Everguard
FIRE·SAFETY

SIEMENS

Secured Cloud Connectivity Enables Remote Access and Maintenance of Fire Protection Systems

Increase the efficiency of your service business.

everguardfiresafety.com

Executive Overview

Timing is everything when it comes to fire safety because people, assets and business continuity are at stake. Keeping fire protection systems up and running is a 24/7 undertaking that involves two important goals today. The first is to make the communication between fire protection systems and the interfaces that collect data quicker, more reliable and smart. The second is to give service providers and their customers a solution that helps fix issues as quickly and seamlessly as possible. Both goals can be accomplished more easily and cost-effectively with remote access and maintenance.

As defined in this paper, cybersecurity is:
"The protection of company assets against harm caused by digital attacks against the availability, confidentiality, integrity, authenticity and reliability of information in cyberspace. Cyberspace is the complex system of interactions among people, software and services by technical means connected to the Internet."

However, fewer than 10% of buildings today have the cloud connectivity needed to make remote access possible. This despite inroads that digitalization and the Internet of Things (IoT) have made in the fire industry in recent years, unlocking new value like real-time operations, optimization and prescriptive analytics. Then comes COVID-19, which might have an unexpected acceleration of remote access use to manage fire safety and other building technologies. Perhaps the pandemic's requirement for everyone to keep their distance will speed the acceptance of remote monitoring, maintenance and control of fire safety systems.

Even with the pandemic, though, the question of cybersecurity comes into play immediately. Is cloud connectivity secured, is the first question asked by many professional services companies, who provide fire safety system monitoring and maintenance for customers of all types and sizes in a broad spectrum of industries. The question is echoed by many of their customers as well.

The answer is a resounding yes – if cloud connectivity follows strict cybersecurity methods. This paper explores the impact of cybersecurity on remote monitoring, maintenance and control of fire safety systems. Cloud connectivity with security in mind stands to make a dramatic difference in how optimal uptime is maintained for these crucial systems.

"Being smart about cloud platforms and services can make the difference between gaining a competitive edge and falling behind rivals."

Capturing the remote connectivity market

The market for remote connectivity for fire safety systems is vast, since about 90% of buildings are not connected to the cloud. Additionally, most sites do not have an on-premise danger management station. This means that service partners and customers can't obtain an overview of happenings at their sites without running to a fire alarm control panel. Fire safety solution partners are left asking themselves:

- How do I gain a quick overview of my customers' fire protection systems?
- How can I reduce high traveling costs and increase customer service quality?
- How can I provide periodic maintenance more efficiently and deliver evidence of executed tests to customers?

Cerberus Cloud Apps from Siemens solve these problems by connecting fire safety solutions to the cloud, which helps digitalize the fire industry and create remote accessibility. Cerberus Cloud Apps use a gateway to connect each site to the cloud so that panel events can be sent to the cloud. Solution partners and customers are then able to directly monitor and operate the fire control panels without having to stand in front of them.

To combat the wide array of security threats that are introduced by this technological transformation, Siemens has developed a layered defense approach that detects, responds and remedies multiple levels of threat. This includes continuous product development and an ongoing process for identifying and mitigating the challenges that come with exposing building and fire data from the local network to the cloud.

"Being smart about the use of cloud platforms and services can make the difference between gaining a competitive edge and falling behind rivals," according to McKinsey and Company's Andrea Del Miglio, Partner, and Will Forrest, Senior Partner.[1]

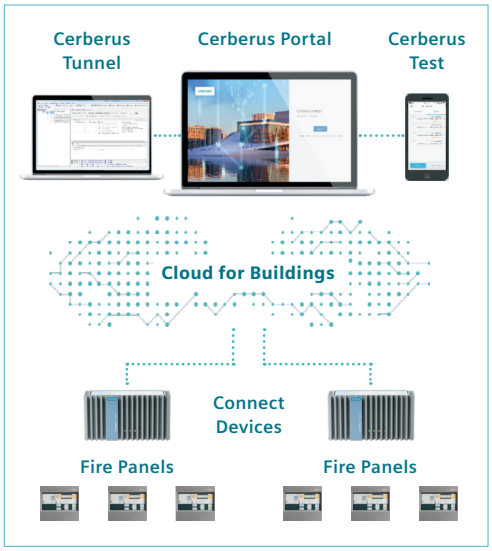


Figure 1 – Cerberus Cloud Apps Portfolio

[1] Del Miglio, Andrea and Will Forrest, "Creating value with the cloud," *Digital McKinsey Insights*, December 2018, p. 3.

Cerberus Cloud Apps portfolio

To help solutions partners and their customers get the most from cloud platforms and services, Siemens developed the Cerberus Cloud Apps portfolio that includes Cerberus Portal, Cerberus Test and Cerberus Tunnel. They are part of Siemens holistic approach to fire protection in which every element of fire protection matters – from detection and evacuation to danger management and cloud services.

Cerberus Portal

The Cerberus Portal application delivers an overview of all connected sites as well as easy access to them. It also eliminates unnecessary service visits and prepares service engineers for those that still need to take place. The system is simple to install and commission without the need for extended training. Furthermore, communications are encrypted and privacy is maintained in order to ensure the safety of the customer's data. Customers control access to their data; even Siemens needs the customer's explicit permission to have data access for other than routine maintenance or troubleshooting.

Cerberus Portal makes services more efficient for both solution partners and customers.

Cerberus Portal makes services more efficient for both solution partners and customers by providing secured 24/7 connectivity, multi-site dashboards, real-time monitoring and simple operation. The 24/7 connectivity allows access to customer sites from anywhere and at any time.[2] So there's no need to be on site unless local regulations require it; permitted users just open their browsers, go to the Cerberus Portal website and login to find everything they need.

Cerberus Portal

The built-in, multi-site dashboard shows a simple overview of connected sites in real time, in one place and at a glance. Color indications on the status bar show which sites are running smoothly and which may be having problems. By monitoring everything in real time, solution partners will often know issues before their customers do. They can learn more about a specific site by just clicking on it to see a detailed overview. Service engineers can also check each site to discover any issues before starting their maintenance routes. That way they'll arrive on site with the right information, equipment and tools, saving time and travel expenses.

Cerberus Portal was designed to be easy to use on any smart device. The user interface is simple so that solution partners and customers can focus on what is important. The application is continuously improved and updated automatically.

[2] Depending on local and technical restrictions. Please check with your local Siemens account.

Cerberus Test

Cerberus Test

The Cerberus Test application enables service partners to deliver efficient testing during periodic maintenance. The application then provides reports of those tests to the customer. Cerberus Test reduces the service engineer's manual work and proves that the fire safety system is running as expected according to the service level agreement.

Cerberus Test is faster and more efficient than regular detector testing since only one person is needed.

Cerberus Test is a native smart-phone application that makes the process faster and more efficient than regular detector testing since only one person is needed. Hands-free text-to-speech functionality increases the speed and efficiency of the maintenance activities. The detector test activities are recorded in the cloud. Cerberus Test displays the tested detector identification in real time and then exports the tested detector list so it can be sent to the customer.

Cerberus Tunnel

The Cerberus Tunnel application solves the problem of sending service engineers to a site without knowing the precise problem or if it could have been fixed remotely. Fire service engineers can use Cerberus Tunnel to remotely access the fire safety sites and fix issues without needing to be on site.

Cerberus Tunnel allows the service engineer to remotely connect the Cerberus Remote software[3] and the Cerberus Engineering Tool. Cerberus Remote displays a virtual PMI version of the panel while the Cerberus Engineering Tool enables remote access of the fire configuration file. The service engineer can then remotely advise the customer and offer additional services and support without having to be on site.

Cerberus Tunnel

[3] Depending on local and technical restrictions. Please check with your local Siemens account.

Additional benefits of Cerberus Cloud Apps

Cerberus Cloud Apps introduce a number of additional benefits for three important groups: system integrators or service companies, owners or investors, and consultants, planners or designers.

Systems integrators or service companies are looking for new opportunities to increase their competitiveness. For example, remote configuration and commissioning of the systems will reduce travel costs and improve utilization of fire safety engineers, who are becoming an increasingly rare commodity.[4] In addition, these companies will benefit from the step-by-step installation and setup of the cloud solution.

Owners and investors find that Cerberus Cloud Apps put peace of mind at their fingertips.

By using Cerberus Cloud Apps to digitalize the service business, systems integrators and service companies can take the next step in further improving their resource utilization. They can monitor, operate[5] and service connected sites from remote locations with minimum hardware costs and without investing in additional in-house server capacity. These companies can also discover new digital business opportunities that extend their offerings, develop new business models and unlock wealth. In addition, they can increase satisfaction for customers and employees alike by offering real-time monitoring, proactive services, notifications and remote operational support.

Owners and investors find that Cerberus Cloud Apps put peace of mind at their fingertips. For example, live overviews let them know what is happening with their fire protection systems at any time and anywhere.[5] The system is set up to initiate quick response to fire events. The owners and investors can determine the category of events that trigger notifications and who will receive them.

If a fire event occurs, a live status update of the fire control panel in question is sent via SMS or email to the appropriate people. Detailed information about the event makes troubleshooting more time efficient. For example, the owner's service provider receives a detailed report that provides the information needed so that a service engineer can either fix it remotely or arrive well prepared to handle it on site.

The owner also appreciates that Cerberus Cloud Apps help maintain business continuity by increasing the uptime of the fire safety systems. The apps make maintenance work more efficient and incident troubleshooting faster. State-of-the-art fire safety solutions also contribute to making the building run smoothly.

The consultants, planners and designers are looking for innovative solutions with future-ready fire protection systems that ensure adherence to standards and regulations.

"Without security, the truly transformative benefits of connectivity and automation are at risk. Embracing cybersecurity means protecting your customers and your bottom line," according to Sedar Labarre, Vice President, Booz Allen Hamilton.[6]

[4] Remote control requires local jurisdiction approval if not permitted under current codes of practice.
[5] Depending on local and technical restrictions. Please check with your local Siemens account.
[6] Labarre, Sedar, "Cybersmart Buildings: Securing Your Investments in Connectivity and Automation," February 2017, Booz Allen Hamilton, p. 3.

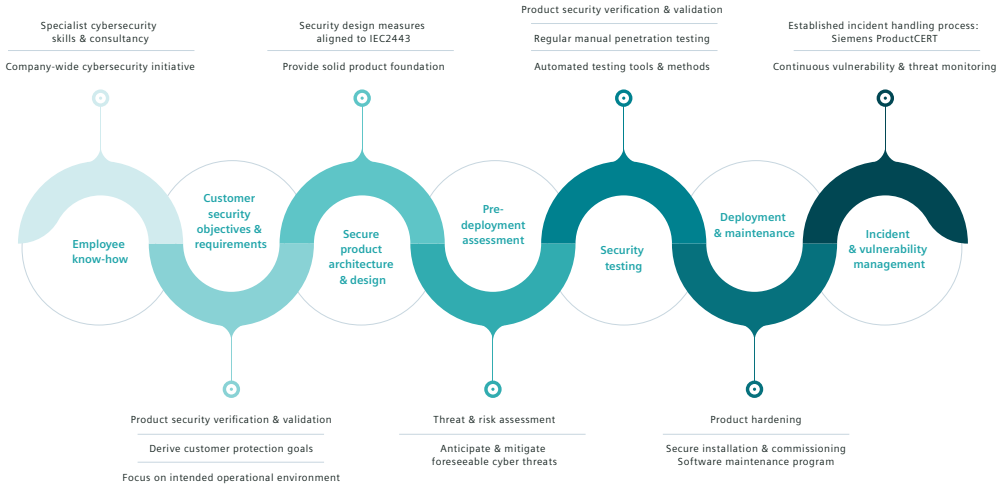


Figure 2 – Siemens Cybersecurity Initiative Highlights

"Security by Design": Siemens commitment to comprehensive security

Cybersecurity is crucial in a world where cyber attacks are among the fastest growing criminal activities. Our company-wide "Security by Design" initiative is our end-to-end approach to product development that builds in security from the beginning, as illustrated in Figure 2. Siemens is committed to developing products, solutions and services that enable you to take a holistic approach to security so that you can respond to a fast, complex and constantly changing threat landscape.

Throughout the lifecycle of the product, solution or service, our experts perform security threat and risk assessments.

Simply put, Siemens designs all products, solutions and services with security in mind. This is true for our Cerberus Cloud Apps, which use a layered defense approach to detect, respond and remedy multiple levels of threat. Siemens is also 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.

Security by Design expertise

The effectiveness of the cybersecurity design for a product, solution or service is attributed to the expertise of the development team. Therefore, Siemens invests 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, solution or service, 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 secured. 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.

Applying Security by Design to Cerberus Cloud Apps

Siemens has taken the Security by Design approach to all aspects of the Cerberus Cloud Apps portfolio. The following is a close look at the key features of our cybersecurity program for these cloud-based applications, beginning with the secured gateway.

Gateway applications are implemented in accordance with controls in the BP Security Framework, which is based on ISA/IEC 62443-3-3. These applications feature end-to-end encryption between devices and access points to cloud services. The apps have certificate-based communication security in place, including easy integration of certificates within the customer's IT infrastructure. Access to the system is based on appropriate user roles and their designated tasks and responsibilities. There are no workstation roles or groups.

The Cerberus Cloud Apps support antivirus and malware protection software on the customer devices. Since the gateway is a closed box, customers and service engineers can trigger updates of gateway firmware via the cloud but they cannot install their own software on the gateway. The apps also support hardware and software firewalls. While the software firewall is built in, customers can deploy additional hardware firewalls on the network. Off-premise, the Cerberus Cloud Apps use Amazon Web Services (AWS) and Microsoft Azure cloud infrastructure to host infrastructure and platform services and to perform access control functions.

The services, along with Siemens Connect Device, enable an end-to-end solution that unlocks new value for customers. AWS and Azure provide the cloud infrastructure hardware, software and networking needed to meet the requirements of security-sensitive organizations. AWS and Azure are also responsible for protecting the global infrastructure that runs all Cerberus Cloud Apps services offered through the cloud. Detailed descriptions of AWS and Azure security protocols can be found at: https://aws.amazon.com/security/ and https://docs.microsoft.com/en-us/azure/security/.

Access control to Cerberus Cloud Apps is a two-step process for both partners and customers. It begins with user authentication and identification conducted by Siemens ID, which is based on an Identity as a Service (IDaaS) platform. The main benefit of Siemens ID is that it provides a single sign-on to the Siemens applications. It includes ID administration and security token service, and features the option for multi-factor authentication for an added layer of security. More information about Siemens ID can be found at https://cdn.login.siemens.com/help/index.html.

The next step in access control is authorization, a security mechanism used to determine user privileges to devices, services, data and application features. It defines the specific part of the infrastructure resource that can be accessed and the set of actions the identified user can perform. Cerberus Cloud Apps implement role-based access control (RBAC), which limits a user to authorized applications and features. Access to sites and devices is limited by organizations and scopes.

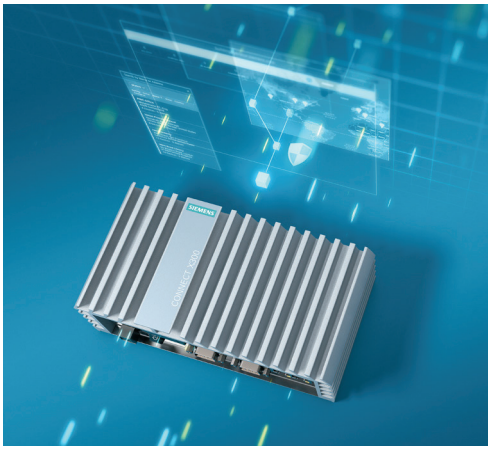
Data privacy is another important feature of the Cerberus Cloud Apps.

All personal data processed in context with the Cerberus Cloud Apps complies with European Union General Data Protection Regulation (EU GDPR), which gives individuals control over their personal data.

All data is secured by encryption both at rest and in transit. Data encryption-at-rest uses standard AWS encryption that conforms to the Federal Information Processing Standard (FIPS) 140-2 standards. All data in transit, such as in communication to and from Cerberus Cloud Apps, is encrypted using HTTPS/TLS1.2.

The Cerberus Tunnel application features remote access to the on-premise fire networks. It enables commissioning engineers to remotely service and access fire networks without requiring inbound connectivity.[7] Cerberus Tunnel has a by-default session timeout of 10 minutes.

The Connect Device is designed with a number of security hardening principles that limit unauthorized access and reduce security risks.



Connect X300 Connect Device

On-premise activities

The Connect X300 Connect Device is the edge connectivity device used to gather building data on premise and then provision it to the Cerberus Cloud Apps or other Siemens digital service. It is connected to the fire network via FCnet, C-Web or XNET.

The Connect Device is designed with a number of security hardening principles that limit unauthorized access and reduce security risks. It employs access control through authentication and authorization. The BIOS is password protected. And its USB and display ports are restricted to keyboard, 4G dongle or display only; support for memory drives or any similar devices on USB ports is disabled.

The Connect Device operating system is a Linux distribution protected by encryption keys with SSH connections disabled. Before the Connect Device can be used for normal operation, it is required to verify the authenticity of the gateway with a 32-digit unique activation key to register and authenticate with Cerberus Cloud Apps. During the initial setup – after the user logs into the Connect Device web for the first time – the user must change the default administrator password.

[7] Depending on local and technical restrictions. Please check with your local Siemens account.

Other considerations to mitigate cyber threats

Communication between the Connect Device and the Cerberus Cloud Apps is via the Internet. The connection is always outbound traffic that is initiated by the Connect Device on premise utilizing HTTPS. All data communication via the Internet is encrypted using Transport Layer Security (TLS) 1.2 and TCP port 443. No other port is used for outbound data communication to the Internet.

All data communication between the cloud servers' endpoints and the Connect Device is also secured by means of JWT token-based authentication and authorization or operational device certificates. All inbound ports on the Connect Device's LAN interface are disabled by default, except for ports 80 and 443. The ports for fire communication are opened automatically on demand.

The Connect Device supports anonymous proxy; however, a DNS server is required. It also leverages containerized architecture, where published software or firmware images are certified and renewed. This verifies the container image is built from an official image source and running as intended. All operating system updates are signed, and the signature is verified before applying the software or firmware update.

Cerberus Cloud Apps cybersecurity deployment

Cerberus Cloud Apps have cybersecurity policies that preserve three things about data: confidentiality, integrity and availability. Only people with the right to view the data have regular access to it. Those who access the data may rely on its accuracy. And the apps make it easy to access the data when and where needed.

However, it must be recognized that security is a shared responsibility. Security is not solely under the purview of the cloud infrastructure and cloud application providers. Neither is it solely under the purview of on-premise IT/OT network managers and users.

The cybersecurity hardening guidelines for Cerberus Cloud Apps are published and maintained throughout their product lifecycles. These guidelines describe how the system needs to be configured, commissioned and operated in order to ensure reliable operation of these services. They consist of, for example, which settings to activate or deactivate, firewall configurations, and the setting of user and system accounts and access rights.

As part of Siemens constant development process for Cerberus Cloud Apps, we periodically release patches, updates and upgrades that remove new known vulnerabilities and increase the level of protection against threats. Patches and updates for the cloud-based applications are made available directly with deployment. Firmware updates for the connected devices are also made available and can be pushed to the devices remotely. This practice ensures that the firmware is up-to-date and secured, both on and off site.

Emergency Management

Siemens has processes in place for handling security incidents. In an event where a cybersecurity threat is suspected or found, immediately contact Siemens Computer Emergency Response Team for products (Product CERT) or your local Siemens customer service.

Siemens ProductCERT is a dedicated team of seasoned security experts that manages the receipt, investigation, internal coordination and public reporting of security issues related to Siemens products, solutions or services. ProductCERT cultivates strong and credible relationships with partners and security researchers around the globe to advance Siemens product security, to enable and support development of industry best practices, and most importantly to help Siemens customers manage security risks.

The team acts as the central contact point for security researchers, industry groups, government organizations and vendors to report potential Siemens product security vulnerabilities. This team will coordinate and maintain communication with the involved parties, internal and external, in order to appropriately respond to identified security issues. Security Advisories are released in order to inform customers about necessary steps to securely operate Siemens products and solutions.

Siemens CERT is a dedicated team of Security Engineers with the mission to secure the Siemens infrastructure. CERT monitors the current cyber threat landscape for Siemens and assesses its potential impact on the enterprise. Based on that know-how and the latest technological trends, CERT consults with the Information Technology department at Siemens to improve the enterprise IT Security. The team is responsible for coordinating the response to cybersecurity incidents within Siemens. To achieve its mission, CERT leverages the relationships with various internal and external stakeholders worldwide, such as CSIRT networks, technical communities and the security researcher communities. CERT is also recognized as a trusted research partner by academia and industry, with numerous projects and publications in its expert area.

Everguard
FIRE·SAFETY

CONTACT US

1.877.514.1441

inquiries@
everguardfiresafety.com

everguardfiresafety.com

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://new.siemens.com/global/en/products/automation/topic-areas/industrial-security.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 https://new.siemens.com/global/en/products/services/cert.html.

RBQ licence : 5806-7075-01