Joint Press Release

Press

from Siemens and NATO CCDCOE

Zug/Tallinn, July 1, 2020

Siemens and NATO CCDCOE advance cooperation on cybersecurity for critical infrastructure

- **Joint training against cyberattacks key in protecting digital grids**
- **Valuable insights on attacks and vulnerabilities enable innovative solutions and safer products**

Siemens Smart Infrastructure and the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) have signed a Memorandum of Understanding (MoU) to continue the cooperation on cybersecurity for critical infrastructure. The CCDCOE organized annual high-level cyber defence exercise Locked Shields exercise provides a key pillar to jointly build up defence capabilities. With the new agreement, the parties advance their existing cooperation on cyber security training for power grids. In experimenting with grid control software Spectrum Power, Siemens gains valuable insights on the potential attack vectors and can thoroughly test new security features or protocols for its products and solutions.

The way grids are operated and managed has changed fundamentally in the last years with the integration of more renewable and decentralized energy sources. The need for network optimization, interaction between prosumers, and the number of new market participants have all significantly increased. With information and communication technology penetrating transmission and distribution networks, the

SIEMENS

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Siemens AG
Werner-von-Siemens-Straße 1
80333 Munich
Germany

NATO CCDCOE
Filtri tee 12
10132 Tallinn
Estonia

growing interconnections create more vectors for potential attacks on digital energy grids. Consequently, cybersecurity is a top priority for power system operators and government bodies.

Since 2010, Locked Shields is an annual cyber defence exercise organized by NATO CCDCOE to train cyber response teams to defend against massive cyberattacks. Siemens has teamed-up with NATO CCDCOE since 2017 to include power grid scenarios into the defense exercise, which includes systems and products such as the Siemens Spectrum Power and Sicam A8000 remote terminal units. These help to meet complex energy grid scenarios with control centers and substations which are interconnected and interdependent. In the exercise, the defenders have to set the defense lines of a complex infrastructure including various systems and applications that should withstand massive cyber-attacks executed by a large group of hackers. Keeping the lights on while performing threat hunting, reporting attacks and recovering the system are some of the challenging tasks the cybersecurity experts learn to deal with in this exercise. Locked Shields is an opportunity to learn through exercise, training and cooperation within the field of defense cyber operations.

Robert Klaffus, CEO of Siemens Digital Grid said: “Power grids and everything connected to them form the backbone of modern societies and are therefore attractive targets for hackers. The learning and experience with the Locked Shields exercise are essential to securing and protecting power grids. With the advanced cooperation with NATO CCDCOE, Siemens can gain valuable insights into new forms of attacks and how to address evolving cybersecurity challenges in digital energy grids. These insights are applied to further developments of our portfolio.” One example of testing new features as part of this cooperation is the open standard communication protocol OPC UA PUB/SUB, which is applied to many IoT-applications.

Siemens AG
Werner-von-Siemens-Straße 1
80333 Munich
Germany

NATO CCDCOE
Filtri tee 12
10132 Tallinn
Estonia

Colonel Jaak Tarien, Director of the NATO CCDCOE said: “Our long-term cooperation with Siemens in training the cyber experts to protect critical infrastructure in general and power grids in particular has been a major asset for the NATO CCDCOE technical cyber defence exercises. With the aim to reinforce the interaction amongst different cyber defence stakeholders, to deepen co-operation and exchange of best practices, this agreement takes our cooperation to a new level. Our societies rely on strong and resilient critical infrastructure. Accordingly, there is a real value in our partnership to advance cyber security together with the key industry partners like Siemens Smart Infrastructure.”

This press release and a picture are available at
https://sie.ag/2CHJEsP

For further information on Siemens Smart Infrastructure, please see here:
www.siemens.com/smartinfrastructure

For more information on NATO CCDCOE, please see here: www.ccdcoe.org

Contact for journalists

Siemens AG
Eva-Maria Baumann
Phone: +49 9131 17 36620; E-mail: eva-maria.baumann@siemens.com

NATO CCDCOE
Karola Mänd
Phone: +372 717 6804; E-mail: media@ccdcoe.org
Twitter @ccdcoe

Follow us on Twitter: www.twitter.com/siemens_press

Siemens Smart Infrastructure (SI) is shaping the market for intelligent, adaptive infrastructure for today and the future. It addresses the pressing challenges of urbanization and climate change by connecting energy systems, buildings and industries. SI provides customers with a comprehensive end-to-end portfolio from a single source – with products, systems, solutions and services from the point of power generation all the way to consumption. With an increasingly digitalized ecosystem, it helps customers thrive and communities progress while contributing toward protecting the planet. SI creates environments that care. Siemens Smart Infrastructure has its global headquarters in Zug, Switzerland, and has around 72,000 employees worldwide.

Siemens AG (Berlin and Munich) is a global technology powerhouse that has stood for engineering excellence, innovation, quality, reliability and internationality for more than 170 years. The company is active around the globe, focusing on the areas of intelligent infrastructure for buildings and distributed energy systems, and automation and digitalization in the process and manufacturing industries. Through the separately managed companies Siemens Energy, the global energy business of Siemens, and Siemens Mobility, a leading supplier of smart mobility solutions for rail and road transport, Siemens is shaping the energy systems of today and tomorrow as well as the world market for passenger and freight services. Due to its majority stakes in the publicly listed companies Siemens Healthineers AG and Siemens Gamesa Renewable Energy (as part of Siemens Energy), Siemens is also a world-leading supplier of medical technology and digital healthcare services as well as environmentally friendly solutions for onshore and offshore wind power generation. In fiscal 2019, which ended on September 30, 2019, Siemens generated revenue of €86.8 billion and net income of €5.6 billion. At the end of September 2019, the company had around 385,000 employees worldwide. Further information is available on the Internet www.siemens.com.

The **CCDCOE** is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 25 nations providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law.
The Centre is staffed and financed by its member nations, currently Austria, Belgium, Bulgaria, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Spain, Sweden, Turkey, the United Kingdom and the United States. Canada, Japan, Croatia, Australia, Luxembourg, Ireland, Montenegro, Slovenia, Switzerland and South Korea are also on the path of joining the Centre.

Siemens AG
Werner-von-Siemens-Straße 1
80333 Munich
Germany

NATO CCDCOE
Filtri tee 12
10132 Tallinn
Estonia