SIEMENS energy

Safeguarding critical infrastructure

Omnivise T3000 Cybersecurity

siemens-energy.com/omnivise-t3000

Focus on energy security

The changing threat landscape

The entire power generation and distribution landscape is becoming more complex and fragmented, as the move to renewables and more distributed generation accelerates. This leads to environmental and sustainability benefits but means operators now face significant new cybersecurity risks. In this paper we show how customers can use new and more advanced Instrumentation & Controls (I&C) solutions to deal with these challenges.

The past 20 years have seen a rapidly accelerating increase in cyber threats specifically targeted on Critical National Infrastructure (CNI), largely driven by increased connectivity. We live in a connected world and expect to have rapid, simple interaction between business and consumer systems as a matter of course. As more enterprises move to the cloud, the level of connectivity grows, and cybersecurity concerns grow at the same rate. Every point of connection, every individual transaction brings a certain level of risk with it, and all of us now have to be conscious of how to stay safe – and keep others safe – online. The issues are even more dramatic when we consider the security of our infrastructure.

A more complex market

Every state classifies key installations and systems as CNI, which means damage to such systems will cause serious disruption, inconvenience and potentially much worse. Of these systems, perhaps the most important are power generation capabilities, because damage to these could bring all other systems to a halt, with potentially devastating impact.

None of us are immune to cyber-attacks, and the real story is not so much the major attacks, which are headline news, but the continuous need for safeguarding, day by day, against constant, low level threats. How big a problem is this? Citing the annual Cybercrime Report from Cybersecurity Ventures (the world's leading cybercrime researcher and publisher) Siemens Energy calculates that financial damage caused by cyber-attacks in the 12 months to mid-2022 had reached $6 trillion US. That's the size of the German and French economies combined: a lot of damage.

Convergence of IT and OT

The convergence of Information Technology (IT) and Operational Technology (OT) is a factor in the growth of cybersecurity threats. Traditionally, these two technology areas have been operationally separate, using different platforms, with different objectives and characteristics. IT systems manage the core business tasks for a business, are typically updated several times a year, are easy to outsource and are rapidly being moved to the cloud in most enterprises. As business systems are Internet capable, they are inherently “hackable”, subject to regular attacks that target data as the key resource.

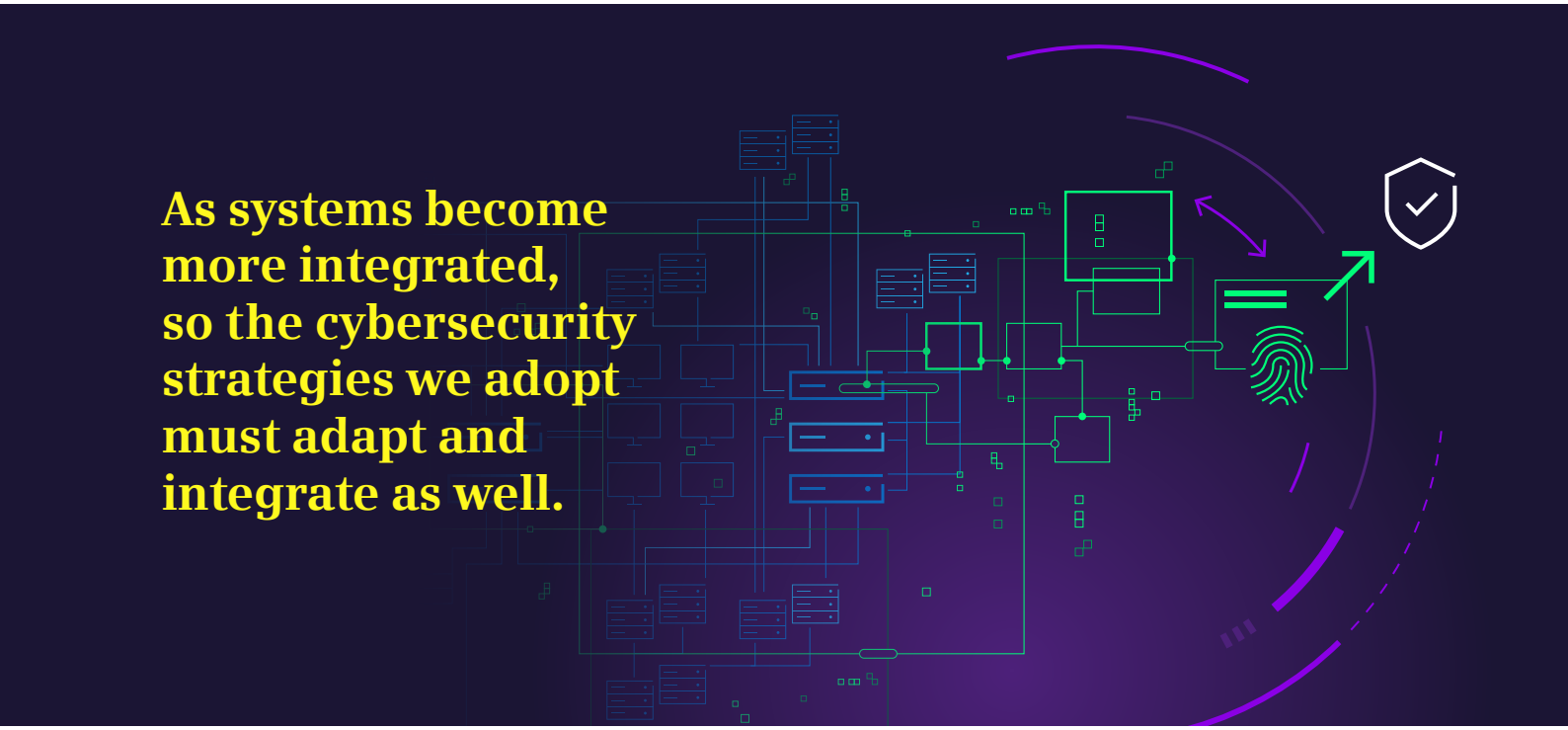
OT systems represent the core assets used to carry out the true business of the enterprise. This means the production assets, ranging from turbines and other generation equipment (for power companies) through to automated production machinery and supporting systems (for manufacturers). The key requirement for such assets is availability. In energy markets, especially, being offline when contracted to deliver power to the grid is a very serious matter.

OT assets need to be seen as a separate class of technology, and require their own management approach and cybersecurity strategies.

Simply applying IT methods to OT will not deliver the desired outcomes. In addition, OT assets tend to have much longer lifecycles than IT systems, so will normally be less cyber-mature than equivalent IT systems and are also more accessible than in the past, because they are more connected.

Convergence makes businesses much more efficient and responsive to changing needs. This inevitable trend, however, can make OT assets visible to external bad actors for the first time. Earlier threats required physical access to the production assets concerned, delivered by USB sticks. Now, it is possible to enter the environment through the Internet, which is a major change.

As systems become more integrated, so the cybersecurity strategies we adopt must adapt and integrate as well.



Compliance and certification

Regulatory evolution and growth

Governments and pan-region regulatory bodies have become increasingly concerned about the potential for serious economic and social disruption that could be caused by systematic CNI cyber-attacks, particularly targeting power generation and distribution businesses.

New standards have now been introduced for CNI companies, while regulators are more efficient in testing compliance and have greater powers to punish non-compliance. As we will see, the basic regulatory frameworks and corresponding standards are in a state of continuous evolution, while new concepts are also being tested. Key regulatory regimes include (but are not limited to):

EU Network & Information Systems (NIS) directive

This is the Europe-wide framework for protecting all forms of IT-based and IT-reliant systems and infrastructures. Based on an original European Commission Directive of 2016, the regulations have been continuously updated to reflect the changing nature and intensity of cyber-threats. Though primarily targeted at enhanced cybersecurity, the regulatory scope is very broad, covering any incident that is likely to disrupt major economic systems, and for any form of threat. At best practice level from conception to retirement, with lowest possible operational risk.

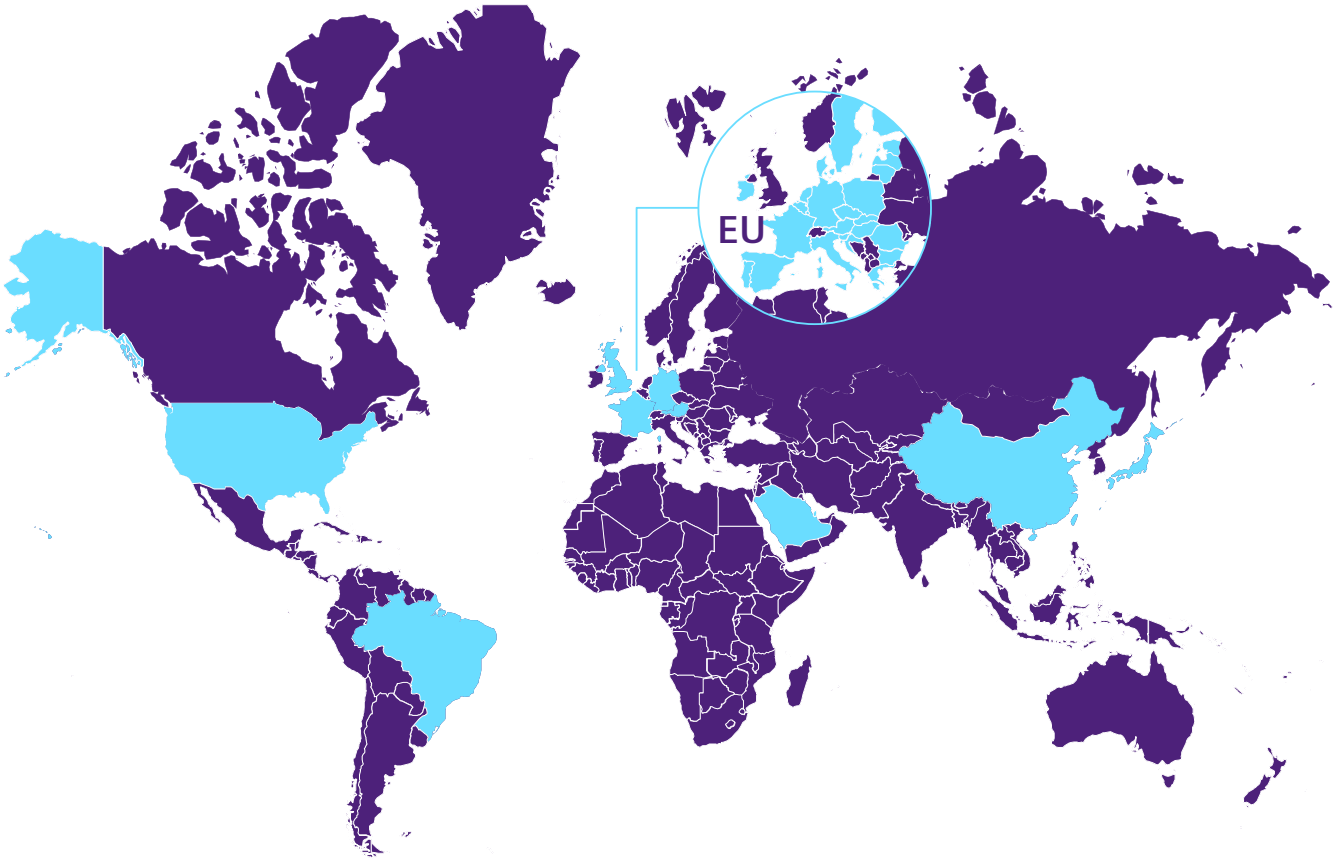
Critical Infrastructure (KRITIS)

Developed by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik), the KRITIS system is compliant and compatible with the over-arching EU framework (NIS), but adds requirements related to registration, inspection and information specifically related to the German economy.

North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)

This is the United States cybersecurity framework, designed to manage threats and protect infrastructure, with a key focus on what is terms the Bulk Electric System (BES). NERC is the de facto standard for the whole of North America, specifically adopted across most Canadian provinces and in some parts of Mexico. NERC CIP essentials include effective protection against attacks, through to restore and recovery plans. Strict controls are enforced across all BES operations and immediate notification of threats to the regulator is a basic requirement.

Other regulatory bodies enforce their own standards, of course, but most of them use either NIS or NERC as models for development.



Country	Title	Type
Brazil	Resolução normativa aneel N° 964	Law
	Manual de Procedimentos da Operação	Regulation
	Requisitos operacionais para centros de operação e instalações da Rede de Operação	Regulation
China	China Cybersecurity Law	Law
EU	General Data Protection Regulation (GDPR)	Regulation
	Cybersecurity Act	Regulation
	Cyber Resilience Act	Regulation
Austria	NIS Act	Law
France	Critical Infrastructures Information Protection (CIIP) Law	Law
Germany	IT-Sicherheitsgesetz 1.0	Law
	IT-Sicherheitsgesetz 2.0	Law
	Telekommunikationsgesetz	Law
	Energiewirtschaftsgesetz	Law
	BSI-Kritisverordnung 2.0 - BSI-KritisV 2.0	Regulation
	IT-Sicherheit im Energiesektor	Law
	IT-Sicherheitskatalog für Strom- und Gasnetze	Law
	IT-Sicherheitskatalog für Energieanlagen	Law
	Verordnung zum Schutz von Übertragungsnetzen	Law
Japan	Act on Prohibition of Unauthorized Computer Access	Law
	The Basic Act on Cybersecurity	Law
Qatar	National ICS security Standard	Law
Saudi Arabia	Essential Cybersecurity Controls (ECC – 1: 2018)	Law
	Critical Systems Cybersecurity Controls	Law
	Operational Technology Cybersecurity Controls	Law
United Kingdom	The Network and Information Systems Regulations 2018	Law
United States	North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)	Law
	NIST Cybersecurity Framework 1.1	Law
	Executive Order on Securing the United States Bulk-Power System	Law

Examples of the cybersecurity laws and regulations in place in different selected countries and parts of the world.

Standards and certification

Regulations impose requirements on CNI and other organisations. To be compliant, and prove compliance, these bodies must meet global standards and achieve certification to demonstrate that fact. Standards in cybersecurity are extremely detailed and complex, requiring high levels of investment and exceptional capabilities.

It is worth noting that Gartner's latest report into cybersecurity proposes reframing the role of Chief Information Security Officer (CISO) away from simply being the person charged with preventing breaches and ensuring rapid recovery to being a corporation's lead risk manager. This implies a more proactive role, as businesses seek to build competitive advantage on assured cybersecurity performance. The new breed of security standard builds on this broader, more inclusive definition, putting cybersecurity where it should be: not just as a defensive structure but as an effective way to strengthen and add depth to the existing risk management systems.

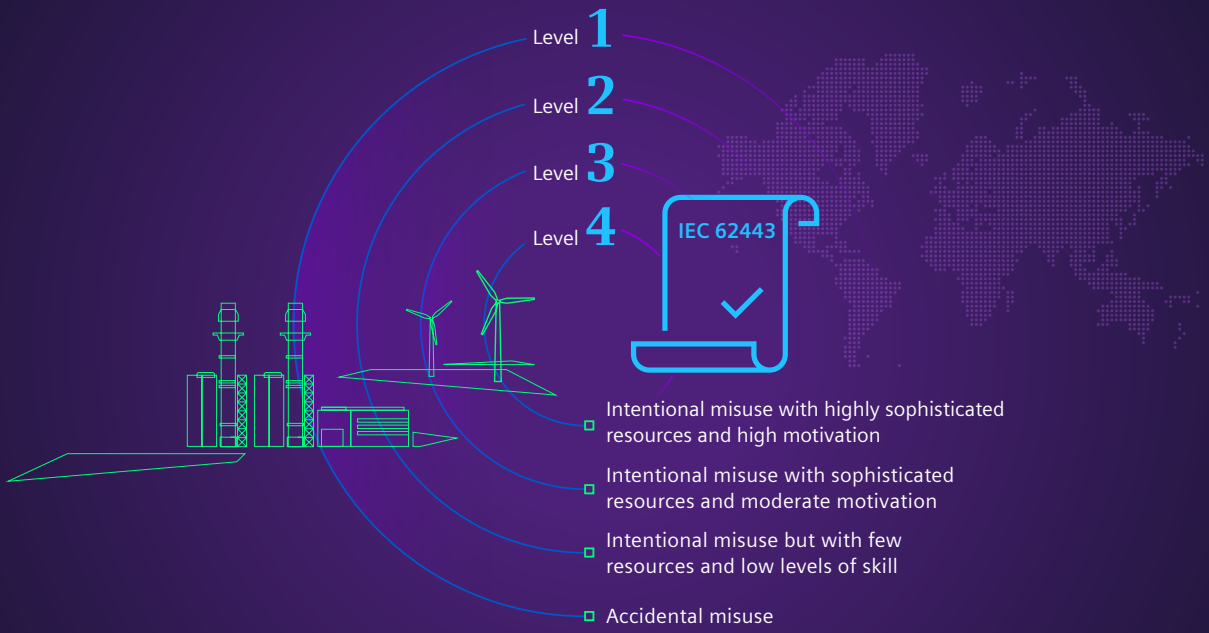
The core standard for developing and successfully managing an Information Security Management System (ISMS) is ISO/IEC 27001.

Siemens Energy is certified as compliant with this standard, which is the basic foundation for all of the more targeted and specialised forms of cybersecurity.

The lead standard for cybersecurity in CNI is the ISO/IEC 62443 family of certifications. These standards have very deep roots, with the first steps in creating a truly effective, always evolving set of standards beginning in around 2002, before the International Standards Organisation (ISO) and International Electrotechnical Commission (IEC) merged to form a single, global body.

The 62443 family of standards is defined by ISO/IEC as "horizontal", which means this must form the foundation for any cybersecurity approach used by major bodies in CNI and related industries. All systems, techniques, methods and applications must be based on the 62443 approach and be compatible with them. Technical requirements are generally assessed as being compatible with four different levels of potential hazards (see graphic below).

As we shall see, the Defense-in-depth concept is highly relevant to this approach. Enterprises that achieve the highest levels of certification will be able to cope with all these challenges, and that is certainly the case for Siemens Energy.

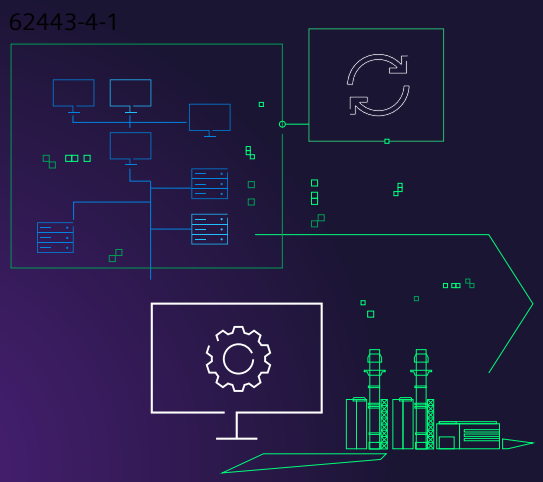


Siemens Energy certifications

As part of the development process for the extended scope of Omnivise T3000, Siemens Energy has successfully gained certification in two parts of the ISO/IEC 62443 family: 62443-4-1 and 62443-3-3. These focus on the two most important aspects of this ground-breaking cybersecurity approach.

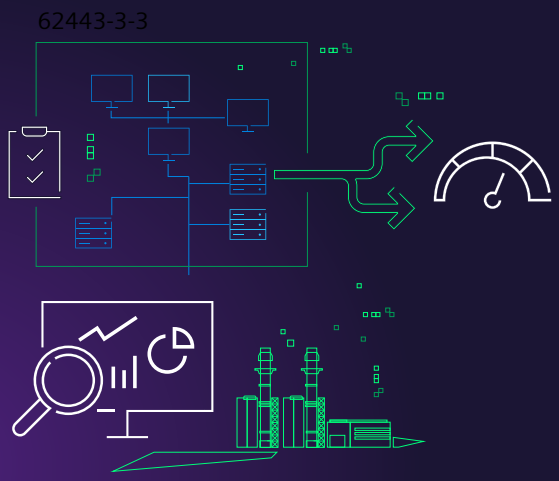
62443-4-1

drives secure development within all industrial automation products and systems. It defines a form of secure product lifecycle that ensures, not simply adequate security quality standards from the earliest stages of development but also ensures all upgrades, enhancements and developments over extended time periods reflect latest insights on emerging threats. This keeps the product and solution platform at best practice level from conception to retirement, with lowest possible operational risk.



62443-3-3

applies specifically to industrial control systems, with a strong focus on continuous assessment, testing and rapid improvement as new threat vectors are identified and analysed. This sees cybersecurity as a continuous cycle of actions, with every update tested for viability against known and emerging threats, leading to further changes as part of a non-stop evolutionary development process that becomes a fundamental part of development and operations.



Siemens Energy sought and achieved certification to the highest level in both of these standards, seeing this as a basic necessity for a control solution that is destined to have a major influence on the security and efficiency of CNI across the world. Meeting these standards is essential but it is only the start of our cybersecurity approach. In the next section of this paper, we will see how compliance and standards fit into the wider context of a proven and successful cyber-strategy.

Cybersecurity strategy and methods

Siemens Energy strategy

Cybersecurity solutions do not exist in a vacuum: They depend on every aspect of the business, its culture, working practices, core processes and, above all, on the commitment and attitudes of its people. Siemens Energy builds security awareness and responses into everything it does, from selection and training of individual employees to structure of processes, right through to product design, which we will touch on later in this chapter. Building on its Siemens group heritage, Siemens Energy now has around 160 years' experience in designing secure industrial systems, and this know-how is key to the ways in which we work with clients to co-design and implement effective cybersecurity solutions.

Our approach is based on engineering problems out of our solutions at design and development stage, before implementing a coordinated lifecycle strategy focused on Product & Solution Security (PSS) and Defense-in-depth. As a leading manufacturer and industrial player, Siemens Energy has one major advantage over cybersecurity specialists with IT-only heritage.

We know how serious the potential problems can be in the industrial setting and are also very clear about the reasons why some industrial machine operators are reluctant to take the necessary steps to protect their OT assets.

- A major systems overhaul can be disruptive and costly, not only in overheads (investment in new systems, consultancy time ...) but in lost production. The same concerns are also true when it comes to key software patches. It is not always clear how effective these will be in the OT environment, nor what unexpected problems might arise. At least until recently, some major companies simply did not implement these upgrades due to lack of confidence.
- The role of digitization is not always understood. Operations leadership can quantify the improvements in efficiency, together with reductions in energy costs and wastage. The changed risk profile is much harder to comprehend.
- Lifecycle implications may also be underestimated (as noted in ISO/IEC 62443-1-4), together with the different approach that may be needed now to keep production platforms (which are subject to upgrade, perhaps on an annual basis) at best practice security level.

As owners of production assets increasingly move towards deeper partnership models (in some sectors even leading to asset lease, rather than ownership), so it becomes even more important for them to understand the cybersecurity implications of every decision, every partnership, and every move to the use of cloud-based digital native systems.

Although Siemens Energy is a confident and innovative user of digital techniques, we are rooted in the world of OT and industrial production. Our approach to digitization therefore begins in the OT landscape and focuses on securing assets end-to-end throughout their lifecycle. We have defined 62443 standard-assured blueprints, which provide templates for use by engineers at design, development, test, planning, review, upgrade and all forms of operational levels.

This approach ensures that cybersecurity requirements are always top of mind for all those participating in the entire product value chain, no matter who they work for and what their responsibilities. This is an engineering response to this essential requirement. It is the key to ensuring that Siemens Energy solutions meet and exceed security expectations in every way.

Product & Solution Security

Modern DCS solutions must be engineered to be Secure by Design. This is the concept that states systems should be built from the ground up with security in mind, following secure development, procedures and policies in line with best practices, aiming to develop a system that is inherently more capable of withstanding cybersecurity threats.

Security by Design is not only about using secure practices but also covers processes related to engineering and installation, together with security of the supply chain and external components connected to the DCS, including service providers and asset owners.

Siemens Energy DCS solutions have secure networking protocols, are able to track assets, and have effective controls over assets that are both physical and virtual, on-site and remotely located.

Siemens Energy has its own internal processes for developing its control system Omnivise T3000 in a secure way, with an entire department responsible for driving and securing digitalisation by holistically protecting Siemens Energy's information security (IS), OT security and the security of products and solutions. Processes are always focused on five stages of cybersecurity awareness:

Stage 1 Working within strong and constantly tested, reviewed and updated security policies, ensuring that all products and solutions are designed to the currently enforced, most recent updates of applicable standards and regulations.

Stage 2 Uncompromising attitude to training, so that every individual engineer involved in design and development has accreditation, with effective training and supervision.

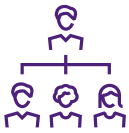
Stage 3 Automation where applicable, using proven systems to carry out core routines to ensure that human error can be eliminated.

Stage 4 Security monitoring is used continuously, ensuring the correct procedures are followed and that they are still secure and valid.

Stage 5 Constant reviews are carried out throughout the entire development activity, testing each protocol and procedure to identify either persistent or new and emerging weaknesses.

The goal is to ensure that problems are engineered out in the early stages, making vulnerabilities as rare as possible. Building on these core principles, we incorporate all Siemens Energy cybersecurity knowledge and expertise in our integrated Product & Solution Strategy, which defines how we approach and manage cybersecurity issues at the deepest level across our activities. The key factors in this strategy can be defined as:

Security as competitive advantage.
Effective cybersecurity is a core requirement today, not a "box-ticking exercise", because we know that outstanding cybersecurity assurance and performance is critically important as a differentiator in the market. We embed cybersecurity requirements into every stage of our activities, demonstrating that our solutions deliver to the highest regulatory standards, and contribute to building trust in the performance of our customers.



Security anchored in the organization.
Cybersecurity is not an "add-on" to normal processes. At Siemens Energy we ensure that security is a basic and important part of every process and activity. The PSS approach is embedded into business strategies and planning, and is an integral part of implementation programmes.

Performance monitoring and continuous improvement targeted on PSS is a part of every individual's assessment and is now at the heart of all risk assessments and risk management activities.

Contribute to improved global standards.
Siemens Energy makes an active contribution to testing and enhancing global standards. As an industry leader, we have a special contribution to make in terms of insight and know-how. Siemens Energy is also seen as a trusted partner, delivering advice seen as objective, honest and useful.

Improve and simplify processes continuously.
The best way to ensure that cybersecurity is engineered into every aspect of product design and development is to keep processes intuitive, simple and easy to use. That is a key concern of our PSS approach. Cybersecurity components are not supposed to be obstacles but useful tools, that are well-designed and highly intuitive in operation. We enhance and improve security processes constantly to make them simple and unmissable. That is the key to sound security engineering. The graphic on the next page gives a simplified view of PSS.

Product & Solution Security (PSS)

Governance

Comprehensive governance framework based on long-term expertise, domain know-how and international standards.

Secure Products

Secure Solutions

Secure Services

Processes

- Business processes (e.g. Product Engineering or Product Lifecycle Management) include security activities such as PSS project classification, security threat & risk analysis or security testing
- Supply Chain Management process includes PSS secure supplier and component selection
- Secure service operation (e.g. field, digital or software services)
- Incident and vulnerability management
- Risk and opportunity management

Technology

- Defense-in-depth protection
- Network security
- Identify and access management
- Secure remote access via common Remote Service Platform (cRSP)
- Data security and integrity protection
- System hardening
- Malicious code prevention
- Security logging and monitoring
- Intrusion and anomaly detection
- Backup and disaster recovery
- Physical security

People & community

- Roles, responsibilities and job-profiles
- Qualification and training
- ProductCERT
- Expert network
- Regulation and standardization activities
- Collaboration with authorities and industry bodies
- Consulting
- Communication

This exemplifies the holistic and integrated nature of the strategy. It covers products, solutions and services, ensuring that every component is covered with equal depth and detail.

- It begins with governance, and includes strategic level initiatives (like PSS) and executive leadership, with specialist officers, backed by security tools and databases.
- It covers our core processes, from Product Lifecycle Management (PLM) at one end through to managing risk and dealing with incidents. In both highly proactive and effectively reactive ways, our processes are engineered for security.
- It covers our technologies, from design to data, access management to physical security. Every part of the technology environment is constantly evaluated, compared with new options, tested and subject to enhancement or replacement as required.
- It covers our people, above all, because we recognise that the human factor is critically important but sometimes underestimated as part of the overall security mix. From initial selection at recruitment stage to onboarding, personal development certification, oversight, and development, we make cybersecurity the responsibility of everyone at all times, across the entire community.

Our PSS approach is designed to ensure that security awareness of management is always present at every level in every activity. It is supplemented by the critically important security vision known as.

Defense-in-depth

Defense-in-depth (DiD) is a strategy for comprehensive protection of complex systems by engineering layers of defences into a system to ensure you are never dependent on any single means of defence. The concept means that every attack, from external or even internal actors, encounters multiple obstacles.

These not only have the potential to defeat an attack but also slow down the progress of such attacks, while providing rapid warning to security professionals, giving them notice of the attack and enabling counter-measures to be launched. The more layers of security technologies, procedures and solutions in place the bigger the "cost of an attack" is to a threat actor trying to access the DCS. This plays a key role in discouraging and reducing the frequency of such attacks.

In an OT environment these layers could include patch management, malware protection, access controls, secure architecture, policies and training. These additional layers of security reduce the size of the attack surface, making it much less likely that an attacker will break through all the layers. Other steps that can be taken for an effective DiD strategy include:

- Hardening DCS components to limit their exposure to external systems and networks.
- Having adequate DCS access controls to help protect operations. Physical and logical access controls help ensure only those authorized and authenticated can access the DCS to make control operations and create changes.
- Regular cybersecurity training for DCS staff provides personnel with the knowledge to act in a secure way and identify unsecure activities related to the DCS.

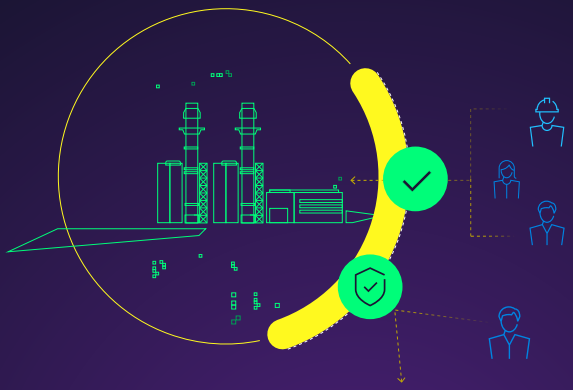
In purely technology terms, the accepted formula for effective DiD is to provide four self-sufficient but interconnected solution layers focused on:

Perimeter defence

Presenting a hardened external face to the world, ensuring that all attempts to pass through the perimeter are properly evaluated, so that only authorised access is permitted.

Host protection

Making sure that the entire infrastructure environment, whether on-premise or cloud-based, is secure and resistant to viruses and other forms of infiltration via potential “weak points”.



Operating systems and applications

Form potentially the most complex area of vulnerability, with near continuous interaction required between large numbers of users, some from outside the organization. Here access protocols will be enforced strictly and all possibleconcerns flagged at once, with access immediately denied.

Data protection

Covers both data at rest (stored in secure sites, with clearly defined and controlled access) and data in transit (where the integrity of each specific network connection and process will be managed individually on a no-trust basis).

Once this technology focus is combined with employee reviews, administrative processes to eliminate errors (as far as humanly possible) and rational security policies, the result should be a secure and well-managed information environment. This approach does not eliminate threats, but it does at least make sure that “everyday” safeguarding issues will be managed successfully.

The Omnivise approach

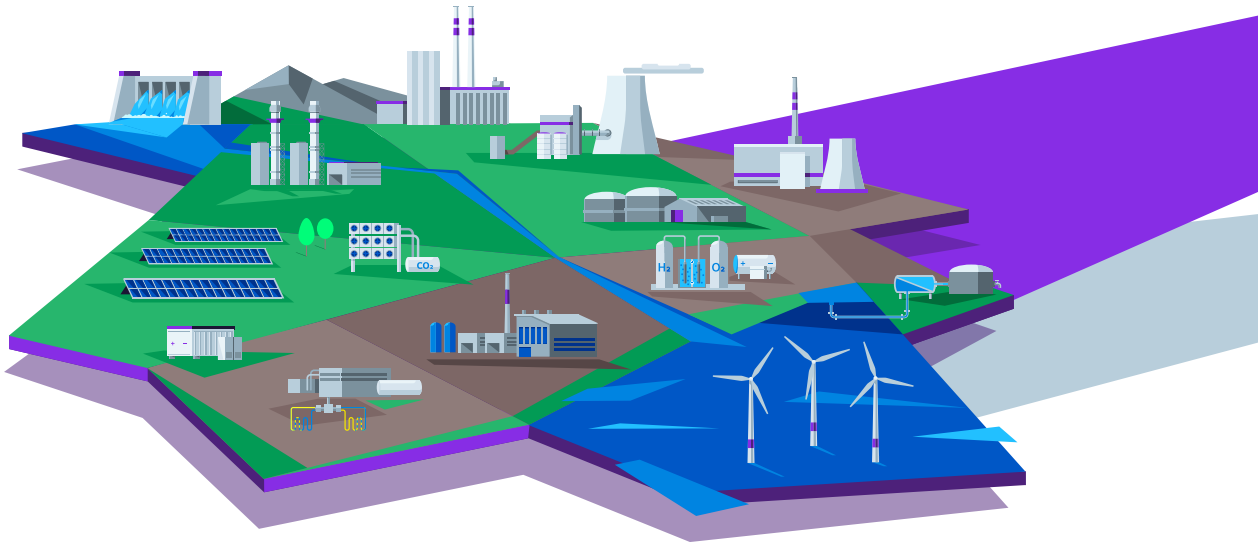
The new energy structures

We stated at the beginning of this paper that a radical change in the development of energy generation and distribution is one key factor in making cybersecurity for CNI a higher priority than ever. The world is moving away from the long-established model of very large, central power generation systems to a more distributed landscape, with many different kinds of energy source, an increasing proportion of them renewable. Not only is this a much more complex CNI environment than in the past, it is also potentially more vulnerable.

The reality of energy generation and distribution today is that the modern equivalent of major coal-fired power plants is now likely to be huge windfarms some distance out to sea. These are efficient and reliable but also vulnerable to physical and virtual compromise, with the need for monitoring, surveillance and rapid response, all through connections that cover a great deal of distance and require Internet and cloud enablement. In the distribution grids, the move away from fossil fuels to electric vehicles, and from gas heating to electric heat pumps adds a greater burden on the grids, themselves.

We are now seeing new developments, such as bi-directional grids, the use of EV batteries as temporary storage for power in the grid, different commercial bodies and complex new methods for system design and maintenance. Yet one factor has not changed and will never change: the need for availability, power continuity, meeting demand, no matter what. The role of system management and control is more sensitive than ever, and cybersecurity is a key factor in making a control system fit for purpose.

Omnivise T3000 has been specifically designed to provide effective, flexible security across all the diverse power generation assets in this picture. It provides an integrated, standards-compliant IS Management System to support our complex energy landscape deliver energy continuity combined with environmental and cost benefits.



The energy landscapeof the future will be complex, mixed and distributed.

Infrastructure designed for security

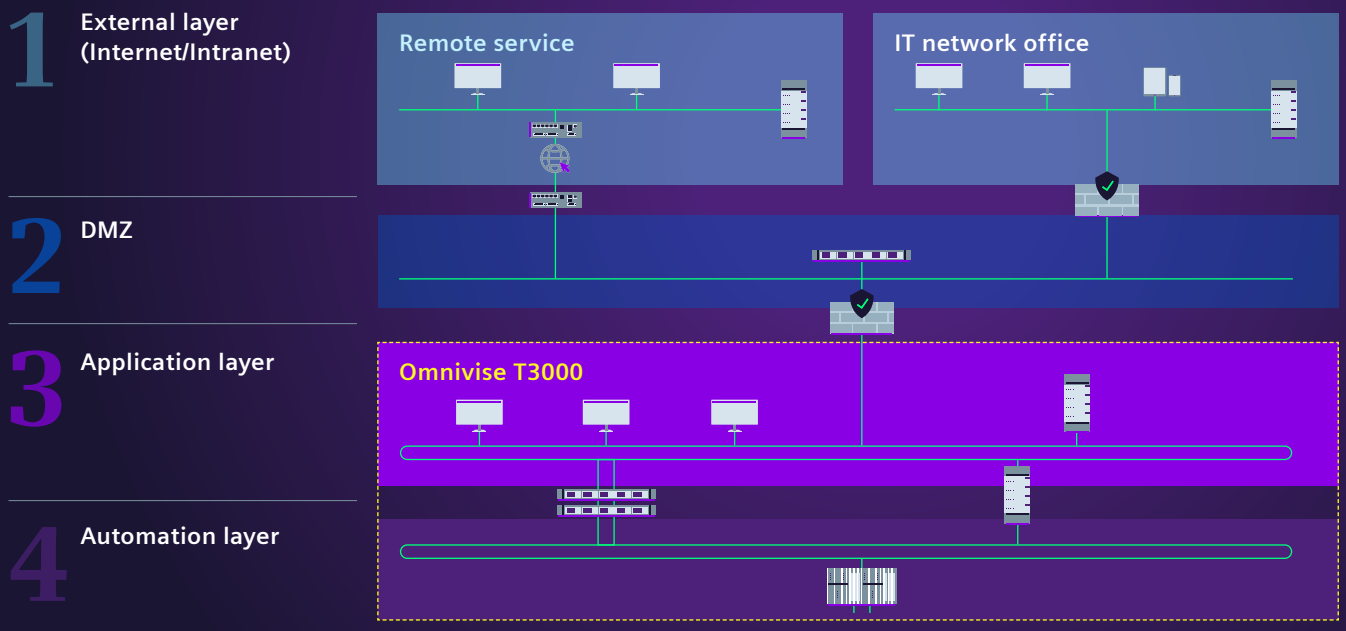
Omnivise T3000 has been designed, structured and engineered for maximum security at all levels. Key design features include:

Layer architecture.
Using the Defense-in-depth approach, T3000 is built in a series of separate layers, each one having its own security safeguards, ensuring that compromise in one layer does not undermine the integrity of the whole solution.
The main layers in the architecture comprise:

- **External access layer**, which is where communication is most open and interfacing with internet and intranet-based assets and where personnel is enabled.
- **Demilitarized zone (DMZ)**, which protects the rest of the solution and the wider environment from external access. The DMZ is placed between the Internet access layer and the rest of the environment, enabling all access requests to be scrutinised and carefully managed, with threats spotted and stopped at this stage.

  Note there may be more than one DMZ in the structure, depending on access requirements. The key principle is that there will ALWAYS be a DMZ between any external access and the rest of the system.
- **Application layer**, which hosts the T3000 appliction software needed to manage the production plants and systems. This also includes the main cybersecurity functions and features, such as the security server, application whitelisting and Security Information and Event Management (SIEM).
- **Automation layer**, this is where tools and capabilities that enable operation of production assets and automated functions of every kind are situated, and also where system intelligence is housed. This is an area of maximum security, because it is able to carry out specific actions with no human intervention.

To ensure further defence against security threats, each layer is air-gapped from the others, further reducing the potential for penetration.



Omnivise T3000 security zone architecture based on protection requirements

Hardening. Individual components are given their own security strengthening protocols as defined and advised by the Center for Internet Security (CIS). Using these industry-standard benchmarks, we can ensure that components can withstand attacks even if system-level safeguard fail. Hardening involves, among other things, removing unnecessary software, constant changes to passwords and cutting out unnecessary services.

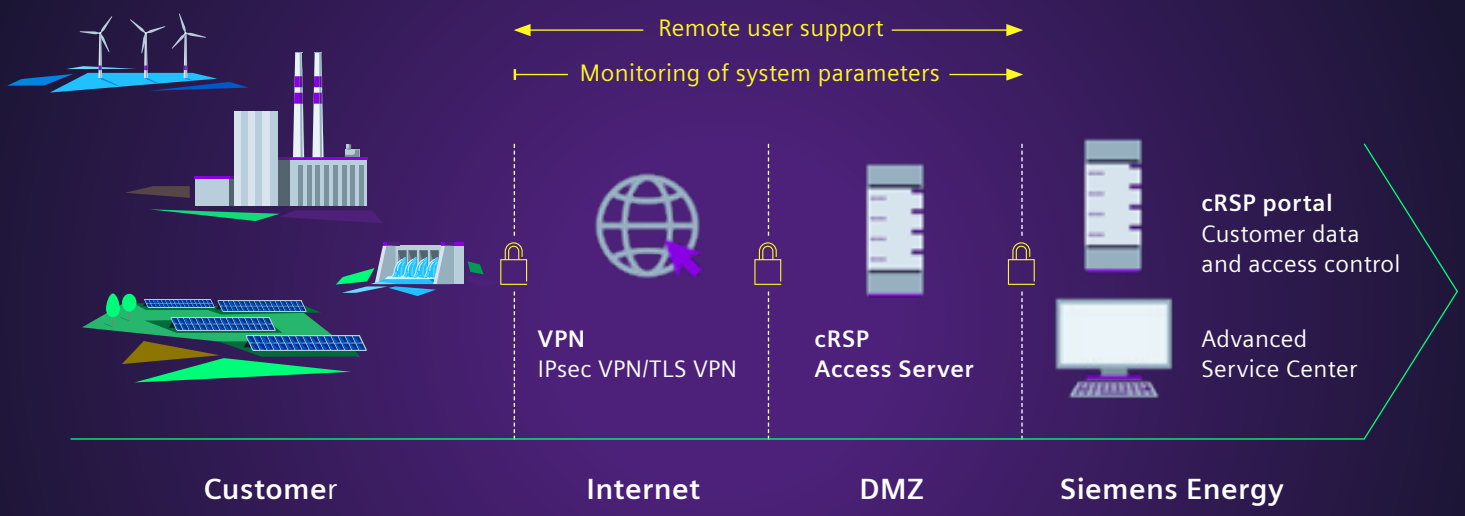
Communication management. Where communication is required between layers and components, this is secured via such methods as spatial separation, firewalls and point to point tunnels.

Network structure. To protect the customer's network as well as the Siemens Energy environment against reciprocal problems and attacks, we have secured the common cRSP server in a so-called DMZ which is secured on both sides by firewalls. The reverse proxy server establishes the connection to the customer's system and mirrors the incoming communication to Siemens Energy.

This prevents a connection from being set up between the Siemens Energy environment and the customer network via unauthorized protocols, since the mirroring takes place only for predefined protocols. This architecture prevents, for example:

- Unauthorized access from one network to the other
- Access from a third network (by hackers, for example)
- Fraudulent use of secret passwords or other access data
- Transmission of viruses or other harmful programs from one network to the other

The graphic below shows how communication and access methods are designed to provide additional protection.



Secure communication that safeguards access to the DCS

Virtual Private Network (VPN) via broadband connection.
We generally recommend using a secure broadband connection over the Internet. This offers maximum level of security, high data transfer rates, high availability, and access to all Siemens Energy Remote Services. The cRSP is relying on two types of VPN technologies: IPsec VPN and TLS VPN.

Security measures for IPsec. Siemens Energy uses the established standard IP security (IPsec) with preshared secrets for encrypted and authenticated data transmission. Preshared secrets consist of an arbitrary string of minimum 12 random characters.

Security measures for TLS-VPN.
The Transport Layer Security (TLS) protocol can be used as an alternative for hardware-based VPN endpoints (IPsec). Before a connection is set up, the device must be registered with a one-time password (OTP). The TLS connection to the VPN server can be established only if the server certificate was signed by an internal Siemens Energy Certification Authority (CA). This ensures that only this specific device can communicate with the cRSP servers. An additional harware-based hash ensures that no unauthorized copy software can set up a connection to the cRSP server.

Security measures in the customer network. The main security features depend on the selection and configuration of the chosen cRSP access router at the customer's end. In principle, a distinction is made between Customer Owned Access (COA) and Siemens Energy Owned Access. In addition, SSL-VPN client is available for fixed and mobile connections. These connectivity options, including the ports to be opened in the firewall for an operational remote connection, are illustrated and explained in detail in the appendix.

Secured cRSP server. Siemens Energy uses Linux servers exclusively for our cRSP access servers. These are designed for stability, while frequent updates make sure that actively developed distributions remain secure.

Secure remote support. Providing effective support is an essential part of the T3000 service, so all aspects of this service are managed via the Siemens Energy common cRSP. This establishes VPN tunnels to ensure that no external access to communication is possible, and two factor authentication is used to further ensure that support services cannot be a point of vulnerability.

In addition to the core functionality of the T3000 solution itself, Siemens Energy customers can also access a growing range of support services. These include:

- Cybersecurity hotline (for reporting issues and requesting intervention).
- Patch Management support, ensuring that every aspect of the solution is automatically kept at best practice level.
- cSOC, providing permanent shared security services, with specialist consultants monitoring performance on a 24/7 basis.
- Consultancy design services, in which Siemens Energy experts can be deployed to identify vulnerabilities in an existing system and provide input to design enhancements.

Finally, we need to understand the market reality, which is that all customer systems are likely to be hybrid, which include technologies provided by a range of suppliers, including Siemens Energy. In a T3000 DCS solution, therefore, we need to consider the integrity of what is normally known as the "System Under Consideration" (SUC), which comprises the total technology landscape relating to the DCS, including standalone controls and monitoring systems across the entire landscape.

Siemens Energy certifies its own technologies meticulously and is able to evaluate other systems, as well. This means that we can carry out cybersecurity monitoring across the complete environment, identifying threats and giving early warning of emerging issues. This ensures that operators have a clear and transparent view of threats across their operational landscape, and can move effectively to protect themselves.

New vision for a new reality

Omnivise T3000 has been designed with the emerging energy landscape in mind. It is not an attempt to adapt old technology to a new reality: it is secured for a complex, changing and highly fragmented world. Let's briefly summarise the issues once more.

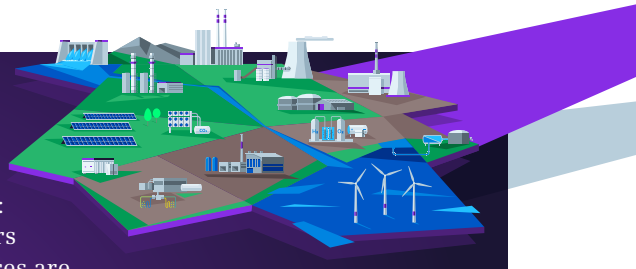
Complexity. Power generation is moving from centralised fossil-fuel driven plants to a network of smaller power plants that use everything from wind, solar, tide, hydro, geo-thermal, biomass, waste, nuclear (including potentially small-scale local plants). This diverse set 'of resources must be harnessed and united into a steady, reliable, energy flow for distribution grids that may need to provide double today's capacity in the next two decades.

Threats. This major strategic change has the unwanted consequence of making threats more persistent, harder to track and likely to cause disruption to entire energy systems due to weakness at just one or two specific points.

In a distributed energy environment managing cybersecurity is certain to be a challenge. The world needs solutions that are specifically designed to meet that challenge.

Solutions. Omnivise T3000 builds on a long heritage of successful operation in large-scale power generation plants, with roots that go back to the earliest Siemens I&C solutions, more than 50 years ago. The new iteration of T3000 has been redesigned and re-engineered to incorporate the capability needed to manage an entire network of individual power generation solutions, geographically dispersed and based on multiple different technologies.

Using a combination of secure connectivity, distributed intelligence and an engineering approach that has security at its heart, we can for the first time make the emerging distributed energy market work more effectively and more securely than all those long-established energy systems, which are now being made obsolete.



The Siemens Energy vision

Let's end with the same thought that started this paper: the environment. Changes from large central generators to multiple distributed, largely renewable energy sources are not happening for frivolous reasons. They are happening because climate change is real (the evidence is now overwhelming and the scientific consensus almost 100%) and the dangers this presents to human society are incontestable. We have to manage the move to clean energy fast. It took about 200 years for society to move from a world of wind powered ships, horse-drawn carts and wood fires for cooking and heating to the hyper-industrialised society of the 20th Century, with its absolute dependence on fossil fuel sources for everything, from light to heat, transport to manufacturing and beyond. To keep climate change within just about manageable limits, we have to manage an equally disruptive transition in about 25 years maximum. What we can see is that the growth in renewable energy sources is being managed faster than expected, keeping to this tight schedule quite successfully. The issues now lie elsewhere: in management and controls. To coordinate, collate, deliver and quantify the energy society needs is a huge and challenging task. Without effective, strategic level management systems, the clean energy revolution cannot happen. Omnivise T3000 has been designed to carry out exactly this task, safely.

Published by

Siemens Energy Global GmbH & Co. KG
Gas Services
Siemenspromenade 9
91058 Erlangen, Germany

Siemens Energy. Inc
Gas Services
4400 N Alafaya Trail
Orlando, FL 32826, USA

siemens-energy.com/omnivise-t3000