SIPROTEC DigitalTwin Cybersecurity Aspects

Siemens · Digital Grid · Energy Automation Product Portfolio

www.siemens.com/siprotec-digitaltwin

Cybersecurity at Siemens Digital Grid

Cybersecurity in critical infrastructure operations is a highly sensitive area that demands a trustworthy partner: a technology partner who understands how products, systems, and solutions integrate with the processes and people behind them and the interactions involved. Siemens' Digital Grid products, solutions and services are based on a solid foundation: expertise in and knowledge of energy automation, customer needs and processes as well as cybersecurity in compliance with international standards.

Understanding Cybersecurity Regulations in the Context of SIPROTEC DigitalTwin

In offering digitalization applications such as the cloud based SIPROTEC DigitalTwin we take into due consideration the regulations, standards and guidelines applicable to operators of essential services and critical infrastructures in the European Union and North America. As an example, the EU Directive 2016/1148, also commonly known as the NIS (security of Network and Information Systems) directive, is focused on ensuring that operators of essential services take appropriate security measures to protect their assets and to notify their respective national authorities about serious cybersecurity incidents. Siemens, in its role as a technology partner and solutions provider is committed to address cybersecurity risks based on international security standards and best practices, and to help customers fulfil their regulatory requirements.

As a technology provider in North America, Siemens understands NERC CIP standards, which are applicable to operators of bulk electrical systems in order to protect their critical infrastructure against cyber risks. Since the SIPROTEC DigitalTwin application only serves the purpose of simulating and testing SIPROTEC 5 protection relays in a laboratory / non-productive environment, it doesn't fall under the Critical Cyber Asset classification of NERC CIP. At the same time SIPROTEC DigitalTwin provides a comprehensive coverage of cybersecurity controls relevant to cloud-based applications in order to mitigate[1] the evolving cyber risk landscape in this context.

Siemens AG
Smart Infrastructure; Management: Cedrik Neike
Digital Grid; Management: Sabine Erlinghagen, Robert Klaffus

Humboldtstr. 59
90459 Nuremberg
Germany

Tel.: +49 (911) 433 0
www.siemens.com

Siemens Aktiengesellschaft: Chairman of the Supervisory Board: Jim Hagemann Snabe;
Managing Board: Joe Kaeser, Chairman, President and Chief Executive Officer; Roland Busch, Lisa Davis, Klaus Helmrich,
Janina Kugel, Cedrik Neike, Michael Sen, Ralf P. Thomas
Registered offices: Berlin and Munich, Germany; Commercial registries: Berlin Charlottenburg, HRB 12300, Munich, HRB 6684
WEEE-Reg.-No. DE 23691322

SCF 04/2019 V13.06

Page 1 of 2

Security by Design in SIPROTEC DigitalTwin

The product development departments at Siemens Digital Grid in Germany, where SIPROTEC DigitalTwin is developed, are ISO/IEC 27001 certified. According to the established product lifecycle management (PLM) processes, a threat and risk analysis has been performed on the SIPROTEC DigitalTwin application to identify possible cyberthreats and risks, and applicable security countermeasures have been duly implemented to adequately mitigate the risks.

The security implementation is based on cloud computing related security standards and guidelines ISO/IEC 27017 and ISO/IEC 27036-4. Concrete cybersecurity controls implemented in the SIPROTEC DigitalTwin include: ‘Siemens ID’ multi-factor authentication for users to access their SIPROTEC DigitalTwin cloud application, VPN and TLS secured connection to the SIPROTEC DigitalTwin cloud instance from the customer’s PC, secured storage for SIPROTEC DigitalTwin data in the cloud, and a malware-protected virtual environment that hosts the SIPROTEC DigitalTwin instance. The host environment is hardened as per industry-standard information security policies. Furthermore, technical assessments (penetration test) are conducted by independent security testers to validate the effectiveness of the security measures.

The Siemens ID identity and access management (IAM) solution for customers and partners brings state-of-the-art security by design. Secured hashing of passwords, encrypted network communication, intrusion detection, security event monitoring, and hosting on partners with proven cybersecurity (SOC2 Type II and ISO/IEC 27001 certified) are among the salient cybersecurity aspects of the Siemens ID IAM solution used by SIPROTEC DigitalTwin.

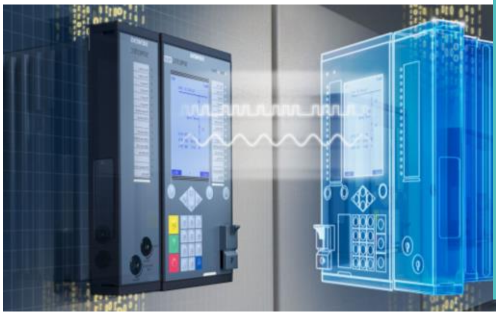
In terms of cyber incident handling and vulnerability handling (IHVH), the Siemens ProductCERT is an industry benchmark, which has ensured a transparent and responsible process of keeping customers informed about security vulnerabilities since 2011. Through ProductCERT, customers and international CERT-partner bodies will continue to be informed about security issues affecting the SIPROTEC DigitalTwin application or its cloud infrastructure.

Benefits of a trustworthy cloud platform

The SIPROTEC DigitalTwin service is hosted on the Microsoft Azure cloud platform, whose mature security and privacy practices and protection measures are certified to be conforming to ISO/IEC 27001 (information security), ISO/IEC 27017 (cloud security), ISO/IEC 27018 (cloud privacy) and ISO/IEC 27701 (privacy information management system) standards. Moreover, the Microsoft Azure platform demonstrates its compliance to the security best practices published by the Cloud Security Alliance (CSA) for cloud service providers. The security and privacy controls provided by Microsoft Azure for its customers include security incident management, response and notification, thereby enabling an end-to-end transparent incident handling, from the Azure cloud platform to the SIPROTEC DigitalTwin customers.

The Charter of Trust Initiative by Siemens

Siemens recognizes the need of making the protection of data and networked systems a prime objective in an increasingly interconnected digital world. As this can only be achieved through global collaboration with technology providers and policymakers, Siemens has joined forces with leading global companies and government authorities to form the Charter Of Trust initiative (visit www.charter-of-trust.com). Through this initiative Siemens and its partners aim to establish a platform of trust built on international security standards and binding policies, ultimately enabling industries worldwide to leverage digitalization to the maximum. Start your journey securely with SIPROTEC DigitalTwin today.



Siemens AG
Smart Infrastructure

Digital Grid

Humboldtstr 59

90459 Nürnberg, Germany

SIPROTEC_DigitalTwin_Flyer_en_V1.docx
© 2019 Siemens AG

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (www.openssl.org) and cryptographic software written by Eric Young (eay@cryptsoft.com)

[1] **Responsibility of the Customer**
Siemens points out that the Customer is solely responsible for the conception, implementation and maintenance of a holistic, state-of-the-art security concept to protect its enterprise, plants, systems, machines and networks against Cyberthreats. "Cyberthreat" means any circumstance or event with the potential to adversely impact the Customer’s plants, systems, machines and networks (including the Works) via unauthorized access, destruction, disclosure and/or modification of information, denial of service attacks or comparable scenarios. For more information on trusted security concepts, visit www.siemens.com/gridsecurity