Authors:

Mario Ayala, BayFirst

Rob Cantu, CTIA

Richard Holder, Department of Homeland Security

Jeff Huegel, AT&T

Niten Malik, Microsoft

Michalina M, United States Government

Adrienne Raglin, U.S. Army Futures Command

Ashley Reichert, Illinois State Police

Ash M. Richter, In-Q-Tel

Kimberley Sanders, Amtrak

Acknowledgments:
The team would like to thank the 2019 Public-Private Analytic Exchange organizers Tammy Padilla, Anita Prichard, Jessie Ramsdell, and their team, our assorted offices, families, and friends, and especially our colleagues in the field who acted as valuable resources volunteering their time to discuss the topic.

Please note: That the opinions expressed within are representative of the individual authors.

Contents

Executive Summary 3
Foreword & Forewarning 4
Section One: Opportunities 5
A Brief Overview of the IIoT Landscape 5
Leveraging Next Generation Technology 8
The Next Gen Landscape 8
Next Generation IIoT Use Cases 11
Interconnected Smart Cities 16
Section Two: Risks 19
IIoT Risk Overview (IIoT) 19
Nation-State Adversaries 19
Criminal and Non-State Actors 20
Supply Chain Risks 21
Risk and Vulnerability Mitigation and Management 21
Section Three: Mitigation 23
Government Efforts to Secure IIoT 23
I: Silicon Valley Innovation Program (SVIP) 23
II: The National Cybersecurity and Communications Integration Center (NCCIC) 24
The National Cybersecurity Assessments and Technical Services (NCATS) 25
Validated Architecture Design Review 25
Industry Efforts to address IIoT Risk Mitigation 26
Public-Private Collaborative Efforts 30
References 31

Core Questions Addressed Herein:

What is the impact of current and future applications and uses of the IIoT on U.S. critical infrastructure/U.S. national security?

What opportunities and risks will a greater confluence of IIoT yield?

What opportunities exist to mitigate cyber risks?

Executive Summary

There are driving pressures in the marketplace for efficiencies, and these pressures extend to critical infrastructure sectors including the electrical grid, telecommunications, and finance—some of the most essential critical infrastructure sectors. Industrial Internet of Things (IIoT)—also referred to as Industry 4.0—deployment is meant to provide additional capabilities at a lower cost. Today a suite of low-cost, energy-efficient sensors with wireless connectivity combined with cloud-based analytics are on the market. These sensors offer new capabilities and cost efficiencies, lower pollution, and offer interoperability that turns into revenue for corporate growth. IIoT adoption leverages many other new technologies, such as LTE, 5G, Wi-Fi and other wireless connectivity technologies; the cloud for analytics and storage; and innovations in battery and solar technologies to enable near-universal placement, connectivity, and power for any IIoT device.

The risks associated with IIoT deployment are well documented in the IT space. There is extensive interest from states and criminals looking to infect these new ecosystems. There are also supply chain risks as IIoT devices are upstart efforts in some cases and have less robust cybersecurity and testing of their electronic components, firmware and software. There is also less rigor in how businesses and utilities might use a device, which is often not for the intended use.

Because of these risks to components, firmware and software, wireless connectivity, and the fact that most devices are always on, mitigations are needed at the device and systems engineering level. The government is addressing some security aspects in the innovation space around IIoT. Governments continue to seek industry inputs and review the marketplace for possible mandatory steps regarding securing IIoT devices and their ecosystems. The U.S. National Institute of Standards and Technology (NIST) and the European Union Agency for Cybersecurity (ENISA) are both attempting to bring guidance to government and direction to industry with some of their voluntary efforts to define IIoT cybersecurity. Industry is working with original equipment manufacturers (OEMs) and other manufacturers to develop good security capabilities in IIoT devices to avoid burdensome regulations that will likely become antiquated quickly as the IIoT marketplace is broad and evolving much faster than government legislation. Industry and government efforts are mainly focused on securing hardware, protecting data, and privacy issues.

Foreword & Forewarning

Why are we worried about the industrial internet of things? Isn't connectivity a good thing? Doesn't it yield even greater optimization of the infrastructure systems that run our daily lives? Won't it save us time, energy, and money if industrial systems talk to each other? Isn't ambient intelligence the cybernetic future of our systems of systems? Yes. Undeniably so.

But there are risks with every great leap forward in a civilization.

And while connectivity of our cyber-physical systems can and will be helpful to society at large, it also creates an even greater cyberattack surface.

If states were to breach current protocols and apply direct pressure on each other's critical industrial infrastructures the results would be devastating.

A country without power would be in a tough spot. We might be able to overcome the absence of some systems—like our traffic lights and home lighting—by reverting to earlier technologies. But in the short time humanity has had electricity, it has become substantially dependent on it for its core economic functions. No power means no banks, no stock market, and no retail activity. With commerce internally and externally at a halt, a nation's earning and buying power would be decimated and the long-term trickle effects of limited access to food and other resources would be extraordinarily painful. Consider even one of our most basic human needs—water. Entire civilizations have crumbled without access to water.

These are the types of systems that the industrial internet of things touches—base pieces of critical infrastructure that are increasingly being digitalized. Digital connectivity means extraordinary leaps in optimization and the potential to expand our cities and keep pace with the rate of human urbanization and expansion.

Digitalization and greater connectivity—especially where it intersects with critical infrastructure—must be protected. Its implementation, growth, and maintenance must be carefully planned and safeguarded.

Section One: Opportunities

A Brief Overview of the IIoT Landscape

By the end of 2019, over 27 billion devices are expected to be connected as part of the vast confluence of technologies, platforms, protocols, standards, and devices known as the Internet of Things (IoT). The IoT is a network of computers and devices that collect and share large amounts of data, which is then sent to a cloud-based service where it is aggregated with other data and subsequently shared with end-users to provide useful insights. The IoT is increasing automation in homes, schools, stores, and a variety of other sectors and industries.

The Industrial Internet of Things (IIoT) leverages many of the same technologies as IoT and applies them to the complex needs of industrial environments. IIoT is a group of technologies that collect and transmit data within traditionally isolated industrial devices found in Supervisory Control and Data Acquisition (SCADA) systems and other Industrial Control Systems (ICS) that monitor and control industrial critical infrastructure that includes factories, power plants, water systems, ports, and other industrial facilities, as well as certain U.S. and allied military systems.

- Critical infrastructure asset owners and operators are increasingly embracing the IIoT to enhance efficiency and optimize productivity, but technology also introduces increased cyber and other vulnerabilities.

- With increased IIoT adoption, traditionally insecure and isolated legacy systems are comingled with new connected devices against the backdrop of disparate, but growing, device security guidelines. This presents more opportunities for device access and subsequent critical infrastructure computer network access by a variety of malicious cyber actors.

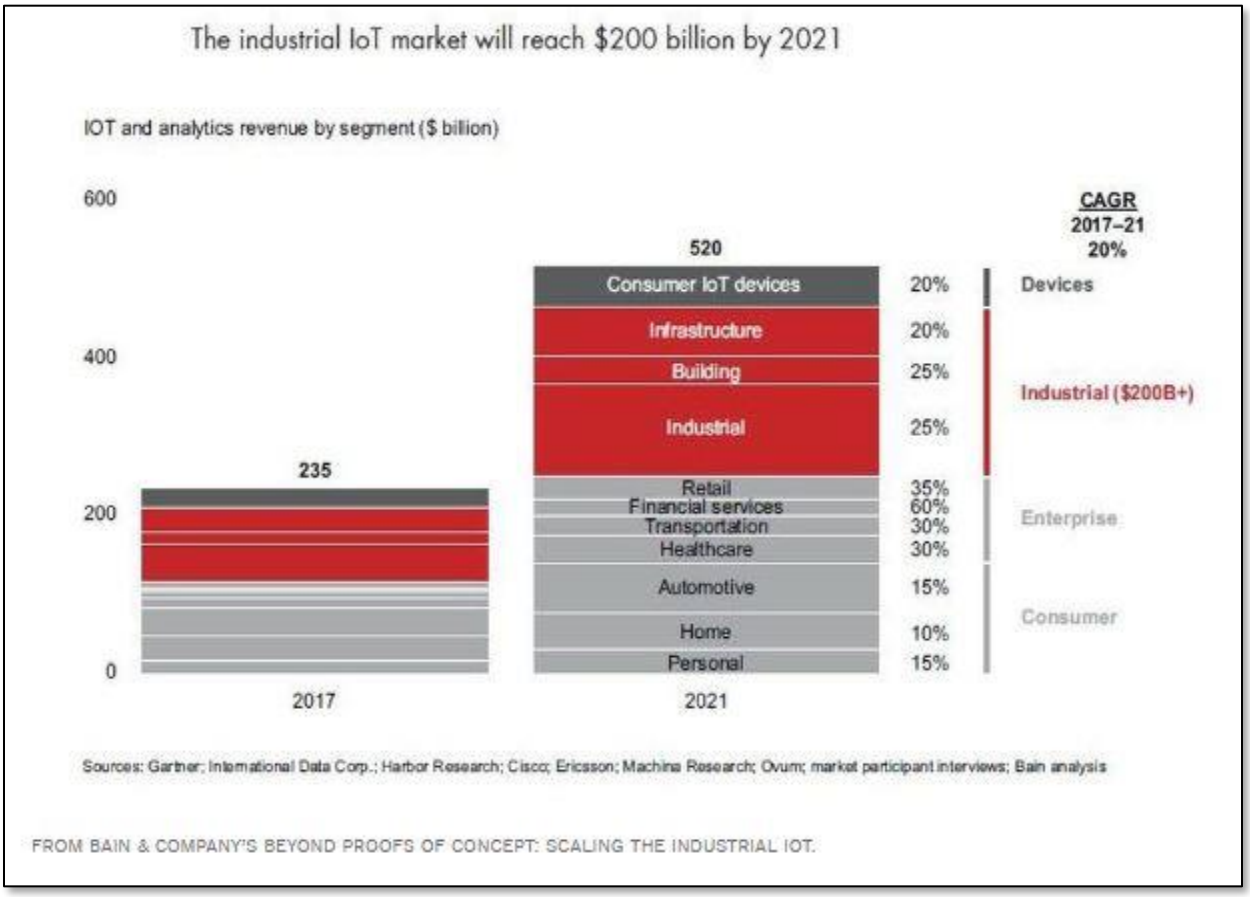
- The increase in publicly and commercially available cyber tools is making it easier for more actors to gain access to vulnerable IIoT components found in critical infrastructure, allowing them to pursue a variety of effects that may not be detected or those that might have financial and potential physical consequences.

Critical Industrial Infrastructure Embracing Digitalization

Critical industrial infrastructure owners and operators are increasingly adopting IIoT technologies to optimize production and delivery of products and services, increase efficiency, improve safety, and cut costs. IIoT sensors and devices provide operators with real-time monitoring and control and also collect data on device performance, which can be further exploited to optimize plant or production performance. For example, smart instruments used on a production line could allow a company to track and analyze their production process, real-time production data could provide insight into plant conditions or uncover additional capacity in a plant, and predictive analytics could help detect corrosion inside a refinery pipe.

- The IIoT is gaining appeal in industries that are geographically dispersed or have facilities or infrastructure located in remote or hard-to-access locations, such as oil and gas operations or renewable energy facilities (Bain.com, 2019) because IIoT technologies enable real-time remote monitoring and control. (Gold, 2019)

- In a Harvard Business Review survey of global industry executives, 74 percent of respondents said that IoT (to include IIoT) technology will become a competitive differentiator within two years, noting that they expected IoT to enhance customer service, improve the quality of products and services, develop new products and services, and reduce operational costs, as the top likely benefits. (Accelerating the Internet of Things Timeline, 2019)



- The IIoT market is outpacing the consumer IoT market and will likely overcome existing adoption barriers to grow into a $200 billion market by 2021, fueled by increased IIoT applications in the manufacturing, infrastructure, building, and utility sectors. (Scallehn, 2019)

- Alongside the adoption of the IIoT, some critical industrial infrastructure firms and utilities are increasingly connecting or converging their Information Technology (IT)—internet connected networks used for a variety of business applications, such as e-mail, customer facing websites, or HR applications—with their Operational Technology (OT)—networks that monitor and control physical processes, including controllers, sensors, actuators, among others, in order to facilitate IIoT adoption, data transmission, and analytics. ICS cybersecurity experts have often recommended segmenting or "air gapping" these networks to limit potential unauthorized access and protect the most critical operational components. (iScoop, IT and OT Convergence--Two Worlds Converging in Industrial IoT, 2019)

Leveraging Next Generation Technology

The Next Gen Landscape

To enable a hyper-connected environment in real-time and on a large scale requires wireless network technologies with lower latency, greater reliability, scalability, security, and ubiquitous mobility. Future enhanced mobile broadband technologies, such as 5G, will enable large-scale applications across factories, plants, utilities, and other critical industrial infrastructures. As IIoT becomes more widespread and smart city and smart factory ecosystems emerge, they will generate large amounts of data that will require significant computer processing speed and data storage capacity. Advanced data analytics, optimization, and visualization capabilities are required to maximize IIoT benefits and enable a robust security posture—thus entangling additional vulnerable levels of artificial intelligence and spatial computing into the industrial internet of things.

Cloud Computing

The large amounts of data and processing required by the IIoT will also lead to growth in cloud computing. While cloud computing has a variety of defensive security features, such as the use of blockchain, cyber analytics, and encryption, cloud data storage has unique risks that are different from a localized computer network. Risks may include the ability for attacks to spread far beyond their initial target, dependency on external software that leaves users less familiar with their digital ecosystem, and difficulties in detecting unauthorized access could possibly allow malicious actors to inspect and learn about the system before they execute an attack.

5th Generation Mobile Communications (5G) Technologies

The realization of 5th generation mobile communications (5G) technologies over the next several years will provide expanded broadband capabilities of mobile networks and advanced wireless connectivity through high data rates, wide-area coverage, and deep indoor penetration. These features will allow hundreds of thousands of IIoT devices to be deployed per square mile and battery saving low-energy operations, facilitating the adoption of IIoT devices for highly critical applications that have demanding requirements for device reliability and availability such as those found in large and complex industrial applications. (iScoop, 5G and IoT: the Mobile Broadband Future of IoT, 2019)

- 5G has the potential to provide wireless connectivity for a wide range of different use cases and applications and in the long-term which might lead to the convergence of many different industrial communication technologies in use today, such as enabling direct and seamless wireless communication from the field or factory floor to the cloud. (iScoop, 5G and IoT: the Mobile Broadband Future of IoT, 2019)

Artificial Intelligence

Artificial Intelligence (AI) is a broad term that encompasses natural language processing, deep learning, speech recognition, computer vision, spatial computing and machine learning technologies. Leveraging AI capabilities helps industries maximize the data collected from IIoT. AI allows factory components to learn and autonomously alert, improve, and sometimes make decisions regarding their own operations. (AI: Making Sense of the Industrial Internet of Things, 2019)

- For example, AI can help factories better understand why a piece of equipment failed and offer potential remedies or help mining or energy companies locate minerals or petrochemicals to extract. (AI: Making Sense of the Industrial Internet of Things, 2019)

- Effective IIoT initiatives will need to provide a comprehensive set of services. These range from basic data analytics services, such as real-time dashboards and key performance indicators, to advanced services, such as predictive analytics. AI-enabled predictive analytics allow IIoT platforms to predict equipment maintenance and anticipate downtimes, enable equipment with auto-diagnostics features, and automated product quality controls. (Garcia, 2019)

- AI can also be trained to recognize security threats. For example, ICS cybersecurity firms are using algorithms to develop a baseline of traffic through critical networks and leverage machine learning—a subfield of AI—to passively monitor ICS environments in real-time to identify any anomalies, advancing current AntiVirus software capabilities. (Dragos Platform Components, 2019)

Spatial Computing and Augmented Reality Applications

Spatial computing is the confluence of geospatial and immersive reality systems with data visualization. Increasingly, the digital twins created for infrastructure layers at multiple levels is understandable not just as a two-dimensional data set of numbers in a spreadsheet, but in three dimensions. As more and more of every nation is 3D mapped at multiple levels (satellite, landscape, building, and street level an increasingly cohesive digital scaffold of multidimensional data exists to act as a base geospatial layer for mapping and visualizing in mixed reality.

For example, rather than a field technician mapping their power plant inspection to a blueprint on paper or even digitally in a basic 3D Computer Assisted Design system, the inspection can include a time-stamped 3D capture of their entire tour through the facility. The tour can be accompanied by augmented reality (AR) guides highlighting features within the power plant to the inspector and allowing them to annotate the virtual space around them with their notes for later reference in AR or through traditional means. AR inspections could also allow other experts to follow along and make contributions to a report in real time from a remote location. Given the cost savings associated with digitizing for performance optimization, safety, and insurance, industries including mining, oil and gas, and critical infrastructure have been some of the first to reliably roll out operational spatial computing. As 3D mapping of roadways becomes more ubiquitous for both the self-driving cars and the construction industry, and the use of spatial and cloud computing.

resources along with greater bandwidth and lower latency from 5G becomes prevalent, support for object detection and tracking in 2D and 3D will increase.

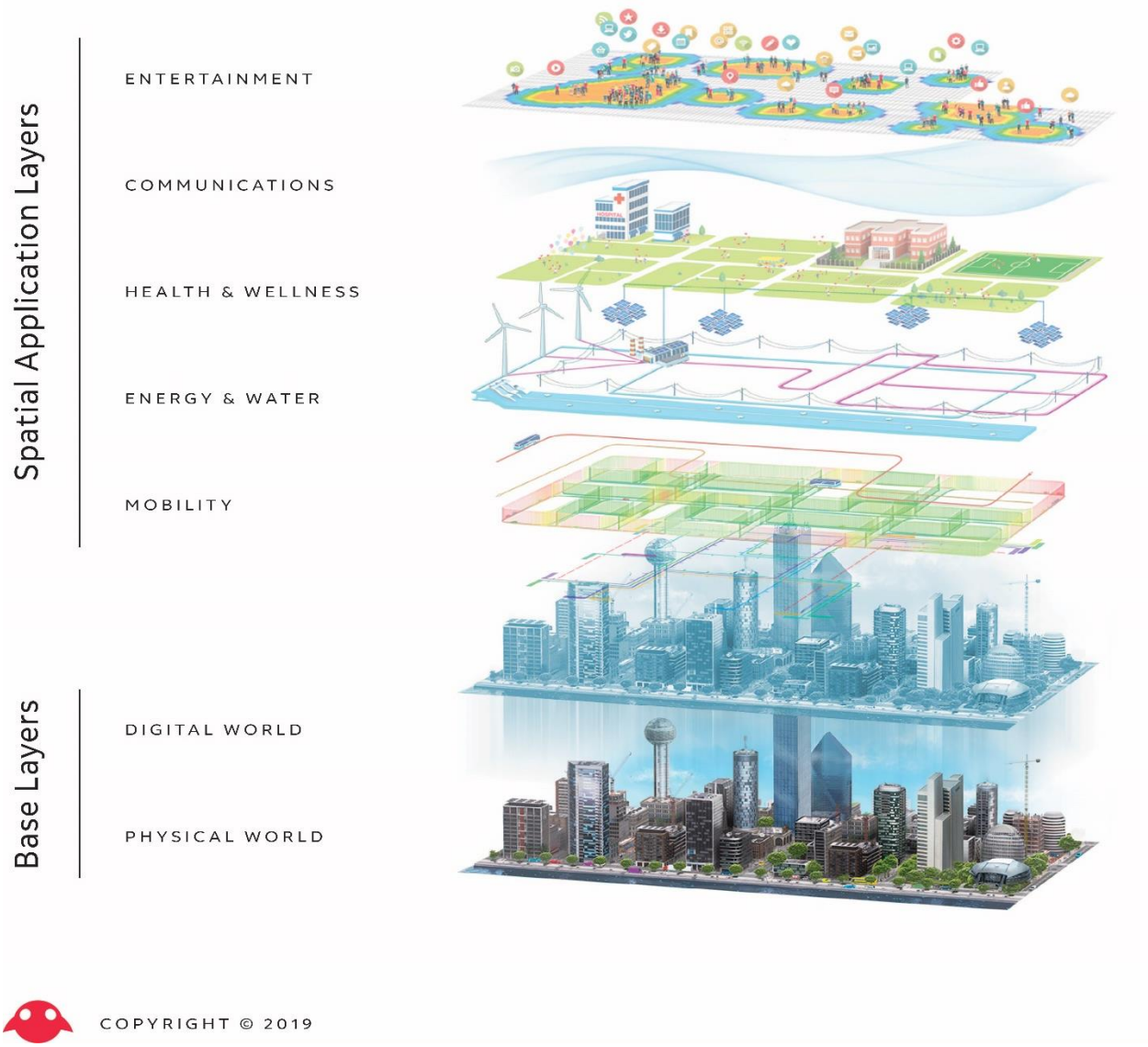


FIGURE 3: A version of the spatial computing world layers designed by mixed reality unicorn Magic Leap.

Next Generation IIoT Use Cases

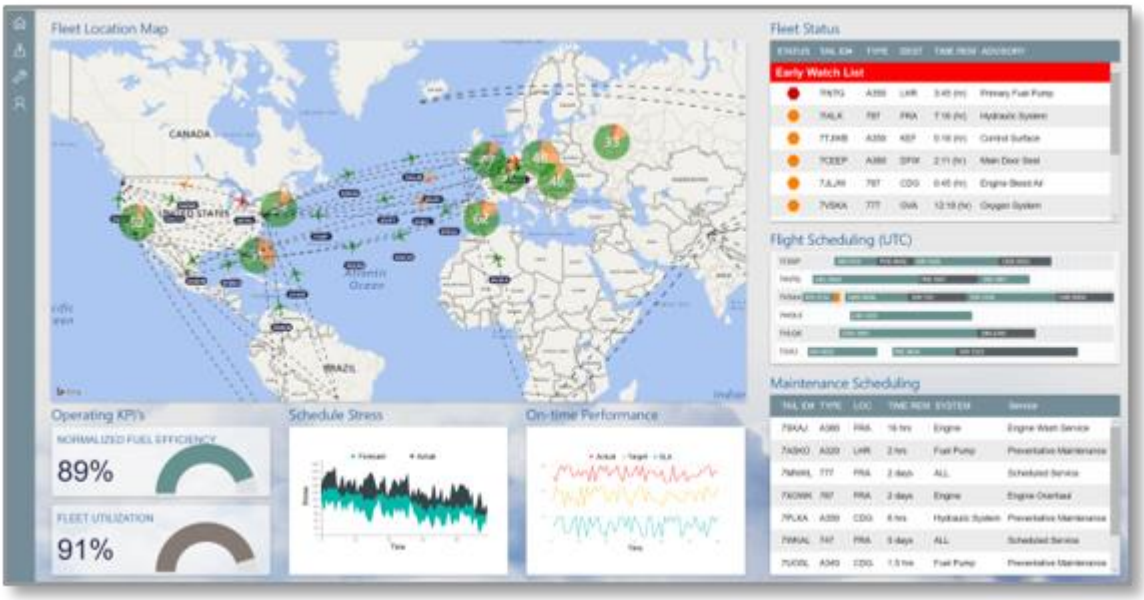
Smarter heating and cooling systems with cloud connected IoT solution

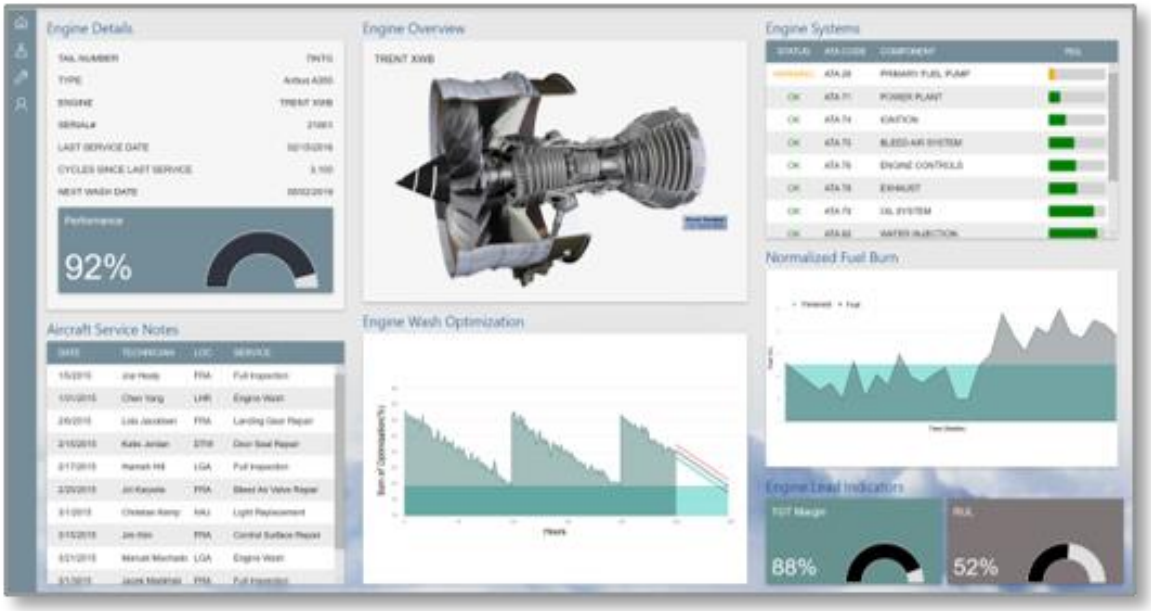
Smart thermostats like GLAS respond automatically to ensure that rooms are at the desired temperature. The sensors can detect airborne substances such as volatile organic compounds and carbon dioxide and collect other data, such as temperature and outdoor air quality data including allergen levels, the air pollution index, and UV levels, which is then presented to the user in an easily viewable format. The system continuously analyzes the data and alerts, homeowners and building managers, if air quality strays from desired parameters. [2]

Aeroengine as a Service

Airframe engine companies analyze millions of data points on the health of thousands of engines in operations globally. The data is used to build better engines, find emerging issues that can be proactively fixed before it results in flight delays or aircraft being grounded. Even a small reduction in "aircraft on ground" (AOG) time results in significant savings for the airlines.

By using IoT and cognitive services companies improve their customer service and add to the airlines' bottom line. For example, an unplanned delay or unscheduled maintenance can result in over $1 million per day in trickle-down costs for an airline. Fuel represents about 40 percent of an airline's operating cost and many factors impact this cost: flight path, weather, engine efficiency, and weight. Using sensors to aggregate data and find insights and trends provides airlines with concrete opportunities to clean the engine at the right time and save on fuel.





Rolls Royce CBM Dashbaord © Rolls Royce

The above dashboard shows the status of engine operations—current location, upcoming flight schedule, planned maintenance and maintenance capabilities at each ground location. We can also see operational metrics such as on-time performance, fleet utilization and schedule stress. Real-time data is analyzed with legacy and historical data. As soon as the aircraft lands, it uploads data to the cloud to be analyzed by Azure Machine Learning algorithms.

Microsoft Artificial Intelligence services help pilots decide how much fuel to take for the flight. Historical route analytics, including information like variances from planned route and altitude are critical inputs as even the smallest deviation can have a huge impact on fuel burn. This information is also used after each flight to make the machine learning algorithms more accurate.

When Every Drop of Fresh Water Counts

Agriculture accounts for about 70% of the freshwater used in the United States, and with population growth this is expected to increase by about 55 percent over the next three decades. SCADAfarm's irrigation and wastewater IoT system are helping farmers manage water resources on farms spread over vast geographic areas. Farmers can remotely monitor irrigators and pumps and customize sprinkler pivot orientation. They can incorporate real-time data on crop type, soil moisture level, soil type, and weather data such as rain, wind, heat, and humidity to develop water management plan that saves water, electricity while increasing crop yield. Based on these inputs, the system is used to create irrigation plans that comply with water regulations.

"I look at our flow meters and sometimes the machine might be saving up to 50 percent of its allocated water use," said Blackburn, whose yields of fodder beet and barley have also increased. "I can attribute that to the efficient use of SCADAfarm. I wouldn't go back without it."

Farmers can analyze water storage and determine how much water is needed to be pumped while also looking at the spot price of electricity. This way they can plan electricity usage to pump water when the price is lowest. (Ho, 2017)[5]

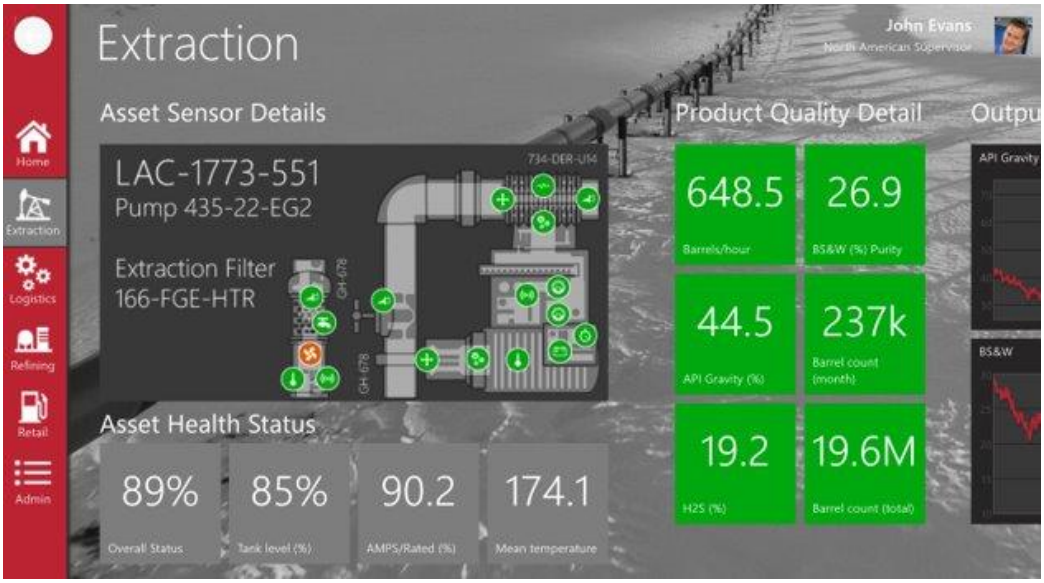
Digital Supply Chain

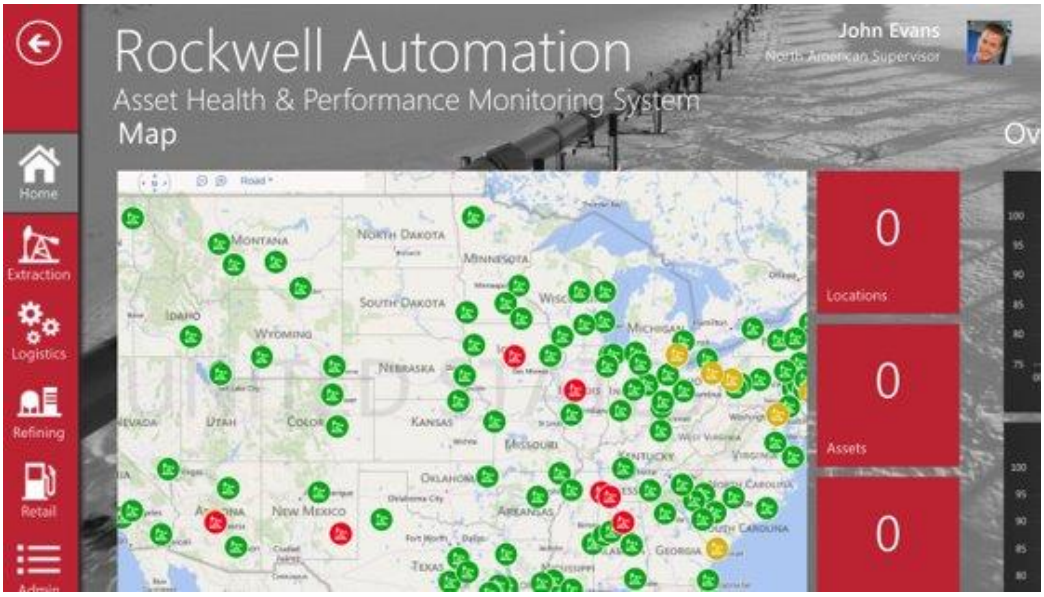
Rockwell Automation is using IoT services to manage the supply chain of highly capital-intensive assets in the oil and gas industry. These devices collect and analyze data in the Azure IoT Hub from remote equipment globally. The data is then organized and integrated for use in predictive analytics to keep the equipment operational and to accurately forecast operational demand or to manage inventory for spares and new equipment.

Off the coastal waters of Alaska's Kenai Peninsula, Hilcorp Energy Company's oil-drilling platforms use electrical submersible pumps driven from variable speed drives (VSD) from Rockwell Automation. Hilcorp stands to lose $100,000 to $300,000 per day when one of the pumps stops working. Sensors on the pumps' VSDs continuously send critical equipment performance data such as pressure, temperature, flow rates, and other data to the cloud for monitoring by engineers on dashboards in the command room in Cleveland, Ohio. The moment any performance metric begins to fall outside the specified parameters, engineers are alerted so they can take corrective action before the issue affects operations

"The last time we had a well trip offline, within five minutes we had a phone call telling us what broke, what to look at, and how to test it," Hilcorp's facilities engineer Mark McKinley said. "It

saved six hours of troubleshooting or more, and we got right back online. The staff is ecstatic, because they get support before they have to break out manuals and figure it out on their own."





Rockwell Automation Dashboards © Rockewell Automation

Once the crude oil is out of the ground moving it through refineries and to the pump is accomplished via a vast network of ships, barges, pipelines, trains and trucks crisscrossing the globe. Pieces of equipment called "skids" measure the amount of product transferred from one container to another as it changes hands. Also called Lease Automatic Custody Transfer (LACT) units, skids have relied on paper-based processes and periodic site visits for routine maintenance, leaving them vulnerable to inaccuracies and failures. Trigg Technologies, in collaboration with Rockwell Automation, is putting IoT sensors on the LACT units and collecting data in the cloud

for remote maintenance as well as to accurately monitor the product transfer from one party to another enabling immediate electronic invoicing. (Automation, 2019)

Industrial Augmented Reality (AR)

As critical infrastructure ecosystems are increasingly digitalized data visualization becomes a central issue. How and where can different levels of information— the connectivity between items, repair manuals, and the ebb and flow of use—be communicated more rapidly and effectively to those who need them? How can a technician in the field best access the context of what they're working with the collective history and expertise of the system and others had worked on it before?

Enter industrial augmented reality (AR)—where collaborative expertise and the visualization of a multitude of data layers in the field and virtual analytics back at headquarters are possible.

As smart glasses and other head-mounted-displays evolve from bulky helmets to smaller, less cumbersome untethered devices—more and more technicians will be able to make use of them in diverse environments.

Let's look at an example of this in action. Drone imaging of a remote powerline provides initial identification of a storm-damaged section that could cause outages. The drone can be piloted from afar via traditional remote piloting, or AR—allowing for rapid documentation and analysis. The need for repair can be demonstrated to decision makers as standard photography, 360 capture, or as a 3D model created via structure from motion (i.e., using the photography to build a 3D replica). A specialized technician is deployed to fix the powerline—and brave the heights of dangling high above the ground during said repairs. The technician reaches the damaged line, but realizes that the fix is outside of his/her know-how. Luckily, the technician is equipped with smart glasses and can pull up manuals or videos of similar previous repairs or they can contact a colleague at the office with more experience..A multitude of companies have emerged in this space including, Apple, Google, IBM, and =. However, there are many technical and logistical challenges, such as how to secure additional layers of data and access,before AR rolls out beyond its current use in factory settings and on oil and gas rigs and pipelines. Moreover,

visualization systems of integrated data sets are intended to optimize operations, but they also have the potential to reveal critical details to malicious actors.

Interconnected Smart Cities

Discussion of the IIoT or Industry 4.0 is incomplete without touching on smart cities. Smart cities are made up of smart buildings, smart counties are made up of smart cities, smart states are made up of smart counties, smart nations are made up of smart states, and a smart planet is made up of smart nations. This is an urban planner's ultimate goal: to optimize our systems of systems.

Arguably, the connectivity of the critical infrastructure that forms the IIoT layer that lies at the base of a smart city is its most important layer. And though it features prominently in smart city discussions and in the guides and resources for civic communities looking to upgrade, it features disproportionately in the metrics that track smart city progress.

Though it is arguably the use of technology and data connectivity that makes a smart city smart, the actual metrics used by research organizations to collate and compare smart cities against each other fail to capture holistic snapshots of technology and data connectivity. This is especially true in reference to their IIoT layers and how well these layers communicate with each other.

Take for instance, the IESE (Instituto de Estudios Superiores de la Empresa) Cities in Motion Index (CiMI) (Ricart, 2019) compiled and published by the most pre-eminent business school in Europe. Though lauded and widely cited as the ultimate smart city index by a variety of major media, the metrics tracked have far more to do with a city being smartly run than with the city itself having any form of ambient intelligence in its operations, such as applied data connectivity, analytics, artificial intelligence and computer vision layers, or even overhauls of their legacy IT.

The IESE CiMI uses elaborate weightings of factors such as human capital indicators (number of theaters and museums), social cohesion (mortality, happiness indexes), economic indicators (ease of starting a business, businesses who have headquarters there, salary), governance (research centers, government buildings), the handful of tech variables (open data platform, use of Uber), environmental indicators (pollution index, solid waste generation), mobility and transportation (traffic index, number of commercial vehicles), urban planning (high rises, people per household), and international outreach (number of McDonalds, hotels, and restaurant indexes).

Yes. That's right. The number of McDonalds a city counts more towards its title as a smart city than any evaluation of the connectivity of its electrical grid, the predictive maintenance of its water system, or the historic record of its cybersecurity practices. The technology indicators for a smart city (like the handful of metrics making up the entirety of the tech section in the CiMI displayed below) should be far, far more robustly expanded to consider the technology at play. Revised metrics need to be established and actively utilized to compare and contrast the current landscape of smart cities to determine which ones are still heavily reliant on human inputs and which ones are legitimately smart and digitally connected.

No.	Indicator	Description / Unit of measurement	Source
84	Twitter	Registered Twitter users in the city. This is part of the social media variable.	Tweepsmap
85	LinkedIn	Number of users in the city. This is part of the social media variable.	LinkedIn
86	Mobile phones	Number of mobile phones in the city via estimates based on country-level data.	International Telecommunication Union
87	Wi-Fi hot spot	Number of wireless access points globally. These represent the options in the city for connecting to the Internet.	WiFi Map app
88	Innovation Cities Index	Innovation index of the city. Valuation of 0 (no innovation) to 60 (a lot of innovation).	Innovation Cities Program
89	Landline subscriptions	Number of landline subscriptions per 100 inhabitants.	International Telecommunication Union
90	Broadband subscriptions	Broadband subscriptions per 100 inhabitants.	International Telecommunication Union
91	Internet	Percentage of households with access to the Internet.	Euromonitor
92	Mobile telephony	Percentage of households with mobile phones in the city.	Euromonitor
93	Web Index	The Web Index seeks to measure the economic, social and political benefit that countries obtain from the Internet.	World Wide Web Foundation
94	Telephony	Percentage of households with some kind of telephone service.	Euromonitor
95	Internet speed	Internet speed in the city.	Nomad List
96	Computers	Percentage of households with a personal computer in the city.	Euromonitor

Analysis of the current state of smart cities and critical infrastructure suffers from two additional weaknesses.

The first is a regional bias. Lists generated in one region of the world analyzing smart cities tend to evaluate their local smart cities and inherent critical infrastructure as more highly rated than that of other regions.

Large cities also trend to the top of such analyses under the presumption that large quantities of people being shepherded through an urban jungle must indicate that city is being run more intelligently. Abstractions of the numbers to focus on quality of technological interactions and the connectivity of the digital systems from the base IIoT layers up to the tracking of individual operators within the cityscape may establish that some of the smartest cities in the world are much smaller testbeds and are currently under the radar. More exposure and attention should be paid to the cities that are smaller but potentially more technologically proficient and agile with updating and integrating their legacy hardware, software and resulting data.

As the population of the world simultaneously increases and migrates into urban landscapes, it is even more essential that cities and the underlying infrastructures that allow for their successful optimization—the transportation systems, utilities, etc.—are able to evolve.

According to the non-profit Smart Cities Council as of 2019 cities account for 1 percent of global land usage and yet house 55-86 percent of the world’s population of 7.53 billion. In the United States, 80 percent of our population lives in urban environments according to the U.S. Census Bureau. Cities account for 75% of the world's energy use and 80 percent of the world's

emissions. Optimizing our cities at all levels, including and especially with reference to their IIoT base layers of infrastructure is crucial.

According to a recent McKinsey report on smart cities, connecting, analyzing, and optimizing extant and emerging systems would reduce emissions by 10-15 percent, water consumption by 20-30 percent commute times (by 15-30 minutes per commuter), and traffic related fatalities by 8-10 percent (McKinsey Global Institute, 2018). Projections for the self-driving car industry predict as much as an 80 percent reduction in traffic related deaths. But more pressing then the savings in connectivity is the knowledge that there will only be an even greater number of people utilizing the various tiers of industrial services. The United Nations projects that by 2050, there will be 9.7 billion people living in cities. That is more than the current world population living anywhere right now. No smart grid in existence is prepared for that jump without serious, thoughtful evolution—nor is any other IIoT layer of any city on the planet.

Section Two: Risks

IIoT Risk Overview (IIoT)

Implementation and use of IIoT devices is growing exponentially. Unfortunately, much of the software used in IIoT systems are developed without appropriate, if any, security controls or risk management.

IIoT devices are networked, often over the public Internet. The access technologies used in IIoT include wireless or mobile communications such as Bluetooth, 3G, 4G-LTE, 5G, and even 2G and older legacy wireless protocols. These access networks connect to corporate, government, domestic, and global backbones. All this interconnection, if not adequately secured, can result in substantial risks.

The risks are exacerbated by vulnerabilities in the devices and their environments from threats such as unsecured physical access, poorly developed software, and even unsecured firmware and hardware. On August 22, 2019, The Security Ledger reported that a survey of over 6,000 firmware images from more than a decade shows no improvement in firmware security and lax standards for software running connected devices. Sarah Zatko, the Chief Scientist at the Cyber Independent Testing Lab (CITL), a non-profit organization that conducts independent tests of software security, said, "We found no consistency in a vendor or product line doing better or showing improvement. There was no evidence that anybody is making a concerted effort to address the safety hygiene of their products."

The threats to IIoT devices, systems, and their operating environments are numerous, varied, and growing. Threat-actors include nation-state adversaries and APTs, non-state actors, criminals, hacktivists, and run-of-the-mill hackers.

> *Preventing attacks against IoT and operational technology (OT) infrastructure is a top priority for 2019. When ranking their top cybersecurity concerns for 2019, nearly two-thirds (65%) of public sector respondents say they're worried about attacks involving IoT or OT assets. 61% are specifically concerned about attacks against OT infrastructure.* - **Tenable: Cybersecurity in Public Sector: 5 Insights You Need to Know, LLC February 2019**

Nation-State Adversaries

IIoT is an appealing target for our adversaries because IIoT devices typically are not as secure as enterprise or business systems. Also, these devices are connected to our most sensitive business and industrial systems. An example of such vulnerabilities includes the breach of a large retailer via a compromise of the network connected HVAC systems. That breach then propagated via internal systems until it reached the point-of-sale systems resulting in a huge loss of customer data, including credit card information. IIoT systems can be hacked to damage equipment, steal information, spy on the environment in which they are installed, and disrupt or interfere with operations or production.

IIoT attacks can be even more impactful than non-IIoT breaches. The breach of a system that controls a power plant can cause an outage affecting thousands of customers including other critical infrastructure, emergency, and medical systems, as well as the citizen population. Some power system incidents can take out a large segment of the country. A breach of a smart city could

cause the shutdown of most city operations, including all traffic controls. A breach of hospital equipment can cause loss of many lives or even the uncontrolled spread of pathogens.

Nation-state adversaries can take advantage of the combination of inherent security weaknesses and significant impact for reasons that include disruption of day to day activities, theft of intellectual property, theft of publicly identifiable information (PII) and sensitive personal information (SPI), and reduced ability to respond to other incidents, among many others. Many of this type of hack have taken place throughout 2019.

In August of 2019, Forbes and ArsTechnica reported that "Microsoft [caught] Russian state hackers using IoT devices to breach networks.

In August 21st, 2019 ZDNet reported that Chinese APT hacking groups are attempting to steal research work from cancer research institutes. This is an example of Chinese APT groups focus on attacking American organizations to speed up their research by stealing corporate data and intellectual property.

In June of 2019, Digital Trends reported that Russian Hackers are probing the US Power Grid. This article referred to an article in WIRED magazine that described how a hacking group known as Xenotime or Triton that is linked to the Russian government attempted to breach the U.S. power grid.

A large proportion of networked cameras are made in China. Several incidents have been reported of such cameras being poorly secured and/or sending their images and data back to Chinese operated controllers. In August of 2019, a Wall Street Journal headline reported that "Surveillance Cameras Made by China Are Hanging All Over the U.S." In July, the Los Angeles Times reported that "banned Chinese security cameras at U.S. facilities are almost impossible to remove."

Many drone brands are also made in China. Several news reports have described drone images and data being sent to Chinese controlled servers. Researchers at Johns Hopkins University described in 2016 the ease of hacking and crashing a drone. ThreatPost reported in March of 2019, how "Drones are Quickly Becoming a Cybersecurity Nightmare". A rogue drone was recently used to shut down Gatwick airport in the UK for several days.

Criminal and Non-State Actors

Nation-States are not the only risk to IIoT systems. Criminal and other non-state-actors are also increasing attacks on IIoT systems. Attacks can include ransomware, cryptocurrency mining, data-stealing, denial of services, botnets, and others.

An attack on wireless IIoT devices by Sierra Wireless resulted in exposure to a range of threats, as reported by ThreatPost in 2018. The vulnerabilities included privilege escalation (CVE-2018-10251, CVE-2017-15043), risk of being used for Reaper botnet or being illicitly used as a proxy.

Source: www.vericidemagazine.com

Supply Chain Risks

Risks also include threats to the supply chain. IIoT devices are sourced in many different countriesand contain many components including hardware, software, and firmware. Each of these devices and components have a supply chain that can be compromised at many points including by the manufacturer, the software libraries, the shippers, the distributors and more.

Risk and Vulnerability Mitigation and Management

Managing and mitigating the risks of IIoT includes many of the foundational best practices for cyber security. These include:

- Know what IIoT you have;
- Scan, assess, and pen-test your devices;
- Keep the device software up to date; and
- See how much the bad guys can find if they look for your devices

Managing the risk also includes an enterprise or organizational risk-management perspective. This means doing a business impact analysis, disaster recovery plan, cost plan, and more.

Refer to and use standards or guides such as NIST's Securing the Industrial Internet of Things or "What is the Internet of Things (IoT) and How Can We Secure It." Additional how-to links are provided below.

These and other mitigation approaches are described in more detail below:

Know what you have

The foundation of any security program is knowing what you have. This means identify and inventory all of your IIoT assets. Include what you own, what is used on your behalf (by contractors, service providers, etc.)Identify the components of your IIoT assets. This includes software versions, firmware versions, and hardware.These inventories will help you manage the risk by associating reported vulnerabilities with your inventory. It will also help in subsequent steps.

Periodically scan, assess, and pentest your devices

Using your inventories, use appropriate tools or qualified service providers to run security scans, vulnerability assessments, and penetration tests of your devices and the environments in which they operate. Collect and correct identified vulnerabilities.

Keep the software up to date

Keeping the software up to date seems an obvious way to mitigate risk, but it involves monitoring vendors and manufacturers for updates and patches and implementing the patches in an operationally appropriate manner. Patches should be applied as soon as stable, tested versions are available.

See what the bad guys see

Use tools like Shodan to scan the internet for your IIoT devices. The bad-actors of the internet are constantly doing this; you should too.

Enterprise or organizational risk management perspective

As IIoT becomes more imbedded in business operations, more formal risk management approaches must be implemented. This includes assessing and prioritizing the impact and cost of downtime. Some approaches to managing risk include business impact analysis, disaster recovery planning, recovery time objectives, alternate or manual operations, etc. The inventories discussed above are critical to these activities. Consider the costs of potential loss of intellectual property, loss of reputation, loss of business, and cost of liabilities when planning for risk management.

Define, document, implement, and test the incident response and disaster recovery plans. Include up-to-date vendor and manufacturer and service-provider contacts. Involve your PR and Legal teams. Include alternate operational scenarios such as what to do if systems are compromised by ransomware, what to do if impacted by a denial of service, how to make and use backups, how to effect manual procedures while automated functions are recovered, and more. Prioritize the threats and responses so you know what to do first.

Harden your systems

Change default user IDs and passwords. Use strong authentication and multi-factor authentication wherever possible. Periodically look for compromised credentials on the darkweb and by using tools like haveibeenpwned, or use a service to monitor this. Use VPNs to communicate with and control IIoT devices.

Section Three: Mitigation

Government Efforts to Secure IIoT

The Government and industry today deal with asymmetric threats across the cyber landscape. Cyber has leveled the playing field for smaller nation-state and non-nation-state actors to carry out attacks against larger targets of interest. The ubiquity of the internet and its ability to seamlessly connect various devices to each other across different platforms and multiple protocols is creating a revolving door of cybersecurity challenges. Today's adversaries are as dynamic as the internet itself. Cyberattacks are being conducted by asymmetric groups that form, disband, and re-form elsewhere making attribution and prosecution challenging at best. Protecting the U.S. from a catastrophic cyberattack will require significant collaboration between the U.S. government and private industry.

I: Silicon Valley Innovation Program (SVIP)

The Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) Silicon Valley Innovation Program (SVIP) is paving the way for delivering cutting-edge technologies and capabilities that address IoT and IIoT security challenges and use cases.

Most governments are not as nimble as private industry. The rapid proliferation of embedded devices into critical infrastructure continues to create security challenges for both the private industry and the federal government. Next generation technologies intended to secure this dynamic environment may still be years away from full adoption as the Research and Development (R&D) lifecycle can move slowly at times.

The SVIP seeks to help S&T keep pace with the innovation community. Acting as a technology accelerator, SVIP is "reshaping how the government, entrepreneurs, and industry work together to find cutting-edge solutions to strengthen national security."

SVIP works with technology start-ups to deliver "solutions to some of the toughest threats facing DHS and the homeland security mission." By Leveraging the Other Transactional Solicitation (OTS) vehicle, SVIP is able to streamline the acquisition process and issue new awards more rapidly than traditional contract vehicles. Eligibility requirements for applicants include having less than 200 employees and having no previously awarded federal contracts (totaling $1,000,000) or more in the past twelve months. In December 2015, SVIP issued its first OTS call focused on IoT Security solutions within three capability areas; Detect, Authenticate, and Update. SVIP's awards consist of four-phase efforts not exceeding $800K over a period of 24 months. The maximum Period of Performance (PoP) for each phase is six months with a funding ceiling of $200K. A program summary is provided below:

- Phase 1 – Proof-of-Concept – Demo
- Phase 2 – Demo Pilot-Ready Prototype
- Phase 3 – Pilot-Test Prototype in Operation
- Phase 4 – Testing in Various Operational Scenarios, Transition/Commercialization

While SVIP's OTS for IoT security does not specifically address security concerns in the IIoT, many of the technologies and capabilities developed under this solicitation are applicable. For example, consumer devices such as mobile phones, fitness trackers, navigation systems, computers/tablets, home appliances, and other smart devices all require firmware updates. Often times, an update may be issued via a third-party vendor. This raises a security concern about how firmware updates are being verified and validated before being installed.

SVIP awarded ADolus an opportunity to develop a capability under the "Update" solicitation objective. ADolus/QED's Secure Trust Anchor (STA) is a "vendor-agnostic tool for verifying and validating third-party vendor updates for IoT devices." IIoT applications for Adolus/QED's STA span multiple industries including Automotive, Manufacturing, Aerospace, Oil and Gas, Medical, and Utilities.

Another SVIP funded performer, Ionic Security Inc., partnered with Swiss IT security company Kudelski Group to develop capabilities for securing video and surveillance streams from smart cameras. The scalability of Ionic's technology "enables both new and legacy content devices to protect the content no matter where it flows.".

SVIP's funded efforts in IoT security have both direct and causal sequence applications for IIoT security challenges. For example, the development of K-9 Wearable technologies that leverage IoT sensors to monitor vital signs and health indicators of the Customs and Border Protection's canine workforce. These efforts are all part of the IoT ecosystem which includes the IIoT, Internet of Battlefield Things (IoBT), Space-Enabled IoT, and others.

Additional information on the SVIP program, their funded projects, and information on how to work with them can be found on the DHS S&T SVIP website.

II: The National Cybersecurity and Communications Integration Center (NCCIC)

Oversight, ownership, responsibility. These types of words are influential in terms of slowing the collaboration between the private sector and the federal government. DHS' mission to secure the homeland includes securing cyberspace and critical infrastructure. The private sector owns approximately 85 percent of critical infrastructure. This creates a gap in the policies, directives, and standards created by the government and the ability and/or willingness of the private sector to implement them. The newly formed Cybersecurity and Infrastructure Security Agency (CISA), formerly the National Protection and Programs Directorate (NPPD) has developed several programs to assist both public and private sector entities in improving their cybersecurity posture. While these programs are not specifically developed for IIoT, there are still direct security impacts as IoT sensors and devices continue to proliferate society.

A common gap area among organizations within any major ecosystem, in this case, cybersecurity, is coordination. CISA's National Cybersecurity and Communications Integration Center (NCCIC) does exactly that. "The Cybersecurity Act of 2015, designated the NCCIC as the central hub for cyber threat indicator sharing between the government and the private sector."). The NCCIC "serves as a central location where a diverse set of partners involved in cybersecurity and communications protection coordinate and synchronize their efforts." "Working closely with its partners, NCCIC analyzes cybersecurity and communications

information, shares timely and actionable information, and coordinates response, mitigation and recovery efforts." Some of the NCCIC's mission activities include:

- Information Exchange;
- Training and Exercises;
- Risk and Vulnerability Assessments;
- Data Synthesis and Analysis;
- Operational planning and Coordination;
- Watch Operations;
- Incident Response and Recovery;

Rapid advancements in technology and connectivity combined with first-to-market business strategies have created a wide array of cybersecurity challenges and concerns. By centralizing coordination between public, private, law enforcement, academia, and other stakeholders; the NCCIC can address cyberattacks and other incidents in an effective coordinated manner.

The National Cybersecurity Assessments and Technical Services

The National Cybersecurity Assessments and Technical Services (NCATS) team is a component of the NCCIC and "supports Federal, State and Local governments, and critical infrastructure partners by providing proactive testing and assessment services." The NCATS team offers various types of assessment services including:

- Red Team Assessment (RTA);
- Validated Architecture Design Review (VADR);
- High Value Asset Assessment (HVA);
- Risk and Vulnerability Assessment (RVA);
- Phishing Campaign Assessment (PCA);
- Cyber Hygiene: Vulnerability Scanning. (DHS NCATS, 2019)

These assessments services are offered at no cost to the recipient. This incentive is especially useful to organizations that may not have robust cybersecurity policies and procedure in place or the resources necessary for conducting a formal cybersecurity assessment. These assessment services are not part of the NCCIC's incident response services. They are intended as a voluntary and proactive measure for identifying, mitigating, and remediating vulnerabilities "prior to exploitation by an attacker." Stakeholder privacy is protected under DHS' Protected Critical Infrastructure (PCII) Program. The PCII program establishes "uniform procedures on the receipt, validation, handing, storage, marking, and use of Critical Infrastructure Information (CII) voluntarily submitted to DHS."

Validated Architecture Design Review

CISA NCATS' cybersecurity assessments program provides a suite of cybersecurity resources that can help critical infrastructure asset owners and operators improve their organization's cybersecurity posture. While all the assessment services can help improve IIoT security, the Validated Architecture Design Review (VADR) has had wider usage with ICS. A VADR assessment can be conducted on both Information Technology (IT) and Operational Technology

(OT) systems. This assessment provides a detailed review of network architecture design and interconnectivity to internal and external systems. VADRs also provide a system configuration and log review and an analysis of network traffic.

VADRs help both public and private sector organization identify and understand the gaps in their cybersecurity defenses. This is especially helpful for traditionally stand-alone or "air-gapped" systems that are being connected to the open internet or integrated with enterprise networks.

As the IoT and IIoT continue to expand, the need for collaboration between public and private sector entities will become increasingly important. CISA components such as the NCCIC and NCCIC programs such as NCATS are examples of the efforts being undertaken by the government to secure the nation's cybersecurity infrastructure. This summary of CISA's services is not intended to exhaustive but instead to showcase a few examples of how the federal government is working with private-sector stakeholders.

Industry Efforts to address IIoT Risk Mitigation

With so much effort across so many industries to capture and analyze data using IIoT, cybersecurity emerges as one of the common issues inhibiting growth in this burgeoning field. Cybersecurity is a central roadblock for many governments and enterprises when it comes to investment and deployment of IoT devices in their cities, building complexes and factories. Industry has tried to address the device and ecosystem cybersecurity challenge with multiple guidelines and a certification program over the 12 months.

The wireless industry brings thousands of IIoT devices to market every year. Part of the U.S. wireless industry approach is to collaborate on working groups hosted by CTIA, the major U.S. wireless industry trade association, and develop standards for wireless connected devices. Their Cybersecurity Certification Working Group developed and regularly reviews the IoT Device Cybersecurity Certification Test Plan which lays out cybersecurity standards for connected devices. CTIA has over 100 third party test labs globally that certify that devices are in conformance with the test plan. The test plan allows a marketplace of test labs to develop speed and processes with IoT manufacturers that focus on time to market and lowering the cost of third party testing.

At least 20 different associations have contributed to a consortium of IoT Cybersecurity approaches led by the Consumer Technology Association. Six of the organizations have their own IoT cybersecurity guidelines. The associations that have shared guidelines are:

- CTIA IoT Device Cybersecurity Certification, Version 1.1, 2019
- CSDE International Anti-Botnet Guide (Draft) 2019 (September Release)
- IoTopia Specifications (Cisco)
- IoXT Pledge, 2019
- Open Connectivity Foundation Security Specification 2.0.1, 2019
- World Wide Web Coalition Web of Things Best Practices, 2019
- GSMA IoT Security Guidelines Endpoint Ecosystem, 2016

Additionally, multiple international government initiatives, committees and consortiums have developed voluntary cybersecurity recommendations. Those government IoT cybersecurity recommendations are listed below.

- Baseline Security Recommendations for IoT by the European Union Agency for Network and Information Security (ENISA), 2017
- Code of Practice for Consumer IoT Security by the United Kingdom Department for Digital, Culture, Media and Sport (DCMS), 2019, further shared as ETSI TS 103 645
    - Additional IoT Security Architectures and references can also be found in the DCMS Mapping of IoT Security Recommendations, Guidance and Standards to the Code of Practice for Consumer IoT Security, 2018
- NIST IR 8259 Core Cybersecurity Feature Baseline for Securable IoT Devices (Draft), 2019
- FDA Medical IoT Cybersecurity Guidance, 2018

Most of the above voluntary recommendations or guidelines focus on device security aspects at the consumer level. Some include additional provisions describing how an organization should securely develop software, patch and update products and how the organization will run and handle reported vulnerabilities. All of the above recommended guidelines and certifications are single tiered and largely presented as minimal baseline security capabilities. CTIA has a multi-tiered IoT device certification that addresses security and risks for consumers, enterprises and critical infrastructure.

Additional ongoing work at the international governmental level includes regulatory bodies in the EU, Japan and Singapore listed below:

- Singapore: The Infocomm Media Development Authority is developing an IoT Cyber Security Guideline. This will be voluntary for manufacturers.
- Japan: The Ministry of Economy, Trade and Industry (METI) is developing a Cyber/Physical Security Framework pertaining to the security of IoT and other connected systems (Ministry of Economy, Trade and Industry, 2018).
- European Union: The Cybersecurity Act will, among other things, allow the EU Agency for Cybersecurity (formerly ENISA) to develop certification criteria for IoT devices and related services (European Commission, 2018).

In addition, Congress has a number of active bills focused on aspects of IoT Cybersecurity. U.S. states have started to create and pass legislation on IoT cybersecurity and privacy related issues. California passed an IoT cybersecurity bill in 2018, and Illinois, Kentucky, Maryland, Massachusetts, Oregon, Rhode Island and Vermont all have active IoT Cybersecurity and/or Privacy bills up for consideration this year.

Additional efforts to mitigate cyber risks include the development, testing and backing of a new technology called “manufacturer usage description” or MUD. MUD was first developed by Cisco so that IoT devices can inform the network of the access and network functionality needed to work properly. Using a PKI construct, an IoT device can join a network and obtain a MUD file from the internet that is shared with a MUD server on the local network. The MUD server notifies the firewall and the router of what that IoT device needs to access for updates (ports, protocols, etc.) and the firewall can block all other access to that device. This happens in the background,

automatically, without the need for misconfiguration by network administrators and helps prevent shodan scans and other tools used to illuminate unprotected IoT devices on networks around the world.

NIST has stood up a community of interest (NIST, 2019) around the MUD protocol. As part of the response to the Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (EO 13800), sometimes called the "Botnet Report," NIST began a project to mitigate IoT based DDoS activities focused on the MUD protocol (NIST, 2019). This project brought together IoT device manufacturers, gateway manufacturers, communications service providers and users of IoT devices.

Based on this project, NIST has released a draft Cybersecurity Practice Guide (SP 1800-15). Multiple efforts continue on this project to build out the ecosystem of support for MUD with the goal of a multipronged effort to mitigate botnet activities focused on the compromise and repurposing of deployed IoT devices. NIST most recently submitted MUD support constructs to 3GPP for inclusion into the standards and specifications of cellular connected devices (3GPP is the cellular communications standards body that developed the standards for 5G.) MUD is looking to be included in those specifications so more cellular connected IoT devices can enhance their security posture.

Government Efforts to Mitigate Cyber Risks Against IIoT

In May of 2017 Presidential executive order 13800, "Strengthening the cybersecurity of federal networks and critical infrastructure focusing on resilience against bot nets and other automated distributed threats," was issued. In the past traditional mitigation strategies were able to absorb the effects of botnets. However, with the advent of IoT the scope of malicious activities facilitated by botnets have increased relative to the sheer number of IoT devices introduced to the internet, rendering traditional mitigation strategies ineffective.

The Departments of Commerce and Homeland Security were directed work jointly on this effort in consultation with the Departments of Defense, Justice, and State, the Federal Bureau of Investigation, sector-specific agencies, the Federal Communications Commission, and the Federal Trade Commission, as well as other interested agencies gathering a broad range of input from experts and stakeholders, including the private sector and academia.

DHS's participation in this effort was focused through the President's National Security Telecommunications Advisory Committee's (NSTAC) and finalized on November 16, 2017. While developing its report, the NSTAC studied botnets and attack vectors used to create botnets (i.e., end user devices and IoT). Through this study, the NSTAC determined that compromised IoT devices will increasingly be used by malicious actors to launch global botnet automated attacks. Due to the lack of security in the design of IoT devices they are now the most target rich environment for malicious actors. In November 2016 an Ericsson Mobility Report predicted that IoT devices will surpass mobile phones as the largest category of internet connected devices within 2 years.

In response to Executive Order 13800 a report. "A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated,

Distributed Threats" was delivered in May of 2018. In that report several tools relating to the mitigation of IoT vulnerabilities were identified.

Future network implementations should include five major principles contained in the NIST Cybersecurity Framework (CSF):

- Identify legacy devices that cannot be secured and remove or replaced them where possible
- Use system architecture to provide additional layers of protection to high risk devices. Employ denial of distributed service mitigations services and implement ingress and egress filtering to prevent network address spoofing and utilize and efficient patching and update process to mitigate vulnerabilities.
- Employ ISP based detection services with near real-time detection of compromised devices
- Established in implement policies and procedures to respond to compromised devices replace, mitigate or patch devices part of a botnet.
- Establish the ability to recover systems compromised by a botnet attack.

Public-Private Collaborative Efforts

Security is not, however, the only challenge facing IIoT. Lack of active, cross-silo communication and collaboration between different categories of companies, between industry and government and academia, between nation-states— have been, are, and will continue to be a concerning issue, one which impedes optimization of cyber-physical data and systems entanglement at scale. In other words—smart cities and smart nations cannot and will not develop in a vacuum or in their own echo chambers. Divides in concepts of privacy and data access are already driving a wedge between nation-states participating in their own variants of the industrial internet of things.

Though there are a number of lauded entities and conferences devoted to IIoT and Smart Cities—these groups and their conferences are not enough. Nor are the individual city test beds and regional collectives being put together. Of those entities bridging the gap between industry and civic governments at the moment the Smart Cities Council is of particular note. As part of their efforts to get industry and local governments on the same page, they have committed to an ongoing publication series of consumable documents like the Smart Cities' Readiness Guide, or their Collaboration Playbook for Smart Cities and Electric Companies (Smart Cities Council 2019).

Documentation and occasional conferences are not enough. More mechanisms for cross-collaboration between relevant bodies need to be established at multiple scales and with actuated power to translate their conversations into actions. More mechanisms for comparing basic technology implementation and interest across active projects and science communication of the results would be an impressive starting point. It would be interesting to see what an international collaboration with significant financing could do if given a city as a test-bed to actuate, evaluate, monitor, and test the resiliency of extreme levels of connectivity. Chances are it would result in a useful guide for what to do and what not to do for other cities and states interested in optimizing and securing their systems.

Though mass-scale test-beds are available and accessible options for countries like China which are actively letting their cities experiment at mass-scale—neither cities in the United States or their utilities have the same level of autonomy and flexibility. In countries where the intertwined government-industrial complex makes such experimentation is possible smart cities could be leaps and bounds ahead of efforts here at home.

References

(2019, January 30). Retrieved from Bain.com: Source: https://www.bain.com/insights/beyond-proofs-of-concept-scaling-the-industrial-iot/

aDolus (2019). aDolus – What We Do. Retrieved August, 2019, from:. https://www.adolus.com/

Ionic Security, Inc., (2019).Ionic Data Trust Services. Retrieved August, 2019, from: https://ionic.com/ecosystem/partners/kudelski

AI: Making Sense of the Industrial Internet of Things. (2019). Retrieved from CIO: https://www.cio.com/articles/3378202/ai-making-sense-of-the-industrial-internet-of-things.html

Automation, R. (2019, May 23). *Customer Stories.* Retrieved from Microsoft.com: https://customers.microsoft.com/en-us/story/fueling-the-oil-and-gas-industry-with-iot-1

Department of Homeland Security (DHS), (2019). DHS – Mission. Retrieved August, 2019, from: https://www.dhs.gov/mission

Department of Homeland Security (DHS), (2019). National Cybersecurity and Communications Integration Center (NCCIC) [Legacy Page]. Retrieved August, 2019, from: https://www.us-cert.gov/nccic

Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), (2019). National Cybersecurity and Communications Integration Center (NCCIC). Retrieved August, 2019, from:https://www.dhs.gov/cisa/national-cybersecurity-communications-integration-center

Department of Homeland Security (DHS) National Cybersecurity Assessments and Technical Services (NCATS), (2018). NCATS Program Fact Sheet. Washington D.C: U.S. Government Printing Office.

Department of Homeland Security (DHS) National Cybersecurity Assessments and Technical Services (NCATS), (2018). Validated Architecture Design Review (VADR) Factsheet. Washington D.C: U.S. Government Printing Office.

Department of Homeland (DHS) Science and Technology Directorate (S&T), (2019).. Silicon Valley Innovation Program. Retrieved August, 2019, from: https://www.dhs.gov/science-and-technology/svip

Department of Homeland (DHS) Science and Technology Directorate (S&T), (2015). ARCHIVES: DHS S&T Releases Innovation Call Aimed at Startups. Retrieved August, 2019, from: https://www.dhs.gov/news/2015/12/11/dhs-st-releases-innovation-call-aimed-startups

Dragos Platform Components. (2019). Retrieved from Dragos: https://dragos.com

European Commission. (2018). EU negotiators agree on strengthening Europe's cybersecurity. http://europa.eu/rapid/press-release_IP-18-6759_en.htm

Federal Emergency Management Agency (FEMA). Critical Infrastructure. FEMA Strategic Foresight Initiative 2011. https://www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf.

Federal Emergency Management Agency (FEMA), (2011). Critical Infrastructure. FEMA

Strategic Foresight Initiative.Retrived August, 2019, from:https://www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf.

Garcia, J. (2019, July 9). *How AI and IIoT Will Provide Insights for Manufacturers.* Retrieved August 12, 2019, from American Machinist: https://www.americanmachinist.com/enterprise-data/how-ai-and-iiot-will-provide-insights-manufacturers

Gold, J. (2019). *What is the Industrial IoT? (And Why the Stakes Are So High).* Retrieved from Network World: https://www.networkworld.com/article/32439828/what-is-the-industrial-iot-and-why-the-stakes-are-so-high.html

History (2019). 1969 Moon Landing [History.com]. Retrieved August, 2019, from: https://www.history.com/topics/space-exploration/moon-landing-1969

Ho, V. (2017, June 10). *Customer Stories.* Retrieved from Microsoft.com: https://news.microsoft.com/transform/schneider-electric-transforms-agriculture-internet-of-things-sustainable-farming/

iScoop. (2019). *5G and IoT: the Mobile Broadband Future of IoT.* Retrieved August 10, 2019, from I-Scoop: https://www.i-scoop.eu/5G/5G-iot

iScoop. (2019). *IT and OT Convergence--Two Worlds Converging in Industrial IoT.* Retrieved from iScoop: https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-of-things-it-ot

Japan Ministry of Economy, Trade and Industry . (2018). *METI Compiles Results of the Call for Public Comments on the Draft Cyber/Physical Security Framework.* Retrieved from Japan Ministry of Economy, Trade and Industry: https://www.meti.go.jp/english/press/2018/1001_002.html

NIST. (2019, August). *National Cyber Center of Excellence (NCCoE) Community of Interest*. Retrieved from National Institute of Science and Technology (NIST): https://www.nccoe.nist.gov/about-the-center/COI

NIST. (2019). Mitigating IoT-Based DDoS. Retrieved from National Institute of Science and Technology (NIST): https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos

Review, H. B. (2019). *Accelerating the Internet of Things Timeline.* Retrieved from Siemens: https://www.new.siemens.com/global/en/product/services/iot-siemens.html

Ricart, P. P. (2019). *IESE Cities in Motion Index.* IESE Business School, University of Navarra.

Scallehn, M. (2019). *Beyond Proofs of Concept: Scaling the Industrial IoT.* Retrieved from Bain and Company.

Smart Cities Council. (2019). Collaboration Playbook for Smart Cities and Electric Companies. https://smartcitiescouncil.com/system/tdf/main/public_resources/a_collaboration_playbook_for_smart_cities_and_electric_companies.pdf?file=1&type=node&id=6777&force=

Weinberger, S. (2015). How Israel Spoofed Syria's Air Defense System. Retrieved August, 2019 from: https://www.wired.com/2007/10/how-israel-spoo/

Leyden, J. (2007). Israel Suspected of 'Hacking' Syrian Air Defenses. Retrieved August, 2019, from: https://www.theregister.co.uk/2007/10/04/radar_hack_raid/

A Report to the President On Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats. Retrieved August, 2019, from: https://www.commerce.gov/sites/default/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf

Additional IIoT Security Resources:

Resources for IIoT security best practices

- https://usa.kaspersky.com/resource-center/preemptive-safety/best-practices-for-iot-security
- https://www.arubanetworks.com/assets/wp/WP_Top_5_IoT_Deployment_Best_Practices.pdf
- https://www.networkworld.com/article/3266375/best-practices-for-iot-security.html
- https://www.iotsecurityfoundation.org/best-practice-guidelines/
- https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices
- https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture
- https://www.zdnet.com/article/ten-best-practices-for-securing-the-internet-of-things-in-your-organization/