols commonly used in the industry, such as Profinet or OPC-UA. Some OT IPS provide deep traffic analysis and can filter based on control commands. Some OT firewalls and OT IPS can even filter IT protocols such as HTTP or SMB. In addition, access points (APs) that are commonly used for wireless networks in automotive factories often operate with limited or almost no security. If someone uses an unmanaged device in the factory network environment, they can find the access ID of the AP and attempt to gain access, thereby affecting production line control computers. EdgeIPS is ideal for deployment between APs and their switches to prevent them from being compromised.

- **Anomaly detection:** When attackers attempt to exploit unnecessary network services or vulnerabilities to infiltrate factory networks, implementing specific traffic rules using firewall or IPS appliances can make attacking the factory's OT network more challenging. The EdgeIPS series features a comprehensive allowlist for devices, protocols, and operations, employing the OT least privilege principle to minimize the OT attack surface, restrict OT network attacks, enhance operational performance, and mitigate the impact of human error. By implementing fine-grained access control at different levels, businesses can strike a balance between availability and security while safeguarding critical data and systems.

- **OT security visualization:** The core of OT zero trust is continuous monitoring, with centralized OT defense consoles providing direct monitoring of the security of your industrial control system. The OT defense console combines outputs from multiple sources and uses alarm filtering technology to distinguish between malicious activity and false alarms. Enterprise can see that security controls protect all ICS assets in daily operation. As network events unfold, you will receive alerts for any violations. This bird's-eye view also reveals shadow OT, which refers to hidden rogue devices that may compromise your network security. Cybersecurity engineers can use the OT defense console to remotely manage large-scale deployments of OT IPS and OT firewalls. It acts as a secure portal for virtual patches, preventing known malicious software signatures and stopping them before most attacks start. Additionally, the defense console allows administrators to edit OT protocol allow lists so that critical production machines can work together. It provides powerful and flexible reporting from log files, and tracks the data needed for policy implementation, protocol filters, node groups, systems, audits, and asset detection.

Reinforce

Ensuring the continuous operation of automated equipment in an automotive factory is crucial to avoid significant financial losses. Factory managers must take proactive measures to apply security patches and updates to the operating systems, applications, drivers, and firmware of critical network systems. However, sometimes technology suppliers may not release patches in a timely manner, or the system may no longer receive update services. In such cases, we believe that using virtual updates is an alternative method to protect devices that are difficult to update.

For example, when a factory is in the middle of production, virtual updates can prevent known vulnerabilities in the MES from being exploited without interrupting the production process. The vulnerabilities can be patched after the production run or at another appropriate time, allowing the automated factory to continue operating seamlessly.

It is essential to note that virtual updates are not a replacement for actual security patches and updates. Still, they can be a useful stopgap temporary measure to maintain the security and availability of critical systems until a permanent solution is available. Additionally, virtual updates should be tested thoroughly in a controlled environment to ensure they do not cause any unintended consequences or disruptions to the production process.

Conclusion

Based on past cybersecurity incidents within the critical manufacturing sector, it is safe to say that the automotive industry supply chain is particularly vulnerable to cyberattacks. With the push towards digital transformation in automotive manufacturing, the threat landscape for factories has expanded and become even more complex. Common digital transformation applications in car factories, such as industrial robots, industrial clouds, digital twins, transportation, and renewable energy technologies, offer opportunities for attackers to gain initial access to the factory network and cause serious disruptions in the production of automobiles. These disruptions not only result in significant financial losses for car manufacturers but can also lead to delays in research and development, preventing them from gaining a crucial competitive edge in the fast-paced automotive industry.

To address the unique and evolving defense needs of OT/ICS workplaces, we propose an OT zero trust approach for digital transformation in automotive manufacturing. By adopting a cyber defense perspective throughout the asset lifecycle, factory managers can deploy more comprehensive and automated OT zero-trust cybersecurity solutions to establish secure supply chains, protect both modern and legacy endpoints, and implement complex cyber defenses. This approach simplifies compliance with cybersecurity regulations, enhances the resilience of the network and endpoints, and minimizes the impact on machine operations in the production line.

txone.com