

# An Overview of Cybersecurity Best Practices for Edge Computing

## White Paper 12

Version 1

by Daniel Paillet, CISSP, CCSK, CEH

### Executive summary

An edge IT environment, such as those found in industrial factories, can have a plethora of distributed endpoints providing a large attack surface for cyber criminals and hackers. Managing this risk requires the proper implementation of network segmentation and various security appliances. Edge computing involves connecting endpoint devices and systems to a network. These connections offer potential avenues of attack for hackers. Mitigating these cybersecurity risks requires solutions that encompass security best practices for devices, networks, and applications. This also requires actions on the part of the user to maintain their required level of cybersecurity. This paper discusses best practices for four key elements of an effective edge computing cybersecurity strategy including: (1) selection criteria for devices, (2) secure network design (3) device configuration, and (4) operation & maintenance to reduce the risk of breaches. Examples are provided as well as references to related cybersecurity standards. Note: While this paper is largely explained in the context of industrial edge applications, the concepts discussed are applicable to all edge IT environments.

RATE THIS PAPER



## Introduction

Incidents of cyber-attacks against IT networks have been intensifying globally. This combined with increasing adoption of IoT devices, the convergence of IT and OT (operations technology) networks, and the use of cloud-based management and analytic systems has led to cybersecurity being an urgent concern for edge IT owners and operators. Cyber-attack risks are worsening due to the increasingly distributed nature of IT. The edge computing trend is putting more and more endpoint devices at the edge of computing networks away from more highly secured, centralized data centers. This has increased dramatically the available attack surface for cyber criminals and hackers.

This paper provided guidance on how to secure edge IT installations and their endpoint devices. However, this is not a hardening guide, per se. The first section will briefly explain the edge computing trend and how this is increasing the risk of cyber-attacks. And then an overview of best practices is provided for each of these four elements:

1. Device selection criteria
2. Secure network design
3. Device setup / configuration
4. Operation and maintenance

These practices reduce the risk of breaches. Examples for these practices are provided along with associated cybersecurity standards. Note that physical security and internal staff threats are critical considerations for reducing breaches but are not the focus of this paper.

## Why edge?

The advent of the cloud has enabled advanced features in Operational Technologies (OT) and Information Technologies (IT). For example, OT is using features like Industrial Internet of Things (IIoT) in factories, smart metering in solar farms, and safety improvement in oil & gas. IT is using features like IoT, smart shelves in retail, and smart cities. Thus, we are seeing a combination of on-premise IIoT / IoT devices and systems sending information to the cloud, creating potential latency which could impact availability of resources and information. Timely information retrieval is critical in business decision making, and edge computing mitigates latency to address these issues.

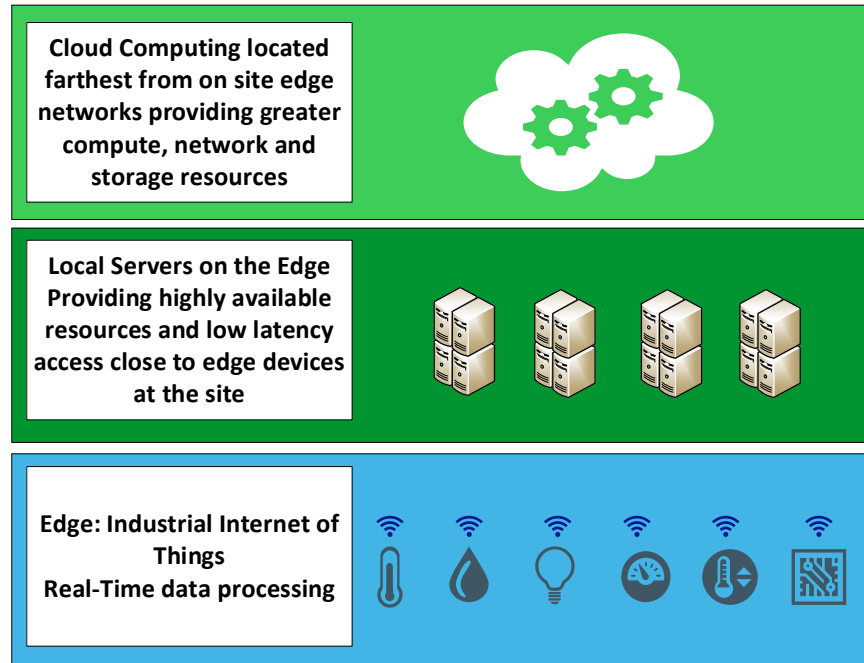
Specifically, latency is reduced by inserting computing and storage capacity on the network edge, in order to lower data transport time and increase availability. Edge computing brings bandwidth-intensive content and latency-sensitive applications closer to the user or data source. For more information, see White Paper 226, [The Drivers and Benefits of Edge Computing](#).

Edge computing has evolved into a framework to mitigate against loss of data from latency and to provide greater bandwidth (see **Figure 1**). The reason for moving towards edge computing is clearly explained in the following:

“An edge location is a computing enclosure/ space/ facility geographically dispersed to be physically closer to the point of origin of data or a user base. In other words, for an Edge to exist there must be a hub or a core; therefore, dispersion of

computing to the periphery would qualify as ‘Edge computing’ and the physical enclosure/ space/ facility can be defined as the ‘Edge facility’.”<sup>1</sup>

This technology supports customers’ demands for lower latency by locating workloads on the Edge of the network, at the customer site, to support the instantaneous aggregation of data and processing.



**Figure 1**  
Example of edge to cloud

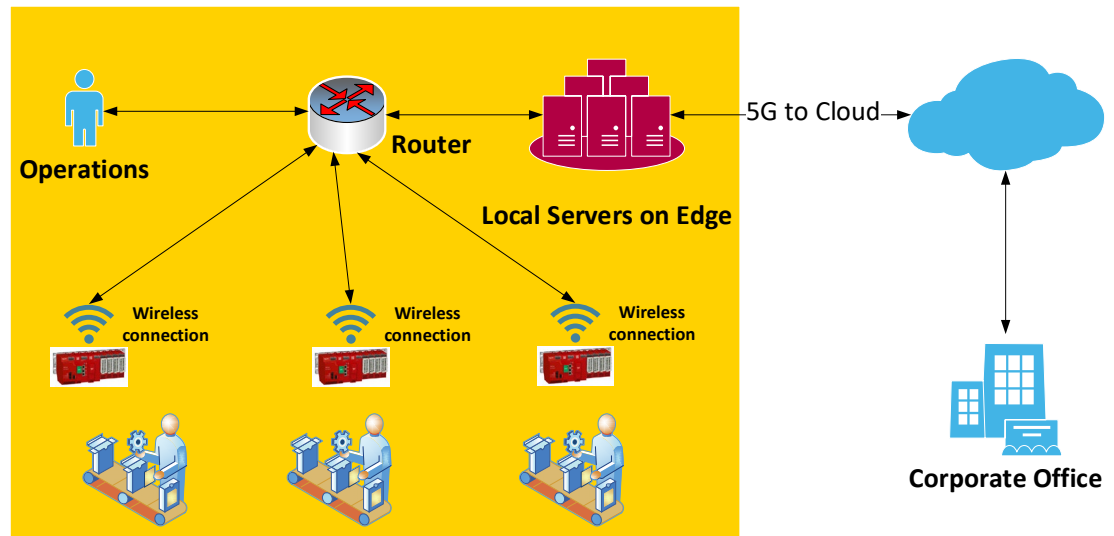
Several industries have already implemented edge computing technologies like IIoT. For example, Smart grid applications have used edge computing to allow utilities to monitor, manage, and control various aspects and functions of the electrical infrastructure. Real-time analytics and capabilities would not be possible without implementing an edge computing framework at the physical network level.

There are many benefits enabled by edge computing, a few of which are discussed here for three industrial applications; Smart grids, oil & gas, and factories. Integration of edge computing into Smart grids is making impacts in solar farms, residential solar, and smart metering, providing data that can assist management decision making for distributed electrical systems. It can also have positive impacts on safety in such critical industries as oil and gas. The resources deployed on the Edge can enable oil & gas facility operators to remotely monitor all incoming data coupled with real-time analytics. This allows them to mitigate against malfunctions that could impact life and safety in a highly optimized and timely manner.

The example in **Figure 2** illustrates a scenario where a factory aggregates information coming from the manufacturing floor. The aggregated data is pushed out from the local edge servers to the cloud. Once it is in the cloud, the corporate office can review the information to make well-informed business decisions in conjunction with local operations.

<sup>1</sup> <https://imasons.org/imasons-blog/can-you-define-the-edge/>

**Figure 2**  
5G example of manufacturing sending data to the cloud via local edge servers



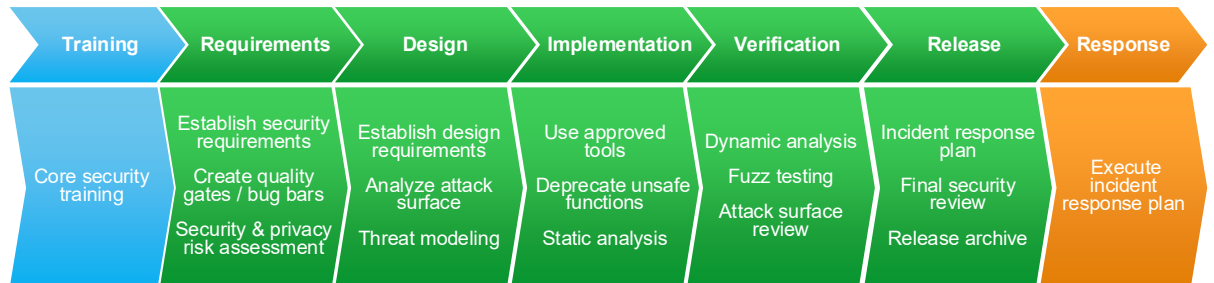
Like all applications that depend on and are connected to the internet, cybersecurity plays a critical role in edge applications by helping to avoid weak links. **Even small edge endpoint devices like a UPS, security camera, environmental sensor, and similar devices can represent a weak link to the overall, larger enterprise network.** This paper focuses on reducing the risk of cyber-attacks through these edge devices. Each element will now be presented along with the associated best practices for mitigating these risks.

## Device selection criteria

Microsoft introduced the Security Development Lifecycle (SDL) to consider security and privacy concerns throughout the entire software development process. It's important to validate that vendors develop their applications, devices, and systems<sup>2</sup> following a well-implemented SDL. A properly integrated SDL process can reduce vulnerabilities and coding errors with the necessary mitigations to secure the application, device, and system, while, improving the reliability of the software and firmware.<sup>3</sup> The SDL process (composed of seven phases) standardizes best practices in security throughout the entire development process to enhance and build highly secure software. **Figure 3**<sup>4</sup> illustrates the seven SDL phases.

SDL practices are updated to address new scenarios and use cases including the cloud, Internet of Things (IoT), and can also be applied to edge computing.

**Figure 3**  
Seven phases of the Secure Development Lifecycle that vendors should follow for the products and services they offer



<sup>2</sup> Monitoring software is an example, of an application, a web card is an example of a device, and supervisory control and data acquisition (SCADA) is an example of a system.

<sup>3</sup> <https://www.microsoft.com/en-us/securityengineering/sdl> (As seen 11/11/2020)

<sup>4</sup> <https://social.technet.microsoft.com/wiki/contents/articles/7100.the-security-development-lifecycle.aspx> (As seen 1/5/2021)

Another standard, IEC 62443, is accepted worldwide in defining security standards developed by industrial control experts. The standard is categorized into four parts as illustrated in **Figure 4**<sup>5</sup>.

- General
- Policies & Procedures
- System
- Component

|                                  |                                  |                                                                           |                                            |                                       |                                       |
|----------------------------------|----------------------------------|---------------------------------------------------------------------------|--------------------------------------------|---------------------------------------|---------------------------------------|
| <b>General</b>                   | IEC 62443-1-1                    | IEC TR-62443-1-2                                                          | IEC 62443-1-3                              | IEC TR-62443-1-4                      |                                       |
|                                  | Terminology concepts and models  | Master glossary of terms and abbreviations                                | System security conformance metrics        | IACS security lifecycle and use-cases |                                       |
|                                  | <b>Policies &amp; procedures</b> | IEC 62443-2-1                                                             | IEC TR-62443-2-2                           | IEC TR-62443-2-3                      | IEC 62443-2-4                         |
|                                  |                                  | Establishing an industrial automation and control system security program | Master glossary of terms and abbreviations | System security conformance metrics   | IACS security lifecycle and use-cases |
| <b>System</b>                    | IEC TR-62443-3-1                 | IEC 62443-3-2                                                             | IEC 62443-3-3                              |                                       |                                       |
|                                  | Terminology concepts and models  | Master glossary of terms and abbreviations                                | System security conformance metrics        |                                       |                                       |
|                                  | <b>Component</b>                 | IEC 62443-4-1                                                             | IEC 62443-4-2                              |                                       |                                       |
| Product development requirements |                                  | Technical security requirements for IACS components                       |                                            |                                       |                                       |

**Figure 4**  
The four parts the IEC 62443 Standard

IIoT embedded devices, and IIoT software using the developmental process outlined by the IEC 62443-4-1 standard can provide a greater level of cybersecurity. While specific best practices are dependent on a given scenario, two broad examples of device selection criteria include:

- The ability to support secure protocols and communications
- The ability to implement (RBAC) Role Base Access Control

“This part of IEC 62443 (4-1) specifies process requirements for the secure development of products used in industrial automation and control systems as well as edge IT applications. It defines a secure development lifecycle (SDL) for the purpose of developing and maintaining secure products. This lifecycle includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life.”<sup>6</sup> Currently ISA/IEC<sup>7</sup> working groups around the world are working on updating and evolving the standard to address new frameworks and technologies

<sup>5</sup> <https://www.infineon.com/cms/en/product/promopages/iec62443/> (As seen 1/5/2021)

<sup>6</sup> IEC 62443-4-1 International Standard, page 11.

<sup>7</sup> ISA (International Society of Automation) and IEC (International Electrotechnical Commission)

such as virtualization, cloud, and edge computing. For more information on SDL, see White Paper 239, “[Addressing Cyber Security Concerns of Data Center Remote Monitoring Platforms](#)”

Note there are certification organizations that can be used to validate 62443 SDL compliance for component/systems and issue certifications stating as such.

## Secure network design

As edge computing evolves and grows so will the need to design network security for the devices and systems running in the edge. Securing access to the edge should include only providing access to resources via encrypted tunnels (i.e., VPN) and the proper implementation of firewalls and access control systems. Other best practices categories for securing networks and the edge include a defense-in-depth methodology and network segmentation.

### Defense-in-Depth Network (DDN)

Some people think that air gapping<sup>8</sup> provides an effective security solution; however, air gapping has been shown to promote a very false perception of security.<sup>9</sup> IT networks are converging with OT networks and will need to integrate edge computing into their respective enclaves. Instead of relying on air gapping, organizations are now moving toward a layered defense-in-depth approach to secure their systems and networks.

Edge computing has made tremendous enhancements to predictive maintenance, hospital patient monitoring, cloud gaming, content delivery, smart manufacturing, virtualized radio network and 5G by building resilience into operations and achieving the benefits of Industry 4.0<sup>10</sup>. However, security needs to be designed and deployed to protect the edge and its potential impacts on the IIoT and the cloud.

A Defense-in-Depth Network (DDN) approach secures edge computing functions and maintains availability of those functions and communication paths. Edge computing makes use of distributed networking, computing nodes, storage, and safety control systems. The challenge is developing the correct security to support the business while protecting the edge from untrusted traffic. Embracing an agile methodology to fulfill the requirements is paramount. The strategy of DDN for the edge is to develop security zones with different defensive elements in each zone. In the article “The Edge Computing endpoints and Defense-in-Depth Network security issues and recent developments,” the author K. Yang proposes the DDN architecture in **Figure 5**<sup>11</sup>.

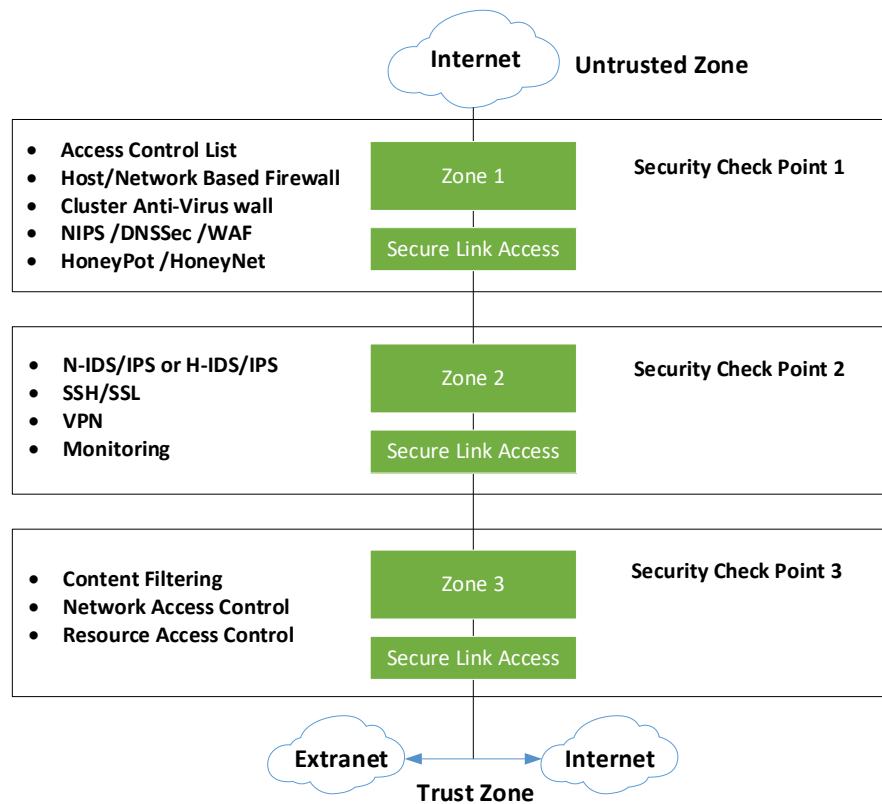
DDN takes a layered approach in securing networks and system environments. **Figure 5** demonstrates a layered approach by implementing zones and security links between the untrusted zone and trusted zone. We must also integrate securing and supporting critical infrastructure with the edge by implementing the same strategy. Server racks with network-connected programmable power distribution units (PDUs), data center cooling systems, power metering, and other industrial automation control systems are critical in supporting and enabling edge computing.

<sup>8</sup> [https://en.wikipedia.org/wiki/Air\\_gap\\_\(networking\)](https://en.wikipedia.org/wiki/Air_gap_(networking)) (As seen 1/8/2021)

<sup>9</sup> <https://continuumgrc.com/ics-security/> (As seen 11/12/2020)

<sup>10</sup> See White Paper 287, [Industry 4.0: Minimizing Downtime Risk with Resilient Edge Computing](#)

<sup>11</sup> <https://secuxtech.medium.com/the-edge-computing-endpoints-and-defense-in-depth-network-security-issues-and-recent-developments-8b6296254a3b> (As seen 11/11/2020)



**Figure 5**  
DDN to secure the edge –  
with recommended practice  
of creating zones

## Network segmentation

As the edge perimeter expands, we must secure access to those compute resources residing within. Network segmentation involves breaking a computer network into smaller pieces with the intent to control data traffic into and out of each segment. Proper network segmentation is accomplished through well tested Access Control Lists (ACLs), the strategic deployment of Next Generation Firewalls NGFWs), VLANs, etc. which provides the ability to filter traffic at the application layer<sup>12</sup> to enhance security on the edge. Data diodes and unidirectional gateways<sup>13</sup>, with the proper implementation, can offer a superior level of security in protecting network segments and safety systems.<sup>14</sup> The concept is very simple, but the implementation of a data diode can present a challenge and must be thoughtfully deployed, since the device will only allow traffic to flow in one direction only. Effective network segmentation can improve cybersecurity by limiting how far an attack can spread.

## Intrusion detection system

Edge computing is a distributed environment, and it is essential that a proper site assessment be done for the creation of a proactive threat detection program. Based on the determined critical access points in the network, appliances known as intrusion detection systems (IDS) should be placed at these locations to identify potential malevolent traffic that could potentially damage, disrupt service, and impact availability to the edge environment.<sup>15</sup> Depending on the skill set of the personnel staffing intrusion detection systems, customized signatures can be developed to “hunt” and

<sup>12</sup> <https://www.forcepoint.com/cyber-edu/osi-model> (As seen 11/11/2020)

<sup>13</sup> “A data diode (also referred to as a unidirectional gateway, deterministic one-way boundary device or unidirectional network) is a network appliance or device allowing data to travel only in one direction.” From [https://csrc.nist.gov/glossary/term/Data\\_Diode](https://csrc.nist.gov/glossary/term/Data_Diode) (As seen 1/8/2021)

<sup>14</sup> <https://www.se.com/us/en/download/document/Securing-Operational-Tech/> (As seen 12/1/2020)

<sup>15</sup> [https://www.se.com/us/en/download/document/998-2095-09-15-15AR0\\_EN/](https://www.se.com/us/en/download/document/998-2095-09-15-15AR0_EN/) (As seen 1/12/2020)



monitor for nefarious traffic based on the created signatures to search for anomalies and unsanctioned traffic that could potentially harm systems running on the edge.

## Secure Access Service Edge (SASE)

Another emerging cybersecurity concept for the Edge is [Secure Access Service Edge \(SASE\)](#), pronounced, “sassy”. SASE is a network security architecture concept that weaves SD-WAN deployments with embedded security. Designed with distributed IT and edge computing architectures in mind, this cloud-based service will simplify WAN deployments by providing better efficiencies for security, as well as better bandwidth management per application. SASE provides better scalability to applications depending on usage and bills accordingly.<sup>16</sup>

## Device setup / configuration

Before an embedded device or software-based system is used in an edge application, proper analysis should be done to understand how the device / system communicates and how the device / system functions within the use case that is required by the customer to operate at the edge. The following practices will help with this:

- Perform port scans and vulnerability assessments<sup>17</sup> on all devices to see the status of the device / system when delivered to the site.
- Use a vendor’s hardening guide to set up and configure a device. However, a careful analysis of the hardening guide should be performed to determine if it meets the site’s edge security deployment strategy.
- Verify that the device can be configured to disable any unsecure or unnecessary protocols and communicate over secured protocols (implementing TLS<sup>18</sup> for example). Any services that can be disabled without impacting needed operations of the device or system should be disabled to reduce the attack surface.
- Update all patches and updates on the device / system and thoroughly test before its final deployment.

## Operation and maintenance

To assist in developing processes and security as technology evolves, global standards provide guidance in best operational practices. [NIST \(National Institute of Standards and Technology\)](#) is known for defining and presenting best practices in IT, IIoT, and the cloud.<sup>19</sup> The scope presented in IEC 62443-2-4 specifies security capability requirements for integration, operational, and maintenance for deployed devices, systems, and network components.<sup>20 21</sup> While there may be specific best practices for particular applications, patch management, vulnerability management, and penetration testing are good practice categories that apply to operating and maintaining all edge applications.

- Patch management
- Vulnerability management
- Penetration testing

<sup>16</sup> <https://www.networkworld.com/article/3574014/what-is-sase-a-cloud-service-that-marries-sd-wan-with-security.html> (As seen on 11/11/2020)

<sup>17</sup> Assessments are performed using software scanning tools that are connected to the network.

<sup>18</sup> TLS - Transport Layer Security : [https://en.wikipedia.org/wiki/Transport\\_Layer\\_Security](https://en.wikipedia.org/wiki/Transport_Layer_Security)

<sup>19</sup> <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-325.pdf> (As seen 11/4/2020)

<sup>20</sup> IEC 62443-2-4, Edition 1.1, 2017-08, page 6

<sup>21</sup> [https://www.isasecure.org/en-US/Documents/Articles-and-Technical-Papers/2018-IEC-62443-and-ISA-Secure-Overview\\_Suppliers-Pe](https://www.isasecure.org/en-US/Documents/Articles-and-Technical-Papers/2018-IEC-62443-and-ISA-Secure-Overview_Suppliers-Pe) (As seen 11/04/2020)



## Patch management

Due to the criticality of embedded IIoT devices and SCADA systems running on the edge, careful co-ordination and planning must be made with operations personnel. In operations there are always concerns regarding maintaining systems and devices availability, and there is a justified fear that an improperly managed patch management scheme can cause instability and unavailability to such systems. Before engaging in any patching deployment, carefully coordinate with the operators, especially in industrial environments, so they can have a precise understanding of what is going to be patched, as well as the required mitigation and timing for applying the patch. It is critical that relationships between IT management staff and the operators be built upon mutual understanding and trust.

Unlike IT environments, industrial environments, also known as (OT) operational technology environments, operate under a different paradigm. The IT paradigm prioritizes confidentiality, integrity and availability. In OT the primary paradigm is reliability and safety, with availability and integrity wrapped inside, so to speak. Confidentiality comes last, unlike in the IT paradigm. OT operators monitor and control many of the critical infrastructure we take for granted today. Some examples of critical infrastructure are transportation, clean water, and electricity, all relying on these devices and systems. OT operations is extremely sensitive when it comes to patch management.

If a patch is not properly researched and validated in an OT environment, an unvalidated patch could impact a sensitive device or system. These devices could be controlling and monitoring critical functions. If an improperly validated patch is applied, instability could impact critical OT functions to where operators could lose connectivity to these devices, or worse, information coming into the control room may not be trustworthy.

## Vulnerability management

Vulnerability attacks against end points on edge computing can introduce a level of operational complexity due to the increased size of the landscape and new attack surfaces. Vulnerability management at the edge, for both known and unknown vulnerabilities, requires a proper program. This management program needs to identify scan coverage gaps and prioritize them. This will require proper asset management to identify the assets residing on the edge network. Great care must be taken when scanning IIoT devices and processes operating on the edge. As with patch management, all vulnerability scans must be carefully coordinated with the OT operators.

As with patch management, vulnerability scans can also cause instability in embedded devices residing in the edge. Passive scanning detects vulnerabilities by gathering information from network data by capturing it from a target device. Packet sniffing is one way of passively scanning information from operating systems, revealing protocols running on standard and non-standard ports. Passive scanning is a methodology that can be used to minimize impact on systems and devices running on the edge. Embedded IIoT devices operate with limited resources and an improper scanning strategy can gravely impact critical processes, resulting in potential damage and unwanted downtime.

## Penetration testing

Penetration testing, also called pen testing, simulates an attack upon either a device, system, or a network environment. Typically, pen testing involves the attempt to create a breach to uncover vulnerabilities, such as un-sanitized inputs that can be susceptible to code injections and can reveal misconfigurations, to name a few

examples. As with patch management and vulnerability management, great care must be undertaken as to not impair the availability of critical devices and system. There are 5 stages to pen testing and they are as follows:

- **Planning and exploration:** scope and goals of the pen test are defined. This can include devices, systems, network and methodology to be used for the test. As part of the exploration, intelligence gathering of target systems are performed to get a better understanding on how the target functions and what its potential vulnerabilities are.
- **Scanning:** this is where static analysis is performed to understand how the target will respond to intrusion attempts. An inspection of the device or application's code is performed to determine behavior while operating. Dynamic analysis inspects the code of a device or application in a running state, while providing a view of the target's performance.
- **Acquiring access:** the pen tester launches attacks on a webserver or web application using cross-site scripting and SQL injections, while trying to find backdoors to leverage a vulnerability found on the target. From here the pen tester will attempt escalating privileges, stealing data, and man-in-the-middle attacks to gain further understanding as to what damage can be done.
- **Sustaining access:** here the pen tester works to see if the vulnerability can be used to maintain a persistent presence in the device or system. This is to emulate what a bad actor would do to gain deeper access into the system.
- **Report:** a report showing an analysis of the penetration test exercise would be presented showing what vulnerabilities were used to exploit and what data of a sensitive nature were accessed, as well as how long the pen tester was inside a system before being detected.

Before engaging in a penetration test, validate the reputation of the company providing the service. If the OT environment is going to be pen tested, validate that the personnel who will be engaged clearly understand the criticality of the systems supporting the operations while working closely with OT operators.

## Conclusion

Edge computing provides high-speed delivery of data for edge applications, essential for today's business. It reduces network latency by providing the processing and delivery of needed information locally. As a distributed model, computing, aggregation, and analysis occur at the physical site instead of being centralized to a server or onto the cloud. This infrastructure includes IIoT devices, switches, routers, servers, virtual systems, other networking devices, integrated access devices, and multiplexers.

An edge environment can have a plethora of endpoints providing a large and complex attack surface to secure and monitor. The implementation of a defense-in-depth strategy and proper network segmentation is a critical strategy to implement in securing these critical business functions. Hardening of devices and systems provide a heightened level of security coupled with well-managed and consistent patch and vulnerability programs. Edge security must maintain integrity, availability, and confidentiality to support and strengthen business needs and objectives. People, process, and procedures will always be integral in securing network environments, including the edge.










### About the author

**Daniel Paillet** is currently Cybersecurity Lead Architect with the Schneider Electric, Energy Management Business Unit. His background includes working in the US Department of Defense on various security projects. His security experience includes working in Information Technology, Operational Technology, Retail, Banking and Point-of-Sale. He holds the CISSP, CCSK, CEH and other agnostic and vendor specific certifications. His current role is to architect, improve and develop secure solutions and offerings within Schneider Electric.

RATE THIS PAPER





-  [Physical Security in Mission Critical Facilities](#)  
White Paper 82
-  [The Drivers and Benefits of Edge Computing](#)  
White Paper 226
-  [Addressing Cyber Security Concerns of Data Center Remote Monitoring Platforms](#)  
White Paper 239
-  [Why Cloud Computing is Requiring us to Rethink Resiliency at the Edge](#)  
White Paper 256
-  [Three Types of Edge Computing Environments and their Impact on Physical Infrastructure Selection](#)  
White Paper 278
-  [Industry 4.0: Minimizing Downtime Risk with Resilient Edge Computing](#)  
White Paper 287
  
-  [Browse all white papers](#)  
[whitepapers.apc.com](http://whitepapers.apc.com)
  
-  [Traditional vs. OCP Power Architecture Capex Comparison](#)  
TradeOff Tool 18
  
-  [Browse all TradeOff Tools™](#)  
[tools.apc.com](http://tools.apc.com)

**Note:** Internet links can become obsolete over time. The referenced links were available at the time this paper was written but may no longer be available now.

## Contact us

For feedback and comments about the content of this white paper:

Data Center Science Center  
[dcsc@schneider-electric.com](mailto:dcsc@schneider-electric.com)

If you are a customer and have questions specific to your data center project:

Contact your Schneider Electric representative at  
[www.apc.com/support/contact/index.cfm](http://www.apc.com/support/contact/index.cfm)