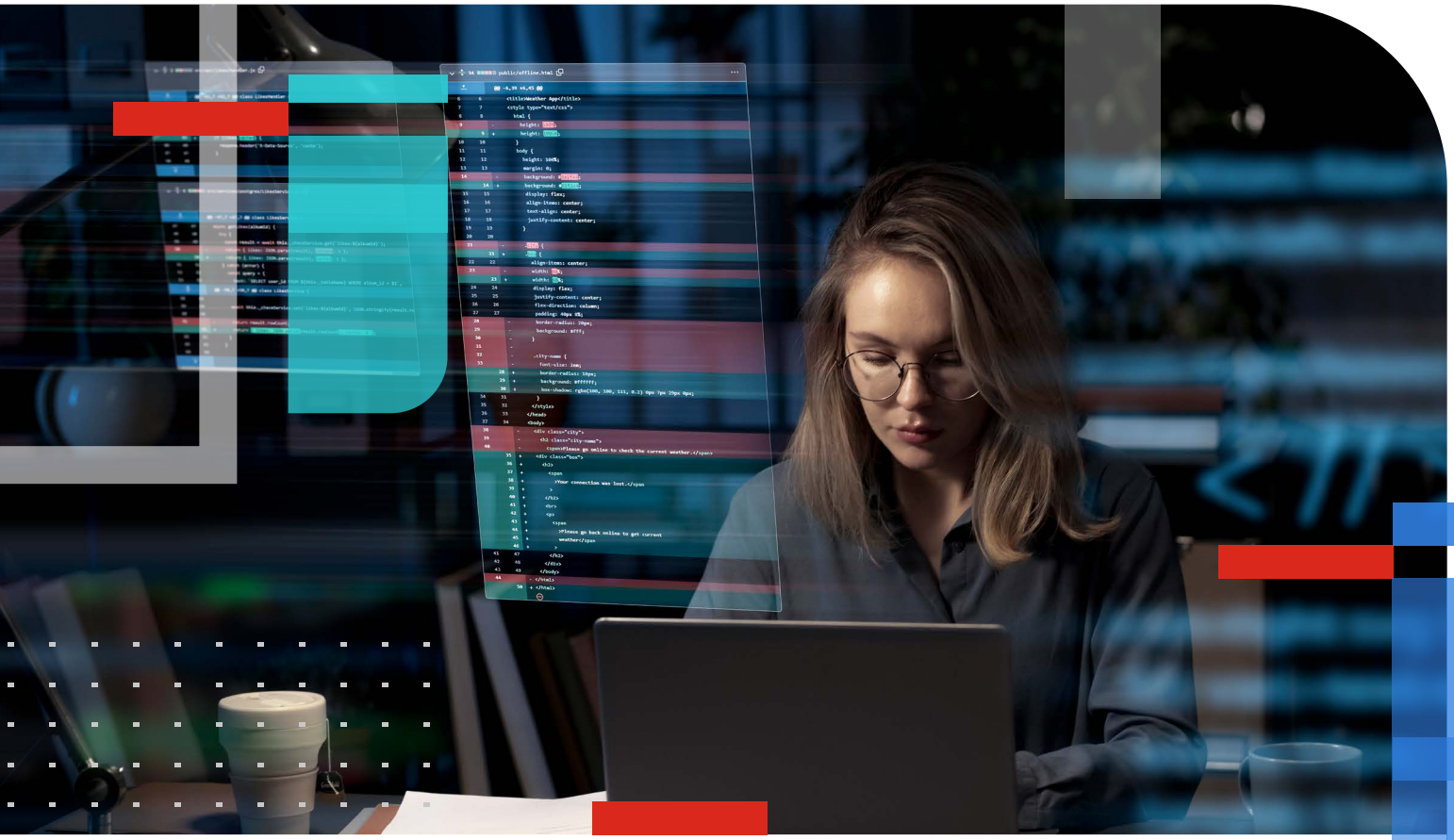
WHITE PAPER

Building Resilience: Exploring Smart Infrastructure and Its Security



Executive Summary

Smart infrastructure, which converges the cyber and the physical aspect of a system, is revolutionizing the way that people, technology, and infrastructure function together. In fact, the global smart infrastructure market is projected to grow from $97.20 billion in 2021 to $434.16 billion in 2028 at a CAGR of 23.8%.[1] Integrating digital technologies into physical infrastructure can enhance efficiency, sustainability, and quality of life through results like traffic-reduced congestion, lower energy consumption, and improved community services.

However, as connected sensors, equipment, and data become more prevalent in the cyber-physical landscape, they create additional entry points for potential security threats. These vulnerabilities extend beyond just manufacturers and include inadequately trained operators, inaccurate processes, and even compromised equipment deliberately inserted in the supply chain at low prices to attract budget-strapped buyers. How can adopters of smart infrastructure, from individual providers to cities that depend on multiple smart systems, recognize and mitigate risk while still driving innovation?

Threat researchers recorded 112.3 million instances of IoT malware in 2022[2]. Smart infrastructure leverages extensive use of both the Internet of Things (IoT) and the Industrial Internet of Things (IIoT).

IT-OT Convergence Comes to Infrastructure

Infrastructure comprises the various systems, facilities, structures, and services that support the functioning of a society, economy, or organization. Some infrastructures are critical to a nation or society, and some aren't. Critical infrastructure—defined on the United States Cybersecurity and Infrastructure Security Agency (CISA) website as "those assets, systems, and networks that provide functions necessary for our way of life"—consists of everything from power plants, roadways, and water supply systems to schools, wastewater treatment plants, and hospitals.[3] In other parts of the world, the critical infrastructure may be referred to as critical national infrastructure (CNI), such as in the U.K.[4] However, non-essential transportation, public spaces like parks or venues, and community Wi-Fi service are examples of infrastructure that is not considered critical.

While some infrastructure is critical and some is not, all infrastructure can be smart. Infrastructure has not been left out of the digital transformation wave that has been sweeping organizations and industries as they seek to leverage the benefits of connectivity, data exchange, and automation. While the digital transformation movement may have originated with information technology (IT), operational technology (OT) began to make the shift as well. In fact, IT and OT have been on a path of increasing convergence, uniting traditional OT with modern information and communication technology. This shift has brought many benefits to businesses like manufacturers looking to stay competitive, such as increased efficiency, enhanced productivity, improved quality and flexibility, and cost reduction.

Infrastructure operators are now looking to reap similar benefits. Just as smart manufacturing converges physical operations (such as in OT) with digital systems (such as in IT), smart infrastructure is simply a combination of physical and digital infrastructure. This involves the application of Internet of Things (IoT) and Industrial Internet of Things (IIoT) sensors, connectivity, automation, and intelligent data analysis using tools such as artificial intelligence (AI) and machine learning (ML) to monitor, control, and optimize various aspects of infrastructure operations. By 2027, it's expected that there will likely be more than 29 billion IoT connections,[5] while the IIoT market size is projected to reach $1742.8 billion by 2030.[6] The orchestration of these physical assets with sensors and other digital components is also referred to as a "Cyber-Physical System" (CPS).

New Innovations Bring New Security Challenges

Smart infrastructure leverages digital technologies to enable better monitoring, analysis, and management, resulting in enhanced safety, reduced costs, increased resilience, and more sustainable operations. The deeper insights captured through the data generated from smart infrastructure will also inform design improvements that can offer better functionality and whole-life value for future new or upgraded infrastructure. However, the connectivity that smart elements require to generate and transmit data also alters the traditional air-gapped environments—exposing infrastructure to new challenges and risks.

- **Security threats -** While data security has been a primary concern with connected IT, a breach of smart infrastructure can have devastating results. Consider the risks to life and property if a smart electrical grid was rendered inoperable or the controls of a dam were altered. Because of the potential for serious impact, smart infrastructure is a high-value target for malicious actors such as rogue nation-states, cybercriminals, hacktivists, and terrorists. Disgruntled insiders or even unaware, click-happy end-users can also pose risks.
- **Data privacy concerns -** Smart infrastructure is driven by data. Operations involve the collection, transmission, storage, and processing of large amounts of data. Sources of that data may be governments, businesses, or private citizens—and it can often include sensitive information. Whether the fear is a compromise of data via a malicious breach, or simply an accidental release or exposure, protection of data collected via smart infrastructure is a major concern, especially given that the global average cost of a data breach is $4.45 million.[7]
- **Standards and interoperability issues -** Smart infrastructure involves multiple entities, systems, and devices that need to communicate and exchange data seamlessly. The absence of uniform standards across different domains and sectors poses a significant challenge. Varying standards make it difficult for different components of a smart infrastructure to interoperate effectively, as seamless data sharing, control, and coordination is a crucial requirement. Integrating and properly securing diverse technologies and legacy systems can be a complex and challenging undertaking.

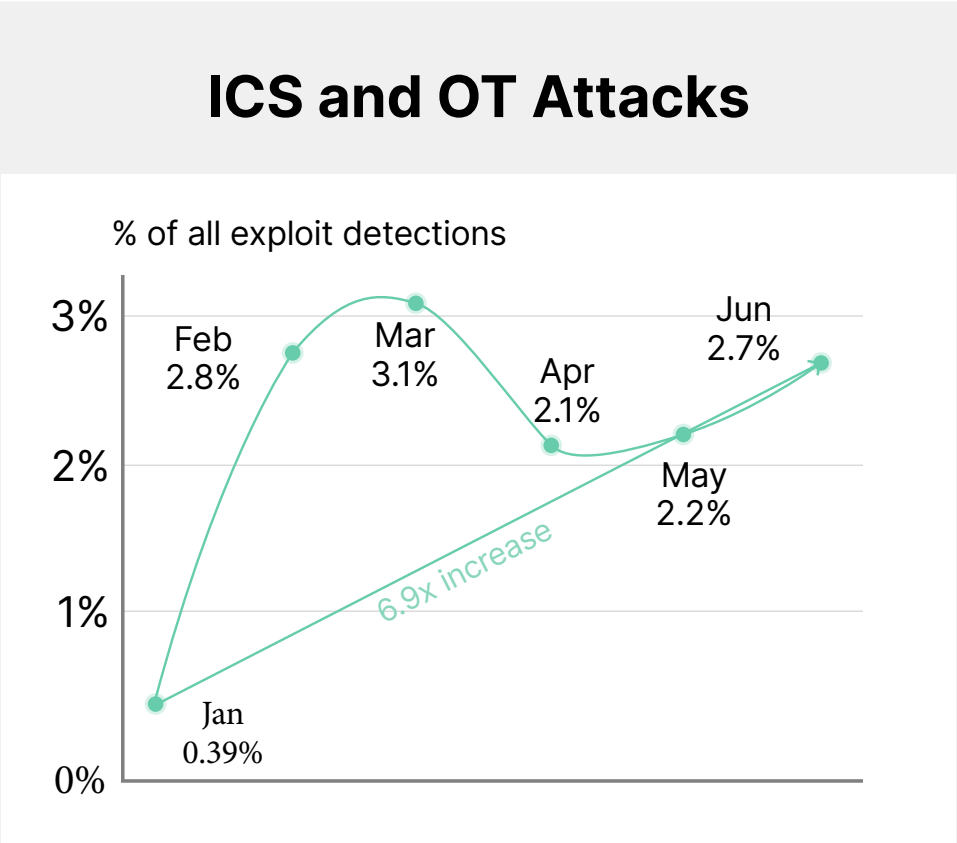


Figure 1: Attacks targeting industrial control systems (ICS) and operational technologies (OT) didn't occur at high volume but trended up over the first half of 2023. Half of organizations saw ICS or OT exploits, with energy and utilities ranking among the top targets.[8]

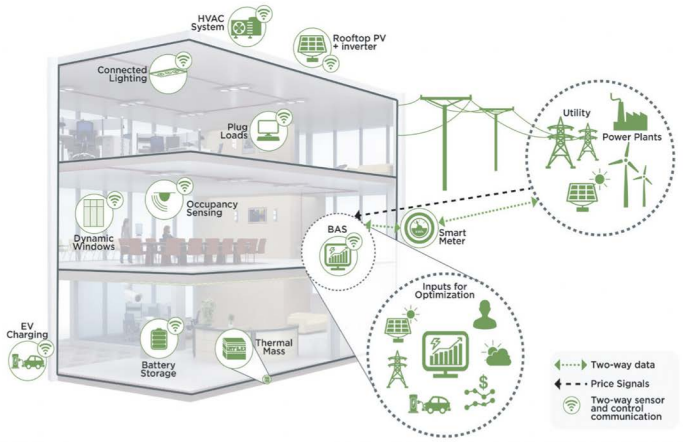
The convergence of the cyber and physical ecosystems that is part of smart infrastructure greatly expands the attack surface of any infrastructure through techniques such as social engineering, ransomware, and malware.

Smart Infrastructure Examples and Vulnerabilities

Smart infrastructure offers numerous, benefits and improvements to the functioning and sustainability of campuses, communities, cities, states, and even nations. Some common examples of smart infrastructure at work—and key security issues—include:

- **Power grids -** A smart grid can create a more flexible, reliable, and sustainable electrical infrastructure capable of meeting the evolving energy needs of modern society. Advanced electrical grid infrastructure utilizes modern communication real-time data exchange, monitoring, and automation technologies to enhance the visibility, ease of control, efficiency, reliability, and sustainability of electricity generation, transmission, distribution, and consumption. Key security issues include ensuring data privacy of consumers as well as grid security.
- **Water systems -** Smart water infrastructure can be used to manage clean water supply or wastewater treatment and disposal. By utilizing sensors, data analytics, and communication networks, operators can monitor, control, and automate various aspects of water management to enhance water management practices, conserve resources, reduce operational costs, and provide reliable and safe water services to users. As with smart grids, key security points include data privacy as well as tamper-free operation of the water systems.
- **Transportation -** Smart transportation integrates information and communication technologies for efficient, connected, sustainable systems, enhancing life quality, mobility, and goods movement. Sensors, cameras, and connected vehicles collect real-time traffic data for updates, collision avoidance, adaptive signals, and coordinated management, ensuring safe commutes. Real-time info, routing, payments, and Wi-Fi enhance public transport, making it efficient, convenient, sustainable, and appealing to commuters. Data privacy, system security, and uninterrupted operations are all key aspects of securing smart transportation.
- **Buildings and cities -** Smart buildings and cities rely on connectivity, data analysis, and automation. A smart building optimizes operations and enhances occupants' experiences. In contrast, a smart city extends benefits to the urban environment, including infrastructure and services. Smart buildings use technology to improve efficiency, sustainability, safety, and functionality. Sensors and automation control lighting, temperature, physical security, and more. Key aspects of a smart city include efficient transportation, energy management, governance, service availability, and public safety.

  It's important to remember that the more systems involved in smart infrastructure, the more complex security becomes. The sheer scale of a smart city, for example, means many more surfaces are vulnerable to attack, and with greater impact—up to and including loss of life.



Grid-interactive efficient building. Image courtesy of Navigant Consulting.

Figure 2: The convergence of the cyber and physical ecosystems that is part of smart infrastructure greatly expands the attack surface of any infrastructure through techniques such as social engineering, ransomware, and malware. This example highlights the the potential attack vectors in a Grid-Interactive Efficient Commercial Building from the Department of Energy.[9, 10]

Seven Factors That Influence Successful Solutions

All infrastructure providers must carefully balance the need for innovative, efficient smart technologies with the risks to security and privacy protection. When you are considering cybersecurity solutions, consider the seven factors below. While point solutions may be able to cover one or two, you can improve value and ease of use by selecting a solution that covers most or all of these.

1. **Integration -** Point solutions can add up in terms of cost and can be difficult to manage. An end-to-end, integrated cybersecurity platform that covers IT and OT, cyber and physical security, plus data centers and multiple clouds is ideal.
2. **Monitoring and management -** It's often tough to find and retain the expertise necessary to properly secure smart infrastructure. Consolidating networking, cybersecurity, and physical security functions into a single platform, with full visibility and control of the infrastructure, offers holistic security and reduces the time to detect and respond to threats.
3. **Endpoint protection -** Budget-stretched smart infrastructure owners and operators must often work with their existing investments. Because legacy systems are often not consistently patched, look for a solution provider that delivers real-time threat protection, both pre- and post-intrusion, even on legacy systems with limited system resources.
4. **Network optimization -** Remote operations are endemic to smart infrastructure. A solution provider who can optimize networks and provide application steering based on bandwidth, latency, jitter, and cost can also drive down the costs of running dedicated leased lines to remote operations.
5. **Enhanced network visibility -** Securing smart infrastructure that relies on modern OT environments begins with establishing continuous visibility of every asset connected to the network, both wired and wireless. Monitoring the activity of these devices will protect the critical OT systems from a rising tide of internet-based threats. An ideal solution monitors network traffic and provides a foundation of transparent visibility and policy-based control to protect the network from unwanted visitors.
6. **Better network segmentation -** Owners and operators often find that there is insufficient separation and control of the IT and OT networks that make up smart infrastructure. They must deploy a solution that provides the right access for the right people when they need it. Managed through multi-factor authentication access, it should observe user behaviors and look for actions not typically associated with that user, such as zero-trust network access (ZTNA).
7. **Ruggedized hardware -** Some smart infrastructure may require environmental considerations. Heat, cold, moisture, and other climate variations, plus other issues like vibration, can be a challenge. Look for a vendor with a broad selection of ruggedized appliances to fit all environmental needs.

Enabling Benefits, Minimizing Risks

With the global smart city technology market expecting a 10.7% compound annual growth rate (CAGR),[11] it's critical to start providing comprehensive security for smart infrastructure now. However, the relative newness of the field means there is often a skills and experience gap in the labor pool. Instead of a solution vendor, consider looking for a security partner, like Fortinet, with expertise in addressing the unique challenges and vulnerabilities associated with every aspect of these complex environments. Once smart infrastructure owners and operators digitally and physically secure their critical systems, data, and operations, they—as well as the constituents whom they are supporting—can embrace every benefit while worrying less about security risks.

[1] "Smart Infrastructure Market Size, Share & COVID-19 Impact Analysis," February, 2022.

[2] "Why Attackers Love to Target IoT Devices," VentureBeat, June 9, 2023.

[3] "Critical Infrastructure Security and Resilience," Cybersecurity and Infrastructure Security Agency CISA, September 21, 2023.

[4] "Critical National Infrastructure," NPSA, September 21, 2023.

[5] "State of IoT 2021: Number of Connected IoT Devices Growing 9% to 12.3 Billion Globally, Cellular IoT Now Surpassing 2 Billion," IoT Analytics, May 18, 2022.

[6] "Industrial IoT Market Size to Surpass USD 1742.8 Bn by 2030," September, 2022.

[7] "IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend despite Soaring Breach Costs," IBM Newsroom, July 24, 2023.

[8] "Global Threat Landscape Report," Fortinet, August 7, 2023.

[9] Dr. Micahel Chipley and Tim Conway, "Next-Generation Cybersecurity for Buildings," SANS, October, 2021.

[10] "Grid-interactive Efficient Buildings," U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy, April, 2019.

[11] Sarah Wray, "Smart City Market to Reach $300 Billion by 2032," Cities Today, May 3, 2023.

November 8, 2023 9:28 PM

123456-0-0-EN