SIEMENS
Ingenuity for life

Desigo CC 3.0 Product Family

Cybersecurity Meets Building Management Systems

Introduction

We live and work in an exciting era. It's one defined by Industry 4.0 – the digitalization of business. Digitalization provides numerous advantages, including greater convenience and increased efficiency. It also presents security challenges. Cyber attacks are a constant and increasing threat due to the across-the-board connectivity that makes digitalization possible. In today's connected world, the likelihood of a cyber attack is high.

How do you confidently face and mitigate cyber threats? You take a holistic approach to security measures across all aspects of your organization. This includes making sure the building management systems that manage your facility's infrastructure are well prepared.

At Siemens Building Technologies, we believe security begins during product development. We've adopted a "think security" philosophy in the development of our products, including the Desigo CC 3.0 family of building management products, solutions, and services. This paper provides insight into how Siemens approaches cybersecurity requirements during the Desigo CC 3.0 product development and lifecycle management processes.

Before discussing cybersecurity, let's define it. For this document, 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. Leading companies and institutions take into account 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 that actively applied 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

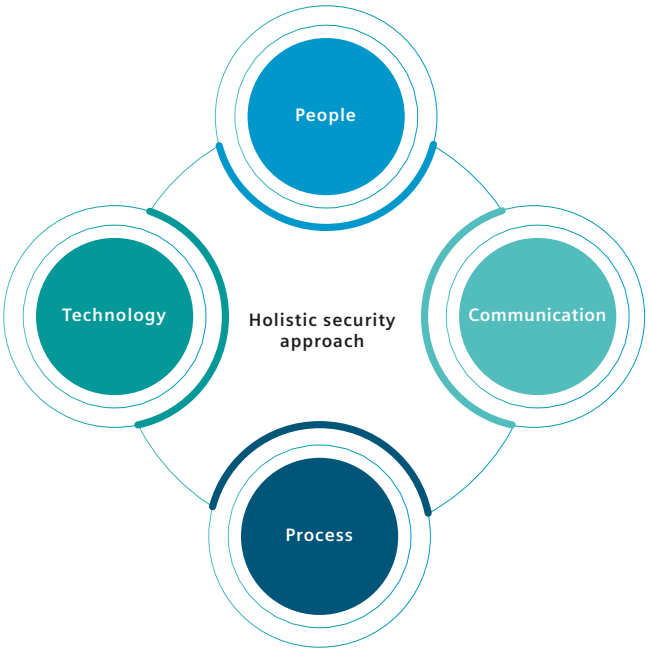


Figure 1 – Holistic Security Approach: Key Factors

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.

"Security by Design:" Siemens Commitment to Comprehensive Security

Cyber attacks are among the fastest growing criminal activities in the world 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. In order to be prepared to respond to a fast, complex, and constantly changing threat landscape, it is essential that organizations like yours take a holistic approach to security.

While the responsibility to secure your environment lies with your organization, Siemens is committed to developing products that enable you to take a holistic approach to security. This is true for our Desigo CC 3.0 family of building management products, solutions, and services, the focus of this paper. The Desigo CC 3.0 product family includes Desigo CC 3.0, Cerberus DMS 3.0, and Desigo CC Compact 3.0.

Our commitment is multifaceted. First and foremost is "Security by Design," our end-to-end approach to product development that builds in security from the beginning. It includes an ongoing cycle of testing, enhancements, and evolution to keep our products and solutions at the forefront. In addition, we are a founding member of the global Charter of Trust, which calls for binding rules and standards to build trust in cybersecurity and further advance digitalization.

Simply put, we design with security in mind. Our company-wide initiative provides a risk management program that actively drives comprehensive security methodology for all Siemens products, solutions, and services. It identifies best practices and sets technical standards, processes, and policies that must be met. We also contribute to international standards and strive to deliver products that meet security standards such as ISA/IEC 62443, UL2900, ISO/IEC 27001, and OWASP.

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 in order to address expected risk in the intended application of use. This assessment starts early on in the process and is repeated as required to identify and mitigate risks appropriately.

In addition, regular product security testing is conducted by external experts who use manual penetration tests alone or in combination with automated machine security testing. The idea is to break the system in order to make it more secure. This testing ensures that the selected product, solution, or service meets our security requirements. The test results are recorded and used to identify any necessary corrective actions.

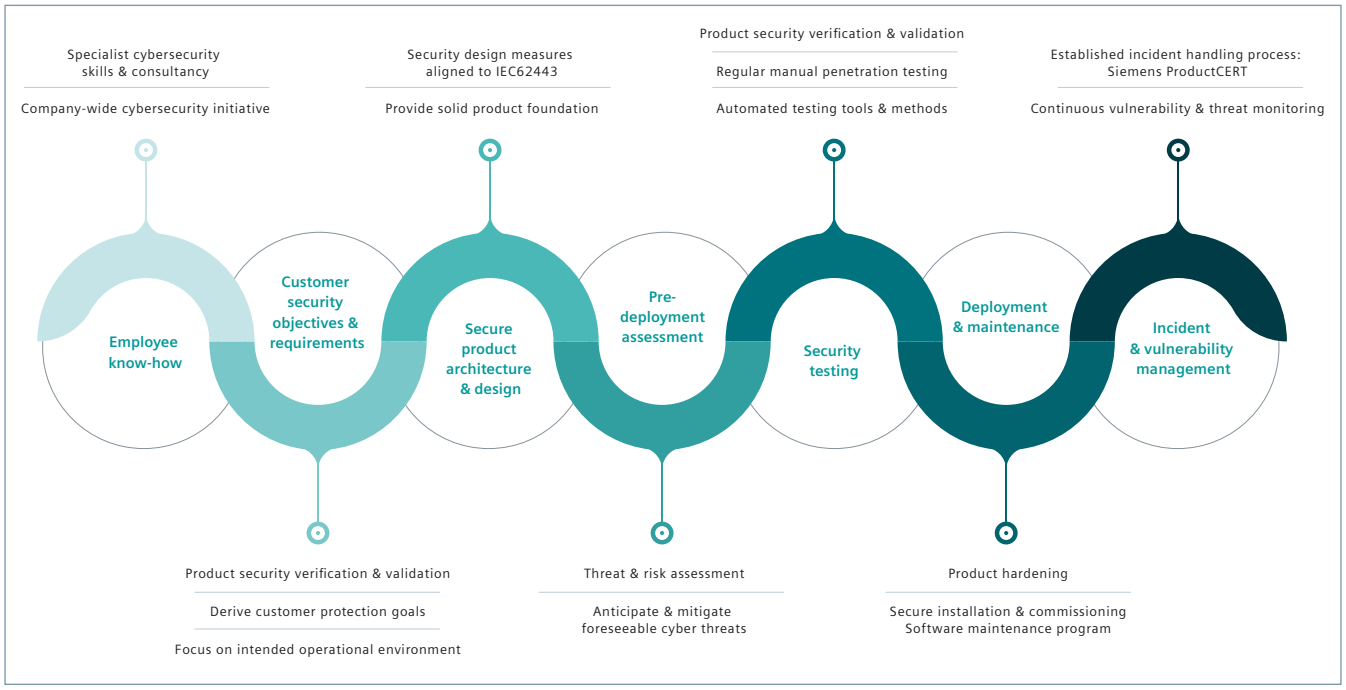


Figure 2 – Siemens Cybersecurity Initiative Highlights

Applying Security by Design to Desigo CC

Desigo CC is a robust, open integrated building management platform that helps create comfortable, safe and sustainable facilities. It enables operation and monitoring of a building.

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

These measures help ensure that coding leads to secure product architecture as well as more secure implementation of software components. The software is designed to be secure by default when installed. This includes that certain features and functions are secure at the default level.

And because we continuously enhance and evolve our products, solutions, and services, Desigo CC will be kept up to date as new security threats unfold. Below is an example of "Security by Design" elements integrated into Desigo CC:

- End-to-end encryption, from client to server
- End-to-end encryption between servers
- Encrypted communication to other devices
- Certificate-based data exchange
- Seamless integration of certificates within customer IT infrastructure
- Microsoft's active directory-based authentication
- Using "least privilege" principle to limit data and application access
- User/workstation groups/roles control access to the system – designating appropriate tasks and responsibilities
- Re-authentication
- Cybersecurity audit trail
- Support of antivirus and malware protection software
- Support of hardware and software firewalls
- Use of network infrastructure that supports physical network or VLAN segmentation
- Segregation of networks into zones
- Controlled access to servers, clients, and applications
- Placing the web server in a "demilitarized zone" (DMZ)

Figure 3 – Desigo CC Incident and Vulnerability Handling Process

Desigo CC Cybersecurity Deployment

We publish cybersecurity hardening guidelines to support the secure commissioning and deployment of Desigo CC products. These guidelines describe how the system needs to be configured in order to foster secure operation of the Desigo CC products and solutions in the intended operating environment. Configuration options consist of, for example, which 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.

As part of our Software Maintenance Program, we periodically release patches, updates, and upgrades that remove new known vulnerabilities and increase the level of protection of Desigo CC against threats. Patches and updates are made available as they are developed, supported by access to technical hotline support run by product experts. There is also the option to subscribe to software updates to ensure that your deployed Desigo CC is always updated to the latest version release.

Emergency Management

For our offerings, we have incident and vulnerability handling processes in place in the event that a security issue or vulnerability is detected in a Desigo CC product or solution.

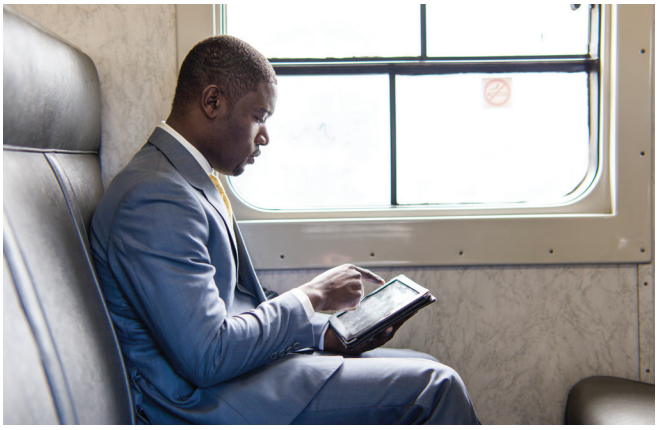
Incident and Vulnerability Handling Process: Our support mechanism for customer-reported security issues is illustrated in Figure 3. Vulnerabilities and/or incidents are submitted to our technical support team, which is supported by the global Siemens ProductCERT team that operates on a 24/7 basis. The 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 enables us to detect and mitigate potential vulnerabilities in our products and solutions. Desigo CC 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 (https://new.siemens.com/global/en/products/services/cert.html), to which you can subscribe.

Remote Services

Remote access is a desirable feature today because of the ongoing performance monitoring and convenience it provides. Desigo CC is prepared to support services that rely on remote data access while remaining part of the environment's security concept. By supporting remote services, Desigo CC allows you to leverage access to data about your building systems and connected equipment so your operations can be optimized.

While remote access is possible through your standard IT mechanisms, we use the Siemens Common Remote Service Platform (cRSP) for more secure remote access. Our reliable, high-performance cRSP provides worldwide access to data and information related to your building infrastructure. This platform ensures that the remote services delivered by Siemens meet stringent cybersecurity requirements. The Siemens cRSP conforms to ISO/IEC 27001 – the norm for systematic cybersecurity management on an organizational level.



Conclusion

As a market leader in building technologies, 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 Desigo CC products, solutions, and services are designed with your security in mind. Therefore, Desigo CC 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. Desigo CC is a flexible and interoperable portfolio that can be scaled to meet the needs of your organization.

Contact

For questions about Desigo CC, please contact your local Siemens representative or find one at https://new.siemens.com/global/en/products/buildings/contact.html.

Published by
Siemens Switzerland Ltd.
Building Technologies Division
International Headquarters
Theilerstrasse 1a
6300 Zug
Switzerland
Tel. +41 41 724 24 24

Cybersecurity Disclaimer

Siemens provides a portfolio of products, solutions, systems, and services that includes security functions that support the secure operation of plants, systems, machines, and networks. In the field of building technologies, this includes building automation and control, fire safety, and security management as well as physical security systems.

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. Siemens 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, Siemens guidance on appropriate security measures should be taken into account. For additional information, please contact your Siemens sales representative or visit https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrialsecurity.html.

Siemens portfolio undergoes continuous development to make it more secure. Siemens 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. Siemens strongly recommends to comply with security advisories on the latest security threats, patches and other related measures, published, among others, under http://www.siemens.com/cert/en/cert-security-advisories.html.