Arthur D Little

Viewpoint

Demystifying the Internet of Things for secure industrial transportation systems

The IIoT promises major efficiency gains, especially in industrial transportation. However, if not properly designed, it may become a major safety issue

The Industrial Internet of Things (IIoT) is the enabling technology for industrial transportation companies to build the foundation for differentiating solutions and to create the mobility of the future. However, when deploying such innovations at the interface of information technology (IT) and operational technology (OT), these advancements come with a caveat as they open new cybersecurity risks across entire transportation systems.

Leveraging the IIoT to capture the full value of data

The nature of industrial transportation has been evolving rapidly in recent years as sensors, networks, and other infrastructure components have become increasingly affordable. This enabled transportation companies to implement and scale Internet of Things (IoT) solutions, yielding vast benefits through efficiency gains in how transportation systems are operated, and in the process generating large amounts of data. Advanced analytics can leverage this big data to achieve intelligent and self-adaptable vehicles and infrastructure.

The main goal of using big data in industrial transportation is to examine transportation system variations and disruptions to predict system performance over a given timeframe. Once predictions can be made – e.g., when a specific part of a vehicle will require maintenance – prescriptive recommendations can be derived. In one such example at a railway operator, the system could not only predict a train component's failure, but also recommend the time and place for the train's maintenance operations that would create minimal impact on the running system.

The increasing implementation of sensors and actuators into transportation networks has enabled the virtual representation of processes and vehicles – i.e., via a digital twin – and further accelerated growth in data volume. The simultaneous development of advanced analytics and the IoT is only natural, and, when combined, they yield huge efficiency gains. The natural progression from the Internet to the IoT, to the IIoT has sparked further developments in all industrial transportation sectors. The upside expected for deploying the IIoT, especially in combination with advanced analytics, is huge from both a financial and a capabilities point of view.

The increasing connection of physical assets creates multiple risks

The IIoT is already being applied within the industrial transportation sector, impacting operating and business models and forcing executives to challenge their businesses' status quo. Nonetheless, many corporations face challenges when implementing IIoT solutions in their organizations, mainly due to the complexity of facilitating adequate security measures.

Cybersecurity has high criticality within the industrial transportation sector, as security directly correlates with safety. Failures or breaches in industrial transportation systems can lead to dramatic reaction chains; for example, a failure of a sensor controlling a railway level crossing can have dangerous outcomes.

The following are some notable examples of such cybersecurity failures:

- In 2008, a 14-year-old Polish student hacked the local tram system of the city of Lodz. He was able to remotely control trams and have them change tracks, in the process derailing four trams and injuring a dozen people.
- In 2017, a European shipping giant was infected with ransomware, suffering a financial loss of US $200 million-$300 million, as the company had to shut down many of its operations to prevent the spread of the virus.
- In 2020, one of Canada's largest trucking companies was infected with ransomware. While this company decided against paying the hackers for the stolen data, the internal data was posted online shortly after the attack, making it accessible to everyone.

The most prominent cyberattacks in the transportation sector largely focus on ransomware or malware infections. This is also highlighted by the report "Top 10 threats to industrial control systems and factory automation" issued by the German Office for Information Security (BSI) in 2019. In its report, the BSI identified 1) infiltration of malware via external hardware, 2) malware infection via the Internet, and 3) human error and sabotage as the top threats to industrial control systems. These findings illustrate the increasing need for industry-specific cybersecurity measures within the industrial transportation sector.

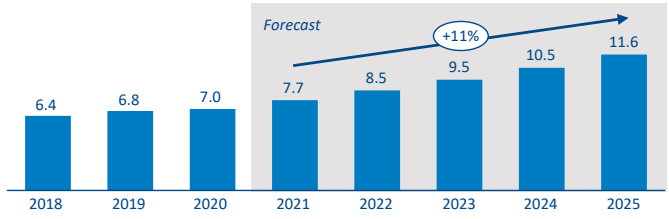
Obstacles to developing a secure IIoT

The IIoT must deal with large and diverse quantities of data, since it consists of distributed, asynchronous systems. To cope with the nature of the IIoT system, autonomous reactions are required, making decentralization necessary as it would be difficult for a central unit to keep track of every aspect. This distributed nature of the IIoT creates potential for cybersecurity attacks since the entire system can be infected from a single compromised entity. In its analysis of IoT devices in US enterprise IT and healthcare organizations, Palo Alto Networks notes that 98% of all IoT device traffic is unencrypted, while 57% of all IoT devices are vulnerable to medium- or high-severity attacks.

Therefore, the resulting increase in spend on cybersecurity within the industrial transportation sector is projected to exceed 11 billion euros by 2025 (see figure below), highlighting the sector's growing demand for cybersecurity.

Three main obstacles to designing a secure IIoT exist: 1) economics, 2) technology, and 3) the workforce.

Global cybersecurity spending by industrial transportation companies (in billions of euros)



Source: Arthur D. Little analysis

Economics conflicts with customer behavior, as security is a hygiene factor in industrial transportation. Customers, who expect safety and security, are not willing to pay additional fees for a running system. Elaborate security measures obviously bring economic factors into play. Many transportation executives are facing the question of how much they should spend on such initiatives.

The ever-increasing number of IoT devices set to be operating within the industrial transportation system necessitates a reliable technical infrastructure. For efficient data transmission, the IIoT requires fast and reliable Internet connections over varying distances to leverage low latency (the time interval between stimulation and response); inefficient data transmission can jeopardize IIoT security.

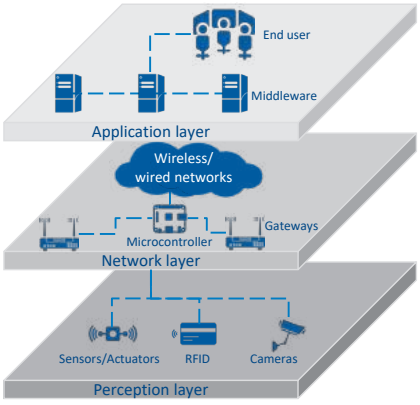
Having a workforce with relevant skills is one of the largest obstacles industrial transportation companies face when designing a secure IIoT. IT, telecommunications, robotics, electronics, and industry-specific know-how are required to varying degrees, while keeping the economic constraints in mind. The human factor is a large determinant of success or failure when designing an IIoT system.

Designing a secure IIoT

To conduct any type of analytics, data must move around the organization. Organizations have traditionally approached network design with a client-server architecture to distribute computational power and data storage across resources. However, mature IIoT devices have greater capability to process computing power closer to the actuator or sensor, at the edge of a network, commonly referred to as edge computing. An edge computing design distributes computational power across the entire network infrastructure, enabling devices to directly interface to the cloud. In turn, data centers can run more efficiently, as most computation is conducted outside the data center. However, while edge computing is an enabler for an IIoT solution, it also opens the door to a vast array of potential cyberattacks, as an entire system can be infected from a single compromised entity, as noted previously.

A high-level IIoT architecture consists of three layers: 1) perception (acquisition of data), 2) network (distribution of data), and 3) application (leveraging the data) (refer to figure below).

Three-layer IIoT architecture

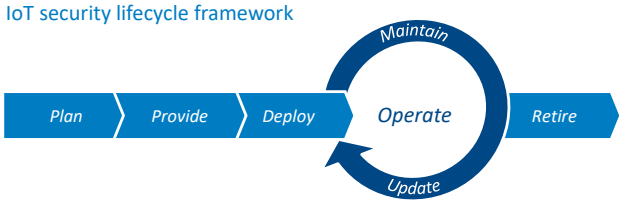


Source: Arthur D. Little analysis

The perception layer consists of RFID tags, sensors and actuators, and other elements that aim to collect data by identifying objects and their conditions. The network layer distributes data in real time from one endpoint to another, namely, from sensors to data centers. Microcontrollers – ruggedized computers controlling entire processes – act as mediators by exchanging information between "things" and people. The application layer provides services based on the collected data, processing and analyzing it to allow people to interact with it and, thus, provide a value add.

Throughout a secure IIoT architecture, both devices and the network itself must be considered holistically. This approach yields a security lifecycle framework, which is shown in the figure below.

IoT security lifecycle framework



Source: National Institute of Standards and Technology (NIST), Arthur D. Little analysis

Planning: The first step in developing any IIoT system is the planning phase, to comprehensively design and conceptualize the overall IIoT landscape and to define requirements for all subsequent phases. Although proper planning takes time, it is worth the effort.

Provisioning: The provisioning phase is when the required IIoT equipment is ordered and evaluated, to meet the defined requirements of subsequent phases. Component replacement is often complex and sometimes requires a shutdown of the respective system, which can lead to costly downtime. Keep in mind that the most expensive compromises are those concerning security requirements.

Deployment: Once the received IIoT components meet the specific requirements, they must be properly installed and tested to ensure security. Before activation, many components require newly set up digital identities, including credentials.

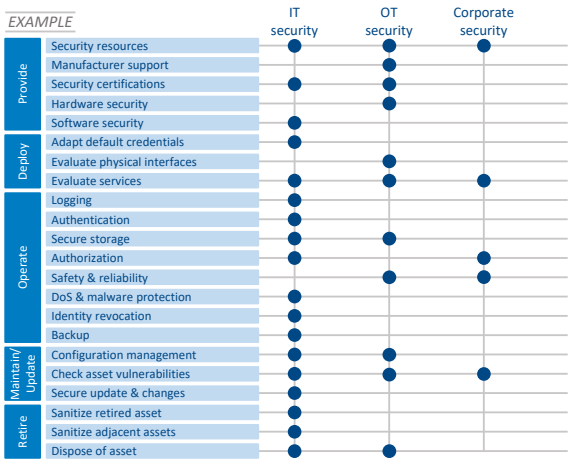
Operation: Once IIoT equipment goes live, it enters the main stage of its lifecycle. Operation makes up the longest and most vulnerable phase of a component's existence since it is exposed to outside threats and failures. Component operation needs to be continuously monitored and evaluated for deviations from the norm.

Maintenance & Updates: Components are subject to wear and tear and, thus, must undergo maintenance from time to time. Maintenance processes must be closely aligned with the overall IIoT system to ensure that no new vulnerabilities are created when components again go live. Furthermore, security should be a process, with systems updated on a regular basis to maintain state-of-the-art capabilities for functionality and security. Care must be taken with each update to ensure that no additional weak spots are created in the system.

Retirement: Even when the lifespan of components and systems has ended, security must be a consideration. Therefore, when disposing of or reusing any part of the system, the security of the remaining IIoT system must not be affected in any way.

After the initial planning phase and once the subsequent requirements have been derived for the entire IIoT security lifecycle, a security checklist can support relevant functions along the IIoT security lifecycle framework.

IoT security checklist based on the IoT security lifecycle framework



Source: National Institute of Standards and Technology (NIST), Arthur D. Little analysis

Our experience has shown that it is vital to the success of securing devices and infrastructure assets to collaboratively develop such a security process among all relevant stakeholders, namely IT security, OT security, and the corporate security division. A comprehensive security process can only be successfully developed and implemented by collaborating across security departments and avoiding silos. Our sample checklist provides an example, but each company's security approach needs to be tailor-made.

Case Study: IIoT-enabled predictive maintenance in the railway industry

Background

A major European railway company identified unplanned wheelset maintenance events as one of the main causes of train cancellations. Furthermore, these unplanned maintenance events accounted for a large portion of all maintenance costs. The main issues leading to these were a lack of transparency into current status, manual planning processes, and limited workshop capacity.

IIoT solution

The railway operator developed a digital twin displaying the current status of wheelsets with recommendations for optimal maintenance times. Hot box detectors enabled the identification of temperature deviations in the wheels to take immediate actions in case of limit-value violations. As a result, the railway operator was able to decrease train delays and maintenance costs, while increasing passenger safety.

Security considerations

When designing an IIoT solution in the railway industry, one of the main issues is that the infrastructure is distributed across vast geographical areas, making sensors and computational entities vulnerable to outside influences and potential cyberattacks.

Once the railway company data reaches the interface to the public wireless internet, the mobile network operator ensures security via appropriate cybersecurity protocols. However, when processing the data on the edge – in this case, on the computational devices on the trains and railway tracks – the railway company is responsible for ensuring adequate security and fail-safe measures. Thus, data protection services are required, which can include firewalls and encryption across the network. This is particularly important at strategic nodes, i.e., when data is transitioning from the private network into the public wireless internet.

Results

By applying the IIoT security framework and bringing together all relevant stakeholders, true end-to-end system security was achieved. The security process combined vehicle security, encryption, and network security measures for a comprehensive approach. By treating security as a process, the railway operator developed an awareness of IIoT security.

Conclusion & vision

The IIoT connects physical assets with the Internet in an industrial environment, enabling the connection of the physical and digital worlds. The connection of physical processes with computing capabilities is not new, as embedded systems are a well-established concept. However, such systems have usually been in closed environments, not exposing the computational capabilities of devices to the outside world. This exposure of physical devices to the Internet has sparked an explosion in device numbers and connections. The increasing number of connected devices expected in the future will challenge industrial transportation companies from a cybersecurity perspective, as keeping track of these devices and securing them is a complex task due to their ever-moving nature.

Asset management needs to be fast and reliable in monitoring a large number of moving devices to quickly identify compromised assets and revoke their identities. However, identifying compromised devices is only the second line of defense. Our experience has shown that physical protection of transportation sector devices and networks is key to a secure IIoT. Edge computing provides increased security and, thus, safety for the IIoT by reducing latency and enabling data centers to run more efficiently, as data is in large part processed on the edge. Combining the IIoT with advanced analytics will be the key differentiating factor in developing innovative solutions for new services and efficiency gains across existing operations. Furthermore, to enable autonomous transportation services and intermodal transportation in the future, it will be of upmost importance to secure the infrastructure as well as the devices. A key lever to achieve this will be the provision of real-time alerts and the quick deployment of countermeasures in the event of security breaches.

Contacts

Austria
virag.bela@adlittle.com

Belgium
vanoene.frederik@adlittle.com

China
harada.yusuke@adlittle.com

Czech Republic
steif.jiri@adlittle.com

France
bamberger.vincent@adlittle.com

Germany
doemer.fabian@adlittle.com

India
maitra.barnik@adlittle.com

Italy
caldani.saverio@adlittle.com

Japan
harada.yusuke@adlittle.com

Korea
lee.kevin@adlittle.com

Latin America
casahuga.guillem@adlittle.com

Middle East
kuruvilla.thomas@adlittle.com

The Netherlands
kolk.michael@adlittle.com

Norway
thurmann-moe.lars@adlittle.com

Poland
baranowski.piotr@adlittle.com

Russian Federation
ovanesov.alexander@adlittle.com

Singapore
harada.yusuke@adlittle.com

Spain
ali.salman@adlittle.com

Sweden
glaumann.martin@adlittle.com

Switzerland
doemer.fabian@adlittle.com

Turkey
baban.coskun@adlittle.com

UK
thuriaux.ben@adlittle.com

USA
vanderschaaf.ben@adlittle.com

Authors

Fabian Claudy, Philipp Mudersbach

Arthur D. Little

Arthur D. Little has been at the forefront of innovation since 1886. We are an acknowledged thought leader in linking strategy, innovation and transformation in technology-intensive and converging industries. We navigate our clients through changing business ecosystems to uncover new growth opportunities. We enable our clients to build innovation capabilities and transform their organizations.

Our consultants have strong practical industry experience combined with excellent knowledge of key trends and dynamics. ADL is present in the most important business centers around the world. We are proud to serve most of the Fortune 1000 companies, in addition to other leading firms and public sector organizations.

For further information please visit **www.adlittle.com** or **www.adl.com**.

www.adl.com/IndustrialTransportIoT