POWER PLAY

Sanjay Chhillar, Dale Geach and Chaitanya Bisale

examine electrical grid modernisation and emerging cyber risks

Traditional grids involving electromechanical technologies to manage predictable and unidirectional flow of electricity from big power plants to consumers have been reliable for many decades with investment in resilience focused towards large items of plant. Today, with power flows becoming less predictable in the grid, electricity utilities are now recognising the strong need for, and huge benefits of, modernising and digitising their operations. Leveraging industrial Ethernet and IP-based communication and international standards for substation automation, such as IEC 61850, are delivering benefits and enabling a range of new opportunities in support of: real time situational awareness of the grid state; load prediction and shift; rapid fault isolation and recovery; integration of renewables and distributed energy resources (DER); achieving net zero carbon emissions targets; reducing employee health and safety risks and enabling remote maintenance and monitoring capabilities to name just a few. The decentralised model enabled by smart grid technologies provides greater flexibility in the event of disruptions as well as potentially reducing the time needed for recovery, as it might be possible to localise disruptions.

However, grid modernisation also exposes it to greater cyber risks due to increased connectivity and inherent vulnerabilities in legacy systems. It has become vital and urgent to address cybersecurity in smart grid design and within legacy systems while the grids are being modernised.

HIGHLIGHTING VULNERABILITIES

Recent exposures and attacks on grids and industrial networks around the world have highlighted the vulnerabilities that can be exploited by bad actors, including nation states and cyber criminals. Intelligence agencies and governments in the USA, UK, EU and elsewhere have identified cybersecurity of their critical national infrastructure (CNI) as one of the top threats to their national, social and economic security. In fact, the EU was concerned enough to introduce the Network and Information Security (NIS) Directive and, in a move to protect CNI, President Trump signed an executive order banning American grid operators from buying and installing electrical equipment manufactured outside the US.

Though the newer industrial control systems (ICS) and operational technology (OT) systems that are used to monitor and control electricity grids and micro-grids as well as industrial processes can be securely designed and hardened, legacy ICS/OT will still have inherent security issues, such as the use of insecure protocols and the inability to enable secure passwords, which create greater cybersecurity challenges.

Due to the increase in adversary capabilities, the critical role of grid infrastructure to nations and the potential for inherent vulnerabilities in ICS/OT systems, electricity grids make attractive targets for bad actors, including nation states, terrorists and cyber criminals. Depending on bad actors' motives, cyber attacks on CNI could be used for geopolitical advantage by nation states to disrupt or destroy power supplies or for ransom by cybercriminals. Unauthorised access to grids and industrial networks can result in widespread outages, creating loss of productivity and revenue, health and safety risks and impact on society due to disrupted transportation, gas, water and other essential services.

In recent cyber attacks, bad actors have demonstrated their capabilities and continued willingness to conduct malicious adventures against CNI. A few examples include STUXNET cyber attack on a nuclear facility in Iran causing equipment damage and BlackEnergy (2015) and Industroyer/Crash Override (2016) cyber attacks on Ukrainian utilities causing power outages. In 2017, WannaCry ransomware attack disrupted services/operations globally across multiple sectors including Health and utilities; and NotPetya, a ransomware attack that prevented Maersk from locating and routing shipments, resulting in a reported loss of up to €300-million, also hit many local utilities. In

MAINTAINING CYBER RESILIENCE ACROSS ELECTRICITY GRIDS IS A MAJOR CHALLENGE

2018, TRITON/TRISIS, allegedly the first malware specifically designed to attack safety systems, was reported to have hit industrial plants in the Middle East. A ransomware attack on a US natural gas company in 2020 caused a pipeline to shut for two days.

In most cases, unless ICS/OT systems are directly connected to the internet, which is possible and can be discovered using the Shodan online search tool, bad actors usually gain initial access to a targeted organisation's ICS/OT system via exposed IT systems, or by exploiting a supplier's network. In many cases, utilities and other industrial organisations don't have the capabilities or expertise in "real-time visibility" of their ICS/OT networks to proactively identify vulnerabilities or detect malicious activities and prevent incidents. For example, in the case of the cyber attack on the Ukrainian utilities in 2015, attackers used spear-phishing techniques to send a malicious Word document via email and compromised an employees' computer before pivoting to their ICS/OT networks. Attackers used compromised credentials and remained in the networks for six months, without getting caught, before causing the outage in December 2015. The attack demonstrated the attackers' sophisticated capabilities and exposed the utilities' inadequate preparations to detect and prevent sophisticated cyber attacks. As a best practice, ICS/OT networks should be segmented from business/office IT networks but in the example above, attackers were able to exploit improper segmentation, design flaws and inadequate security controls to pivot to and gain foothold in their ICS/OT network.

Modernisation exposes the grid to greater cyber risks due to increased connectivity

Lack of visibility and monitoring, insecure legacy protocols, unpatched systems, inadequate access controls and improper segmentation plus a shortage of ICS/OT cyber expertise are key challenges for many utilities and other industrial organisations.

Maintaining cyber resilience across electricity grids and CNI ecosystems is a major challenge for governments, owners and operators of essential services. The OT/ICS systems were not originally designed with cybersecurity in mind, so we must live with inherent vulnerabilities in legacy systems for some considerable time to come. Cyber threats are a new reality in today's hyperconnected world, but any panic or fear due to hype must be avoided. With the right strategy; cross sector collaboration; partnerships with governments and intelligence agencies; and board accountability, threats can be adequately addressed and organisations can prepare for and handle any emergency.

For effective cybersecurity measures, international standards and best practices such as IEC 62443, NIS Directive, NERC CIP, NIST CSF, MITRE ATT&CK framework for ICS, *etc*. may be very helpful. In a realistic world, there is nothing even close to 100 percent protection, so organisations need to be pragmatic in their approach. It is important to understand the threat landscape and prioritise mitigations based on risks and impact to critical systems rather than trying to implement everything in one shot. In the ICS/OT world, we must be aware that patching of all systems may not be realistic and segmenting an existing OT network may not be feasible. Therefore, leveraging passive monitoring solutions for gaining visibility into assets, communication flows and detecting anomalies and intrusions may be a powerful value proposition and deliver a better return on investment.

Cybersecurity measures are more than technologies and processes. An effective cybersecurity programme requires board/executive management support and leadership and a security culture across the organisation, built upon proactive risk management and ability to recover in a predictable manner from an attack.

The risk landscape is continuously changing so strategy and plans must evolve and be adjusted to keep pace. The Chief Information Security Officer (CISO)/ Chief Risk Officer (CRO) should be reporting to and periodically updating their boards about cyber risks and their preparedness. Cyber capabilities should be realistically assessed, as well as the organisation's security posture compared with their risk appetite and industry peers. Cyber threats are inevitable and no

Picture credit: Siemens

Risk Management, Governance and Board Oversight	Secure by Design	Continuous Threat Monitoring and Incident Response
☐ Threat modeling and risk assessment	☐ Secure network architecture and hardening	☐ Baseline and continuous threat detection
☐ Board oversight and accountability	☐ Change and configuration management processes	☐ Monitoring for unauthorised changes
☐ Supplier risk management	☐ Updated inventory	☐ Continuous vulnerabilities assessments
☐ Awareness and skills development	☐ Role Based Access Control	☐ Periodic tabletop exercise to test incident response plan
☐ Policies, plans, metrics and reporting	☐ Segmentation between IT and OT network, Transient Systems	☐ Retainer's services agreement with an external incident response partner in the event of an emergency (optional)
	☐ Periodic patching (wherever feasible or as per compliance requirements)	

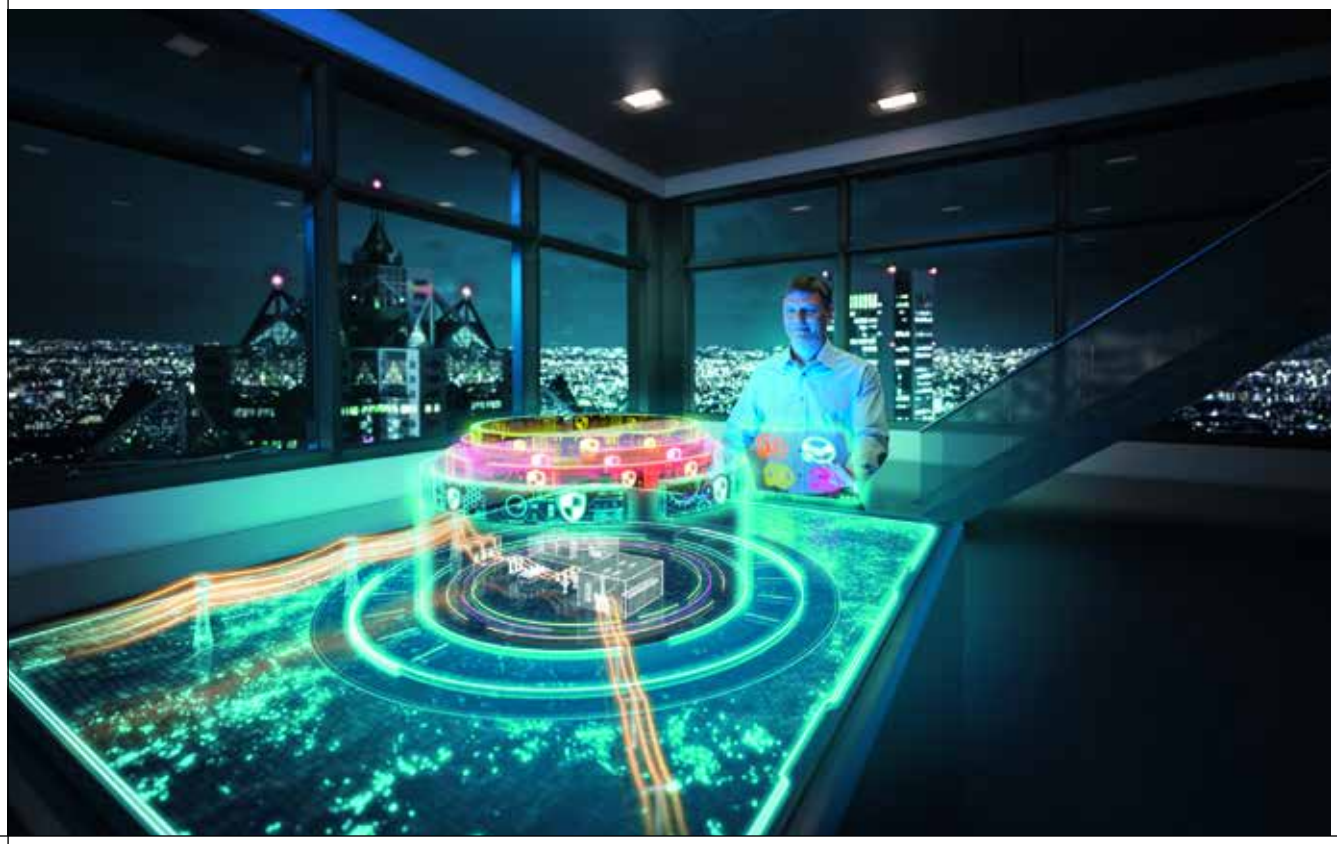
Sanjay Chhillar, Head of OT/ICS Cybersecurity at Siemens UK
Dale Geach, Technology and Innovation Manager at Siemens UK
Chaitanya Bisale, Cyber Security Product Manager and Senior Key Expert at Siemens

matter how robust an organisation's security posture is, it is still susceptible to zero-day and sophisticated attacks. Therefore, in addition to having robust security design and risk management practices, organisations must prepare for emergency situations and always have a tested incident response plan in place and a team of experts trained and ready to handle incidents.

The table above provides a high-level summary of the core pillars and sub-objectives (covers only the key objectives) for establishing a sustainable cybersecurity/cyber resilience programme.

As we transform our traditional grids to modern/smart grids, we will have to deal with hybrid environments containing OT/IOT components that are very advanced and legacy components that are very old and everything in between. Network segmentation may not be easy and patching of all legacy systems will not be realistic, so we must live with inherent security vulnerabilities. To counter cyber threats to grid networks and CNI in general, organisations across all critical sectors and international governments need to partner to secure their CNI without creating an environment of fear and panic. Boards must be held accountable for security of their critical infrastructure and regulatory agencies must empower and incentivise organisations to continuously enhance cyber resilience. Only a secure by design network with continuous threat detection, tested emergency response plan and enterprise risk management with board oversight can defeat adversaries and defend national, social and economic security ●

Electricity grids make attractive targets for bad actors



Picture credit: Siemens