8 DECENT WORK AND ECONOMIC GROWTH

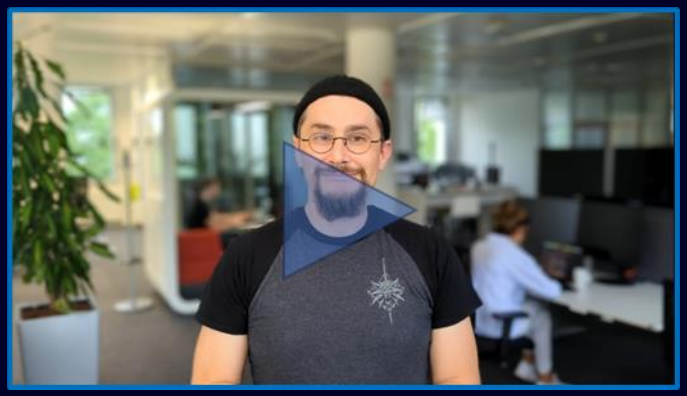
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE

12 RESPONSIBLE CONSUMPTION AND PRODUCTION

Sustainability through cybersecurity

Enabling IT & OT Systems with Zero Trust Technologies

Cybersecurity isn't just about protecting devices; it's about safeguarding a sustainable future: Imagine an environment that operates safely and effectively without interruption by malicious actors. Envision a world where everything and everyone collaborates dynamically in creating the values and goods we need. This includes reducing machine downtime, conserving valuable resources, and ensuring the protection of every entity, device, and person involved.



At Siemens, we consider cybersecurity as one of the company's sustainability goals. We live in an ever-evolving environment filled with digital threats and risks. Only through robust cybersecurity can we effectively address those risks. This includes safeguarding information and intellectual property by preventing digital attacks from materializing in the real world, or by supporting businesses and production sites to operate without disruptions.

"Identity-based Access" and "Never trust. Always verify." are fundamental Zero Trust principles for combining the digital and the real world: From humans to robots, from applications to data, every entity not only requires a tamper-proof identity, it also requires technology that facilitates deploying such identities in an easy and secure manner. Technology used at ease will simplify the life of employees, create acceptance, trust, and finally create a more secure and safe world for us all.

Zero Trust is an important architecture for modern cybersecurity. This holistic approach aims to use as many high-quality, real-time signals as possible to verify and authorize access in all information technology and operation technology areas. Knowing the identities of those with whom we interact instills confidence and peace of mind in all of us.

However, Zero Trust in industrial systems poses unresolved challenges:

As of today, Operational Technology (OT) environments consist of a variety of components. These components are not only difficult to inventory, maintain and reuse without precise identification, but legacy OT communication protocols are also not Zero Trust enabled. It's a similar story in Information Technology (IT) environments, albeit with some differences. Identities play a crucial role to both sustainability and Zero Trust, as we can only handle what we can identify.

Why Zero Trust?

New working models and new trends in the design of OT environments require a paradigm shift in security architectures: what you are allowed to do can no longer be based on the question "where are you", but rather on the question "who are you". Home office should be no different from work in the office; the office will eventually be a place where people from different organizations collaborate. A similar transformation is expected in production environments, where different players will work together in one factory. The Zero Trust architecture enables this new security paradigm in a scalable and manageable way.

With Zero Trust we can apply the principles of "Identity-based Access" and "Never trust. Always verify." to the existing world of Operational Technology (OT) and Information Technology (IT) everywhere at Siemens: in all our applications, devices, products, factories, and locations. This will not only allow us to collaborate easily and securely with our partners and customers, but also to deliver solutions aligned with the latest security standards and models the world has to offer.

Zero Trust will protect critical infrastructure and marks one key component of the successful digitalization of OT & IT environments. It will supercharge a sustainable and digital transformation by providing a foundation for secure and scalable growth while bringing the focus to productivity, innovation, and a faster

time to market. Implementing and enabling Zero Trust at Siemens and providing it as a standard solution for our customers will have substantial impacts for all of us:

- Siemens products are built to last for decades. This is impossible without a state-of-the-art security architecture.
- Boosting Cybersecurity with the protection of sensitive data and processes, will prevent unauthorized access to critical information, systems, and infrastructure.
- We can foster a more secure digital environment for society, by breaking the never-ending circle of cyber threats.
- Other organizations will benefit from our knowledge and will be able to adopt sophisticated security measures and promote optimal security practices.
- We will promote more confidence in partners and customers, ensuring they can trust the identity of everyone, and everything involved in their collaborations, products, digital tools, or services they are using.
- Our products will enable our customers to build more dynamic, efficient, and thus more sustainable production environments.

In a nutshell: With industrial Zero Trust we will ensure Siemens' devices, products, applications, locations, factories and security services to set the state-of-the-art and make the world a more connected, more secure place. It will help extend the usage for factory machines and increase productivity even further. It will support a decrease in cybersecurity risks and resulting processing costs or emissions for production lines, applications, devices, and products and render collaboration with partners and customers more sustainable.

What are we looking for?

The challenges we face are easy enough to describe but hard to master: We are looking to implement Zero Trust principles everywhere at Siemens, in all our applications, products, factories and locations to easily and securely collaborate with our partners and customers and to deliver solutions aligned with the latest security standards and models the world has to offer.

Have an impact and solve the Zero Trust challenge by sending in:

- Your proposals and design ideas on how to equip different OT devices with a secure identity, since these devices often operate in a (near) real-time environment while their IT-capabilities are constrained or limited.
- Your solution ideas on how to integrate existing, legacy OT devices and machines into Zero Trust architectures.
- Concepts, processes and tooling proposals on how to equip applications with a future- and tamper-proof, unique identity, no matter which hardware or services they run on.
- Your ideas on how to make existing legacy communication protocols aware of Zero Trust principles.

Make sure to consider recent standards and concepts in this area, like the IEEE standard for secure device identities (IEEE 802.1AR) or IETF RFC 8995 for bootstrapping remote secure key infrastructure.

We're looking forward to receiving your ideas towards innovative solutions for inhomogeneous, constrained, and industrial brownfield environments in an economical and applicable way! Work together with us on your individual solution, which we will explore together in the co-creation phase within a lab environment. Our goal is to test and deploy your ideas to a real production environment!

Join us, because only with you, we can make the ideas of tomorrow a reality today!

Who are we?

We are part of the central Cybersecurity department at Siemens, looking to solve the problems of the future and looking for bright minds joining our ranks. Ethics stands for a strong sense of principles that govern behavior, and protecting ourselves with Cybersecurity is part of ethical behavior. We as Cybersecurity experts at Siemens are committed to both: to our organization and society.

Peter Stoll
Director Siemens Security Next Generation

Rolph Kreis
Cybersecurity Expert

Roland Koch
Cybersecurity Expert

Join the campaign and create impact on real problems together with go-getters and solution seekers of the world by submitting your ideas.
https://siemens.com/techforsustainability