# FIN | Framework 5

Security and reliability by design

CYBERSECURITY WHITEPAPER

J2INNOVATIONS
A Siemens Company

www.j2inn.com

# Introduction

Digitalization and IoT provides numerous advantages for building owners and operators and their product and service providers. Modern digital platforms and products show greater usability and flexibility, higher asset and energy efficiency, and reach new levels of user comfort. Furthermore, modern digital platforms are open and extensible to fit evolving market requirements, but Digitalization also presents security challenges.

Cyber-attacks are a constant and increasing threat due to the ubiquitous connectivity that makes digitalization possible. In today's connected world, the likelihood of a cyber-attack is high. How do you confidently address such cyber threats? By taking a holistic approach to security measures across all aspects of your organization, building assets and automation systems. This includes making sure the building automation systems that manage your facility's infrastructure are secure.

At J2 Innovations, we have taken the next step in providing best in class cyber security with the release of the latest FIN Framework, FIN 5. We've adopted a "think security" philosophy in the development and advancement of our FIN Framework product. This paper provides insight into how J2 Innovations has approached cybersecurity with the release of FIN 5, and continues to do so along the entire lifecycle.

Before diving in, let's first discuss what cybersecurity means. We define cybersecurity as the protection of life and company assets from harm caused by digital attacks against the availability, confidentiality, integrity, authenticity, and reliability of information in cyberspace. Cyberspace is the complex system of interaction between people, software, and services that is facilitated by using technical means to connect them to the Intranet and Internet.

Let's also define what it means to take a holistic approach to security. There are four key factors that impact security strength: people, communication, processes, and technology.

In general:

- **People** need a broad and lasting awareness of the importance of security; both physical security and cybersecurity
- **Communication** helps establish a culture of security when it is clear and concise
- **Processes** are as important as technology in protecting organizations from cyber threats
- **Technology** needs to be tested, vetted, and matched with other suitable building blocks in order to secure an organization's assets

The spectrum of security challenges is broad. While physical threats are more obvious and change less often, cyber challenges can be more nefarious due to an ever-changing threat landscape. When it comes to aligning security with business needs and the inevitable move toward convenience, we put a focus on cybersecurity from the outset.

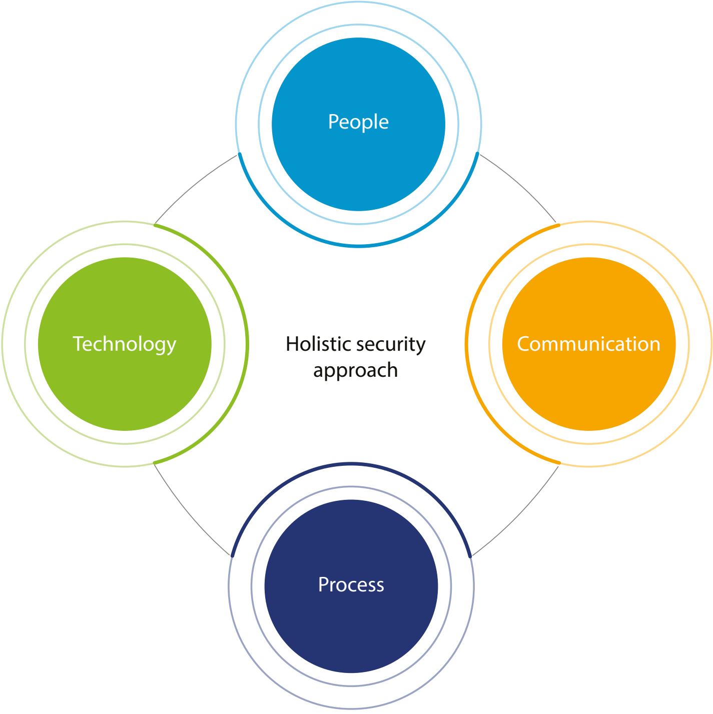

Fig. 1 –Key Factors

# Security by Design:
# J2 Innovations' commitment to Comprehensive Security

Cyber-attacks are among the fastest growing criminal activities today. They range from insider threats, ransomware attacks, opportunist threats, and hacktivism, all the way up to business espionage, terrorism, and state-sponsored cyber terrorism. Keeping organizations like yours safe and operating as usual takes a holistic approach to security.

J2 Innovations is committed to evolving the FIN Framework so users can respond to a fast, complex, and constantly changing threat landscape. Our commitment is multifaceted. Our end-to-end approach to product development builds in security from the beginning. We call it Security by Design. It includes an ongoing cycle of testing, enhancements, and evolution to keep our products and solutions at the forefront. In addition, we are part of the Siemens group, and jointly participate at the Charter of Trust, a global effort to develop and implement rules for ensuring cybersecurity throughout the networked environment. Simply put, we design with security in mind. We also contribute to and follow leading international standards such as ISO/IEC 62443 and OWASP as cybersecurity guidelines.

## Security by Design Expertise

The effectiveness of a product's cybersecurity design is attributed to the expertise of the development team. As part of our Security by Design methodology, we invest not only in technology developments for digital protection and product security, but also in the training required to maintain high levels of employee cybersecurity expertise.

Throughout the lifecycle of the product, our experts perform security threat and risk assessments (called TRAs) to address expected risk in the intended application of use. This assessment starts at the beginning of the process and is repeated as required to identify and mitigate risks appropriately.

In addition, regular product security testing is conducted by Siemens AG and external experts who use both manual penetration tests and automated machine security testing. The idea is to break the system in order to secure it. This testing ensures that the FIN Framework meets our security requirements. The test results are recorded and used to identify any necessary corrective actions.

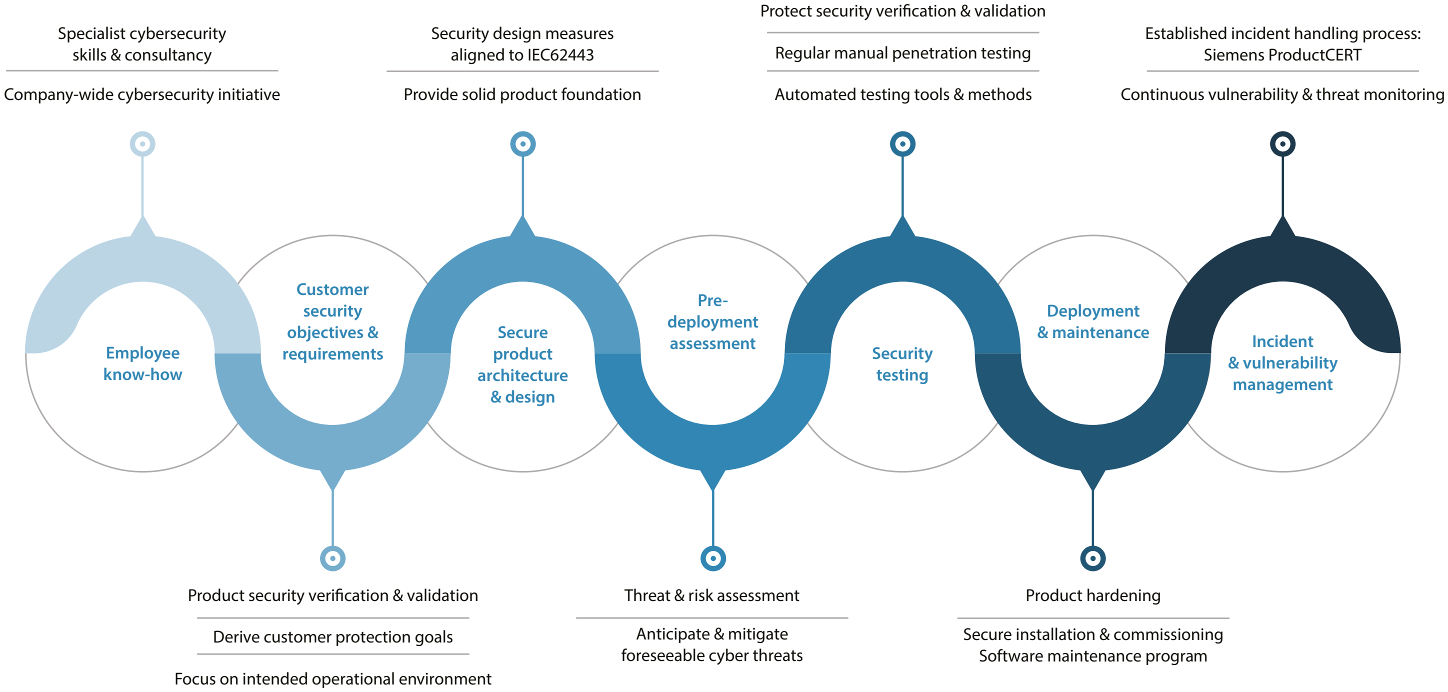
Specialist cybersecurity skills & consultancy
Company-wide cybersecurity initiative
Security design measures aligned to IEC62443
Provide solid product foundation
Protect security verification & validation
Regular manual penetration testing
Automated testing tools & methods
Established incident handling process: Siemens ProductCERT
Continuous vulnerability & threat monitoring
Employee know-how
Customer security objectives & requirements
Secure product architecture & design
Pre-deployment assessment
Security testing
Deployment & maintenance
Incident & vulnerability management
Product security verification & validation
Derive customer protection goals
Focus on intended operational environment
Threat & risk assessment
Anticipate & mitigate foreseeable cyber threats
Product hardening
Secure installation & commissioning
Software maintenance program

Fig. 2 – FIN Framework Product Cybersecurity Landscape

## Applying Security by Design to FIN Framework

FIN Framework is an open and robust platform for building automation and IoT that is at the center of creating efficient, sustainable and comfortable environments. It is also highly extensible so that OEM partners can customize the product to meet their specific market and customer requirements. As a software platform that functions as the heart and brain of a building, security by design is an essential pillar.

Our FIN Framework design experts adhere to the Siemens company-wide cybersecurity initiative as illustrated in Figure 2. They follow the mandatory internal security policy that provides measures for ongoing development of FIN Framework products in accordance with the appropriate security level. FIN Framework products are aligned with ISO/IEC62443.

These measures help ensure that coding leads to secure product architecture, as well as secure implementation of software components. The software is designed to be secure by default when installed, which means certain features and functions are secure out of the box. As new security threats continue to unfold, we continuously enhance and evolve the FIN Framework. We've integrated the following elements to make the FIN Framework secure by design:

- End-to-end encryption, from client to server
- End-to-end encryption between servers
- Encrypted communication to other devices
- Asymmetric Key Certificate-Based Encryption
- LDAP Authentication
- Using the least privilege principle to limit data and application access
- Support of hardware and software firewalls
- SCRAM-SHA-256 authentication
- Sensitive Information is stored in an encrypted database
- Role based authorization
- Action based auditing
- Configurable password complexity enforcement
- Use of verified third-party components

## FIN Framework Maintenance Program for highest level Cyber Security

As part of our Software Maintenance Program, we periodically release patches, updates, and platform upgrades that remove new known vulnerabilities and protect FIN Framework against threats. Patches and updates are made available as they are developed, supported by access to a technical hotline run by product experts. By participating in the FIN Framework Maintenance program (which is free of charge in the 1st year after license purchase), you not only gain access to latest innovation and new functionality, but also to latest improvements in product robustness and cyber security.

## FIN Framework Cybersecurity Deployment

We publish cybersecurity hardening guidelines to support the secure commissioning and deployment of FIN Framework products. These guidelines describe how the system needs to be configured in-order to ensure secure operation of the FIN Framework product in the intended operating environment. Configuration guidance includes: applications to install, which settings to activate or deactivate, firewall configurations, and the setting of user and system accounts and access rights. The hardening guidelines are maintained throughout the product lifecycle.

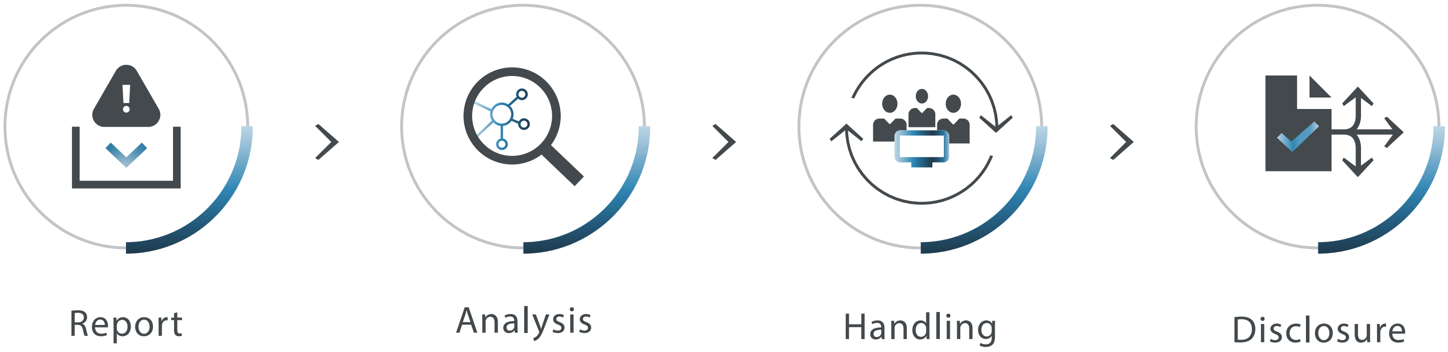

Fig. 3 – FIN Framework Incident and Vulnerability Handling Process

## Emergency Management

If a security issue or vulnerability is detected in a FIN Framework product or solution, we have incident and vulnerability handling processes in place.

Incident and Vulnerability Handling Process: Our support mechanism for customer-reported security issues is illustrated in Figure 3. Vulnerabilities and/or incidents are submitted to our technical support team, which is supported by the global Siemens ProductCERT team that operates on a 24/7 basis. The necessary steps are taken to handle the situation and the incidents and remedies are disclosed.

Vulnerability Management: This is our internal detection process for fine-tuning the security of our products and solutions. Continuous threat monitoring allows us to detect and fix potential vulnerabilities in our products. FIN Framework software components are registered so that if any security vulnerabilities are found, the necessary remedies can be implemented and disclosed. Identified vulnerabilities are announced by the ProductCERT team via the ProductCERT security advisories.

## Conclusion

As the leading open platform for building automation and IoT, we understand the challenges you face in meeting your cybersecurity needs in today’s world. Our comprehensive security approach to the product lifecycle means our FIN Framework is designed with your security in mind. This ensures that FIN Framework can be part of your holistic approach to security that takes people, processes, technology, and communication into account.

Ultimately, smart organizations make security one of the cornerstones of their businesses today. FIN Framework is a flexible and interoperable portfolio that can be scaled to meet the needs of your organization. FIN Framework is Security by Design.

**Cybersecurity Disclaimer**

J2 Innovations provides a platform for building automation and IoT that includes security functions that support the secure operation of plants, systems, machines and networks in the environment of building automation and IoT.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain  a holistic, state-of-the-art security concept. J2 Innovations' portfolio only forms one element of such a concept.

You are responsible for preventing unauthorized access to your plants, systems, machines and networks which should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. Additionally, J2 Innovations' guidance on appropriate security measures should be taken into account. For additional information, please contact your J2 Innovations sales representative.

J2 Innovations portfolio undergoes continuous development to make it more secure. J2 Innovations strongly recommends that updates are applied as soon as they are available and that the latest versions are used. Use of versions that are no longer supported, and failure to apply the latest updates may increase your exposure to cyber threats. J2 Innovations strongly recommends to comply with security advisories on the latest security threats, patches and other related measures, published, among others, under **www.siemens.com/cert/en/cert-security-advisories.htm**

J2 INNOVATIONS
A Siemens Company

1550 Valley Vista Drive, Suite 200
Diamond Bar, CA 91765
tel: 909.217.7040
email: support@j2inn.com