

Industry 4.0



Leveraging Digital Transformation for Growth

Introduction

Nearly every aspect of modern life depends upon the uninterrupted function of industrial control systems [ICS]. ICSs keep the lights on, ensure clean drinking water, and provide other critical infrastructure processes. Beyond power, energy and other utilities, ICSs are also responsible for manufacturing of our computers, our cars, and countless other physical items that we rely on every day.

It is imperative that ICSs are protected against all cyber events - accidental or malicious - because the physical ramifications of such events pose a major threat to both public safety and to any industrial entity's ability to stay operational and competitive.

But it's not realistic to apply cybersecurity best practices from the information technology [IT] side of your business to the operational technology [OT] side. IT and OT environments consist of completely different types of devices and network structures. OT environments also experience widely different risks and threats than IT environments.

Let's learn more.

The Industrial Revolution

The first Industrial revolution, known as the Machine revolution (mid 1700's to mid 1800's), marked the transition of manufacturing processes away from hand-made to machine-made products. The energy driving these machines came from water turned into steam.



The second Industrial revolution, known as the Technological revolution (late 1800's to WWI), introduced electricity, telegraph, and rail systems. These additions further optimized and automated factories with lighting for round-the-clock production, telegraphs introducing real time communications, and rail systems optimizing and accelerating delivery routes and time to market.

The third Industrial revolution (mid-late 1900's) was the Digital revolution. The digital revolution leveraged advances in electricity, technology, and computers to shift away from legacy analog and mechanical systems to fully digitize and optimize every facet of Industrial

production systems. Many of these advances remain in production today. But, in many areas, there still remains an analog component at the edge, in proximity to the machinery.

The 4th Industrial revolution (2010 – present) is known simply as Industry 4.0 – the collective initiatives to make our industries, the manufacturing processes and the building & cities we live in to become smarter. These initiatives are highlighted by the utilization of rapidly evolving technology advances for real-time data collection and analysis to bring efficiency, safety for the citizens & workers, security for processes that deliver critical resources and lastly reduce cost, the carbon foot-print, and wastage.

Key Components of Industry 4.0:

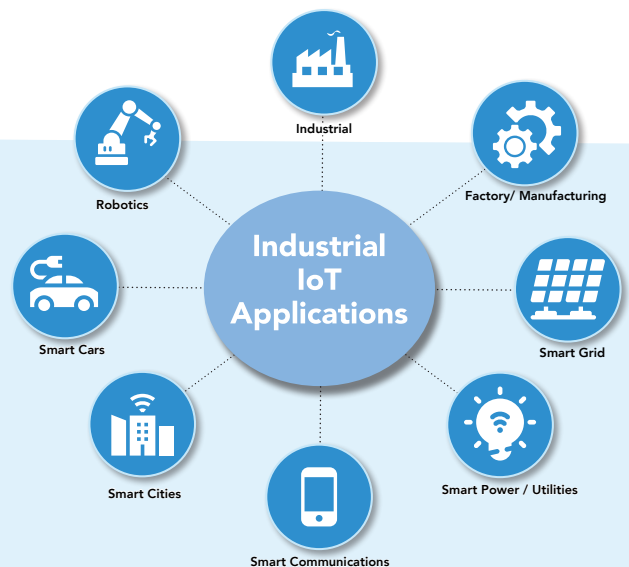
- 📶 Robots & Drones
- 📶 Connected & Cognitive networks, machines and devices
- 📶 Augmented & Virtual reality
- 📶 Artificial Intelligence & Machine Learning
- 📶 Just-in-Time supply chains with real-time track & trace
- 📶 Asset and location tracking
- 📶 Facility, Asset, Fleet and Worker location & contact tracing for safety
- 📶 Computer vision driven quality control systems
- 📶 Predictive maintenance solutions
- 📶 And many more

The Promise of Industry 4.0:

Industrial facilities have been increasingly reliant on the industrial Internet of Things (IIoT) to enable a highly productive and efficient operations environment.

Today, many manufacturing factories, energy plants, and even agricultural sites have hundreds of IIoT devices that help manage and streamline such operations.

Thus, at the heart of the Industry 4.0 revolution is the prolific use of hundreds of millions of IIoT sensors and other devices connected predominantly via a vast array of wireless technologies and protocols.



Wireless - The new invisible attack surface

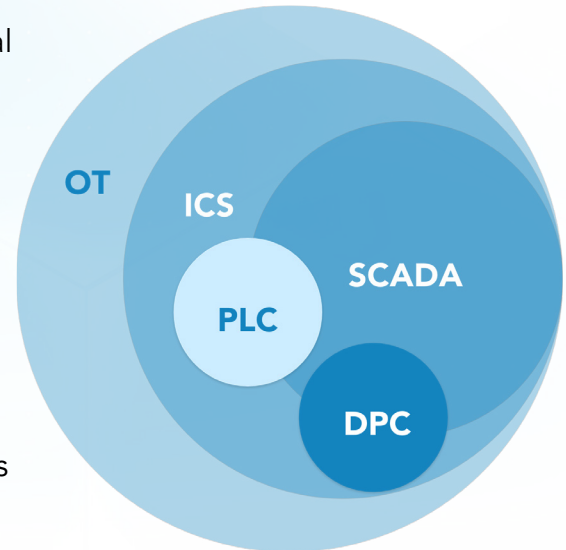
In industrial environments, operational technology (OT) and information technology (IT) are more interconnected than ever. This convergence provides industries with optimized automation and better visibility, among other benefits. Along with traditional enterprise and IT functions, the critical change with Industry 4.0 for IT is the communication flow associated with the collection and analysis of data that comes from within and outside of the industrial facility.

SCADA Primer:

The usage of OT computing systems to manage industrial operations such as production lines, mining, oil & gas exploration, electrical utility grids, etc. have been around for decades. Industrial Control Systems is a critical component of OT with the mission critical purpose of monitoring and controlling industrial processes - production material handling belts, power consumption on grids, alarms from building information systems, etc.

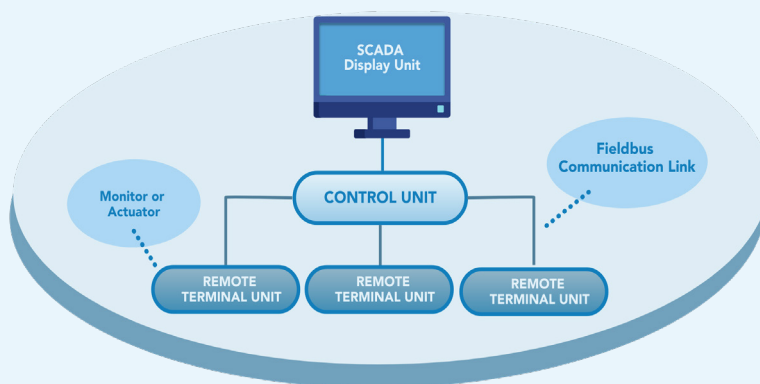
Most ICS systems are used as either continuous process control systems via programmable logic controllers (PLC) or as discrete process control systems (DPC) also via PLCs or some other batch process control device.

Industrial control systems (ICS) are often managed via a Supervisory Control and Data Acquisition (SCADA) systems that provides the user interface for management.



Other key components in the OT environment are Remote Terminal Units (RTU) that attach to the device/process being managed/monitored as well as Control Units which connect the RTUs in the SCADA system. The key point to note is that the RTU locations may be in the next room or hundreds of miles away. Using radio frequency communications is many times the only viable option in such mission critical applications. These communications systems are expected to have high availability for data processing and transfer in real-time with low latency.

Typical SCADA Configuration



With 80% of new IIoT deployments being wirelessly deployed, wireless is the new network and new attack surface. This applies to OT environments as the exponential use of licensed and unlicensed broad spectrum radio frequency (RF) for interconnectivity communication is a reality. The primary factors driving this trend being the remote location(s) and geographically wide spread of such operations. Other factors driving the growth of the market include increasing adoption of industrial robots, the growing demand for the smart automation solutions, and the increasing emphasis on regulatory compliance.

Additionally, 4G/LTE leased lines from carriers are being replaced with 5G connectivity as well as private cellular networks such as CBRS (Citizens Broadband Radio Service) are being considered for IIoT connectivity.

SCADA IIoT:

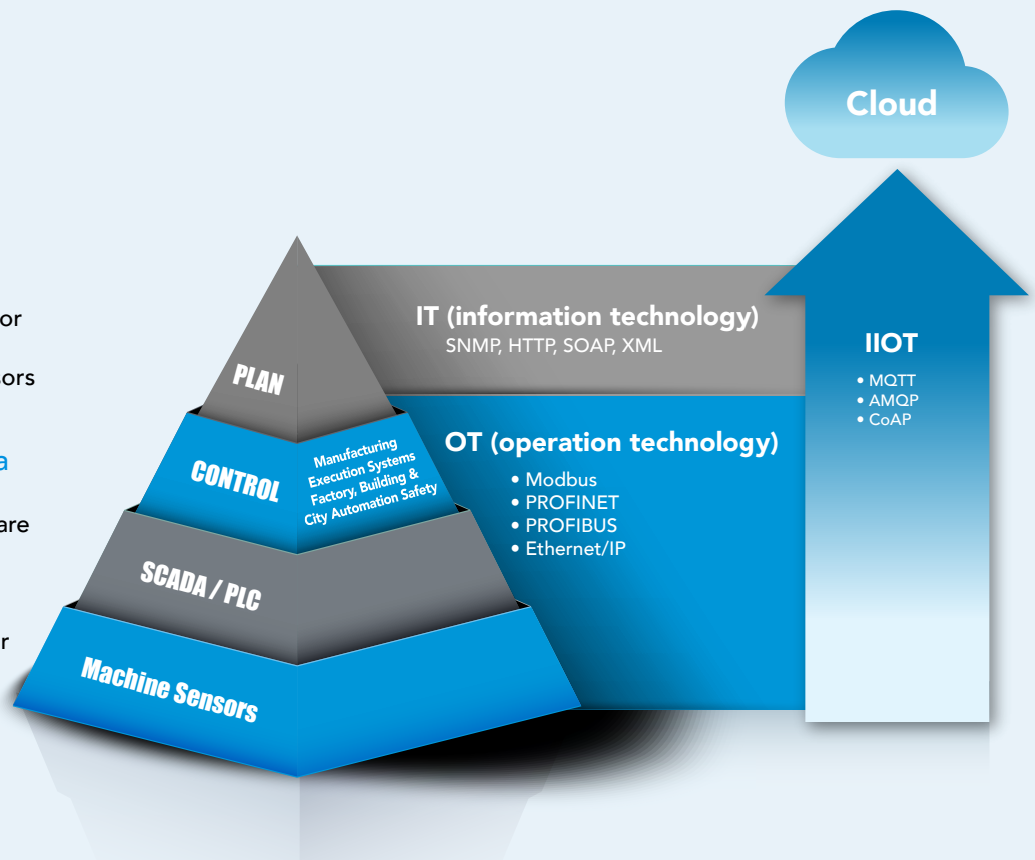
SCADA has served the industrial sector extremely well over the last five decades and will continue to be an important part of leveraging data and providing remote operating capabilities, however, the system does have its drawbacks.

Cloud-based and cloud-supported SCADA systems have become a more popular choice to alleviate the in-house maintenance or a computer-based approach. The cloud allows for more flexibility both in storage, cost, and scalability, and allows for data access from anywhere. While migrating SCADA to a more modern approach, the best future-proofed solutions leverage the internet. IIoT systems can be designed to integrate with SCADA to make the transition much easier. And in the long run, producing the kind of quality data that will power current technologies is more beneficial.

Bridging the gap from SCADA to IIoT isn't a plug and play replacement.

SCADA systems control key functionalities on a manufacturing floor - data collection and processing of the various control components using sensors and the PLCs or RTUs.

Furthermore, in addition to data communications through routers, servers, the historian, and into a software application – communications are now increasingly taking place over cellular networks into the cloud directly. While such streamlined and optimized cellular communications are easier and faster to set up, they are now a new attack surface for bad actors to exploit.



This new approach now opens up security concerns associated with 4G/5G networks as well as Broad-Spectrum IIoT networks whereby even a simple man-in-the-middle attack or rogue cell tower attack can create havoc.

Industry 4.0 IIoT:

As ICS devices become increasingly wirelessly connected, they also become increasingly vulnerable. By and large, industrial organizations are underprepared for digital convergence of their IT and OT converged environments; the rate of new connected devices is outpacing the rate of device security.

Physical equipment that was once only mechanical is now entering the fast-growing world of the industrial internet of things (IIoT). Having smart machinery improves efficiency, but without the proper precautions - it also offers cybercriminals remote access and attack opportunities they did not have before.

Unique RF in Industry 4.0 Environments

DOMAIN	DESCRIPTION
Instrumentation	IEEE 802.15.4 standards - ISA 100.11a, WirelessHart (IEC62591:2016), IEC 62601, and ZigBee. High performance standards built on IEEE 802.11 - Factory Automation (WIA-FA) IEC 62948.
Wide Area Sensing	LoraWAN and Sig Fox as well as moded of 4G/5G cellular radio standards.
Enhanced Communications	Private LTE: Licensed 4G/5G, Unlicensed UNII3; Shared CBRS
Other Commercial	Satellite, cellular, directional microwave data links, optical (visible light, and land-mobile radio)
Custom Solutions	Radiating coaxial cable and tropo-scatter solutions that are designed for unique mission criteria

The main drivers for exponential adoption of Industrial IIoT solutions are:

1. Cost Reduction:

- a. Optimized inventory management
- b. Real-time asset tracking
- c. Reduced downtime
- d. Optimal energy use

2. Mass Customization

- a. Tracking inventory
- b. Just-in-time manufacturing operations
- c. Real-time forecasting
- d. Optimized shop floor scheduling & routing

3. Improved Safety

- a. Real-time worker safety monitoring
- b. Elimination of risks and hazards
- c. Protections for citizens
- d. Split-second first response

“ If policy makers and businesses get it right, linking the physical and digital worlds could generate up to \$11.1 trillion a year in economic value by 2025. ”

Source:
<https://www.mckinsey.com/the-internet-of-things>

The Challenge of Security in Industry 4.0:

As with most things, new methods and the use of new technology introduce new challenges.

Many of the latest and most advanced production systems in Industrial and Manufacturing environments today, utilize the benefits of hyper-connected systems and devices to negotiate and monitor real time processes that run the environments production systems. But these facilities now also have to defend against new threats that take advantage of weaknesses and other attack vectors that come with the adoption of new technology.

According to Gartner, **80% of these systems and devices are wirelessly enabled today** creating a massive security blind-spot.

Along with the ubiquitous presence of wireless communications technologies in the Industrial environment, come with new challenges and unintended consequences that must be addressed. In order for the promise of Industry 4.0 to be fully realized, the industry must first acknowledge the risks, so that they may adequately address them before they become a problem.

Industry 4.0 makes IIoT-integrated facilities more susceptible to cyberattacks due to the prolific use of wireless and RF for connectivity. Closed systems that were once air-gapped are now online as wireless broad spectrum, 802.11, Bluetooth and Cellular communications has made it easier for operational performance efficiency and competitive advantage.

From an information and network security perspective the risks lay in the inter-hyper connectivity of all the devices in the Industrial environment that rely on wireless technologies to function.

These devices are virtually everywhere in the Operational Technology (OT), Internet of Things (IoT), and Information Technology (IT) environments. As we see these three worlds collide OT/IoT, and IT, there is a significant lack of visibility to monitor heterogeneous wireless environments. Very often these IIoT devices use non-standard frequencies and protocols to communicate while still utilizing network access.

Wireless OT and IoT networks have fundamentally created the world's largest and most vulnerable collective attack surface whereby every device is a point of entry into the network. Own the device, own the network.

Industrial organizations are still relying on legacy wired-side security tools to secure ICS systems, however, these solutions have proven to be ineffective, so a new approach is required in order to detect and assess risk.

While these legacy tools are effective at monitoring the wired network for security exposure states, they are completely blind to what is happening "off the wire", or at the wireless link layer. If a man-in-the-middle attack, phishing attack, or device identity theft happens over the air, the production network and everything behind it are oblivious to attack event which could lead to data exfiltration and ultimately data breach.






While IIoT holds the promise to deliver real-time monitoring, control, measurement and other analytics, a robust and secure underlying communications infrastructure is at the forefront of all deployment discussions today.

While OT and IT both need to protect their systems and data from compromise, OT cybersecurity professionals tend to approach their systems differently than traditional IT because they have varying priorities.

ICS control engineers can be reticent to upgrading their equipment even when it would enhance their cybersecurity posture. This is because their focus on maintaining constant uptime and measuring performance characteristics such as overall equipment effectiveness rivals other priorities like running the latest firmware. The three imperative tasks that dominate the OT cybersecurity conversation are; safety, quality and uptime.

With the convergence of wireless IIoT into the OT environment, this has reprioritized the tasks as wireless now creates the invisible espionage threat to the business.

LOCH Security for Industry 4.0 IIoT

- 
Wireless IIoT Deployments: In environments where Wireless/RF is used for connectivity, LOCH is the single truth for device inventory. Any device that is emitting an RF signal, will be identified and located.
- 
IIoT Security: Cybersecurity tools that manage such devices are based on network-centric solutions that use deep packet inspection and protocol dissection of flows from the subnets/VLANs. LOCH's auto discovery will find devices that were missed due to incorrect subnet/VLAN configuration.
- 
IIoT Device Scanning: LOCH solutions includes an 'outside-in', continuous edge vulnerability management solution to provide security validation of devices preventing misconfigurations of open ports, services and threats..
- 
4G/5G Security: In addition to traffic monitoring against established baselines for anomalies, LOCH can sense the presence of adjacent RF channels to thwart man-in-the-middle hijack attempts.
- 
LTE Connectivity: LOCH delivers the ability to monitor traffic from SIMs to alert on excessive use and changes in Device/SIM association.



The future battlespace is constructed of not only ships, tanks, missiles, and satellites, but also algorithms, networks, and sensor grids. Like no other time in history, future wars will be fought on civilian and military infrastructures of satellite systems, electric power grids, communications networks, and transportation systems, and within human networks. Both of these battle- fields—electronic and human—are susceptible to manipulation by adversary algorithms.



Courtney Weinbaum and Lt. Gen John N.T. "Jack" Shanahan | "Intelligence in a Data-Driven Age," (Joint Force Quarterly 90, 2018)

IloT has created the world's largest attack surface, the scope of which is only broadening with exponential growth in the deployment of 5G. Today's networks and organizations were never built to handle this extraordinary volume, velocity, and hyperconnectivity of IloT technologies.

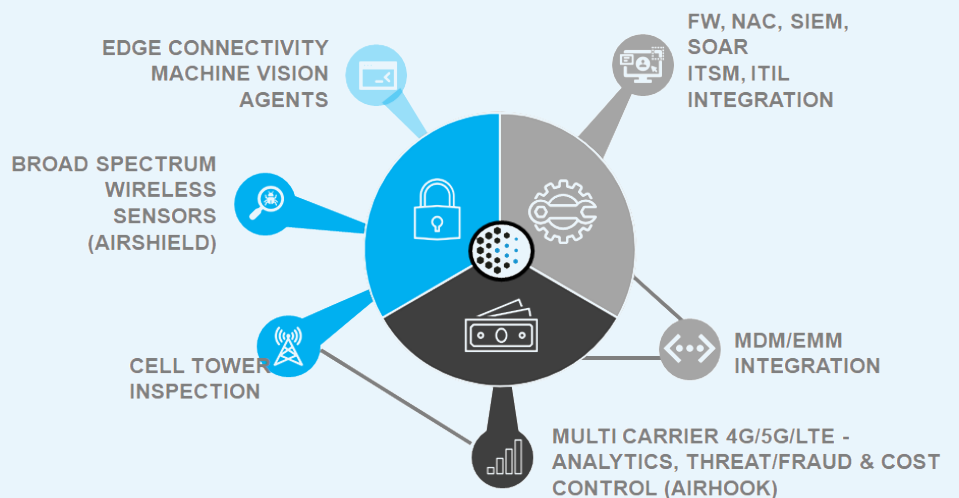
The Solution:

Loch has created the world's most intelligent wireless security platform, sensing all environmental communications in the customer's RF spectrum from 100MHz to 6GHz. Loch deploys its patented AirShield sensor in the customer's physical environment where it scans the airwaves for wireless communications irrespective of the device manufacturer, native OS, communications frequencies, channels, or protocols.

The AirShield sensor gathers local intelligence from the air and passes relevant event data back to the LOCH platform in the cloud where Loch's machine learning engine works cooperatively with the AirShield sensor to perform real time device discovery, asset classification, behavioral analysis, deviation to policy investigation and enforcement, vulnerability assessment, and threat detection.

Why LOCH? - Wireless Machine Vision™

LOCH Wireless Machine Vision™ platform provides next-generation wireless AI driven threat intelligence across 3G/4G and 5G deployments, broad-spectrum wireless IoT, Citizens Broadband Radio Service (CBRS) as well as 802.11/Bluetooth WiFi environments by providing customers with full IoT discovery, asset classification, risk analysis and actionable remediation capabilities based on a Zero-Trust framework.



- Real Time Analytics**
- Device Discovery
 - Asset Classification
 - Behavioral Analysis
 - Policy Enforcement
 - Vulnerability Assessment
 - Threat mitigation
 - Cost management (WAN)

Key Differentiators

- Single pane of glass to manage ALL wireless threats across cellular 3G/4G/5G, broad-spectrum wireless, CBRS and 802.11/Bluetooth Wi-Fi devices
- Early Warning System - detecting threats before they hit the wired network
- Edge IoT Vulnerability Scanning to identify exposed threats before they are abused
- Monitor Enforce Zero-Trust Policies and “No Phone” Zones
- Deployable in air-gapped environments also

Core Competencies

- Software defined radios to detect broad spectrum RF
- Comprehensive classification of all assets in the environment and continuous Intrusion Detection
- Wireless Security Threat Research for rapid anomaly detection
- Decoding of all IoT operating systems and protocols
- Zero-Trust Policy Enforcement
- Rogue Cellular Tower and Stingray Detection
- API integrations for threat mitigation & remediation

Security Posture and Operational Efficiency for IIoT Devices



Critical Infrastructure - crucial for delivering essential resources and services. Eliminate threats using broad spectrum RF backdoors.



Factory and Process Automation - critical for productivity and efficiency. Ensure network segmentation and unauthorized access.



Long Range Radio Communications Over Wide Areas - Ensure proper network segmentation and detect hijacked relay stations.



Network Infrastructure - wired and wireless network correlation for misconfigurations that create blind spots for cybersecurity initiatives.



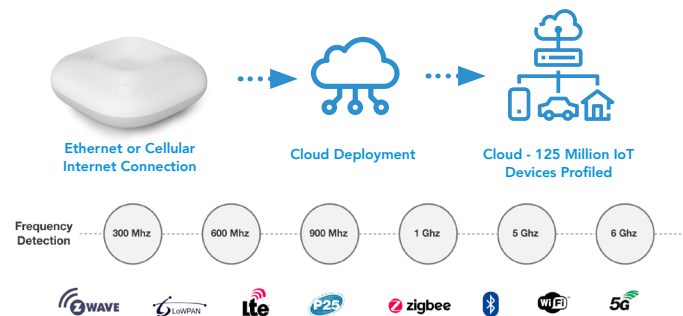
Sensors - critical for facility, asset and worker safety. Ensure proper network segmentation and block unauthorized access.



WiFi USB - Check for all communications into or out of the network for data loss or potential exploitable backdoors for lateral attacks.



Rogue Cell Towers - Validate 4G/LTE/5G or Private LTE communications for exfiltration and/or malware/process injection.



Summary:

Industry 4.0 promises hyper automation of industrial and manufacturing systems, evolving to a semi-autonomous state, replacing humans in many cases with machine speed decisions and processes that significantly optimize operations, increase quality outputs, and reduce error rates and downtime.

When these systems are integrated with ERP and other supply chain systems, then the entire organization gets closer to realizing the vision of frictionless, automated production. Businesses must recognize the sophistication of their extended networks as they reach further outward to increase optimization through technology. They must also recognize the risks inherent in the nature of their far and wide wireless environments. Change around the way they view and design their businesses, must also include changing the way they view and address the security of their production systems and devices.

The threat of wireless compromise is invisible, but very real. LOCH has the answers.