Cyber security

Protecting critical infrastructure in a changing world

SEBASTIAN OBERMEIER, SASCHA STOETER, RAGNAR SCHIERHOLZ, MARKUS BRAENDLE – Twenty years ago, the cyber security of systems and devices used in critical infrastructure such as energy transmission and power production was not an issue. Networks were truly isolated, and engineers expected devices to receive exactly the kind of data for which the devices were designed. No one imagined that it would be possible for an attacker to inject arbitrary data packets into isolated networks or to directly influence the underlying production process. As industrial control systems gradually changed from being isolated or from using proprietary networks, to being highly interconnected using commercial off-the-shelf technologies and open standards, these concerns and the demand for cyber security slowly but steadily grew. By the beginning of the new millennium the importance of cyber security in industrial control systems had become self-evident. But cyber security has long been an important initiative for ABB, having evolved from a research topic to being fully embedded in the company's global organization and in all levels of the product and system life cycle.

Title picture
Cyber security protects all aspects of critical infrastructure.

1 Cyber security safeguards against unauthorized local as well as remote malicious access to control rooms.

Cyber security is an integral part of ABB's products and systems. It is addressed at every phase, from design and development to maintenance and support of the product. Threat modeling and security design reviews, security training of software developers, as well as in-house and external security testing as part of quality assurance processes, are examples of the numerous steps ABB is taking to increase the reliability and security of its solutions.

Cyber security embedded in the product life cycle

ABB was, for instance, the first SCADA (Supervisory Control and Data Acquisition) vendor to partner with the US Department of Energy's Office of Electricity Delivery and Energy Reliability through its National SCADA Test Bed program at Idaho National Labs. Work began in 2003 to perform cyber security assessments for ABB's Network Manager SCADA/energy management system (EMS) product. Results from that initiative led to many security upgrades and improvements.

One very important initiative within ABB is the Device Security Assurance Center (DSAC). The objective of the DSAC is to provide independent and continuous protocol-stack robustness and vulnerability assessments of embedded devices as part of the development process. The test center utilizes a suite of state-of-the-art open-source, commercial and proprietary solutions, and the testing scope includes device profiling, known vulnerability scanning, and protocol fuzzing. The DSAC currently performs more than 100 tests per year, helping ABB to continuously improve the robustness and resilience of embedded devices.

ABB has identified cyber security as a strategic initiative and therefore established a formal cyber security organization.

Examples of the improvement of cyber security capabilities include the recent releases of ABB's Extended Automation System 800xA, which has a substantial set of security capabilities to support the secure operation of process automation solutions. These capabilities include support for third-party malware (ie, malicious software) protection solutions (antivirus as well as application whitelisting), granular access control (flexible account management as well as granular access permissions and role-based access control), and secure communication using IPsec (ie, Internet Protocol security) → 1. However, the security considerations are not limited to system capabilities, as they also include support during the product life cycle; eg, providing validation of third-party security updates and a firm process for vulnerability handling.

Another example of the company's efforts to improve cyber security is the RTU560, widely used as a classical, substation-automation, smart-grid and feeder RTU (remote terminal unit), or as a gateway. Its security capabilities address the market needs induced by NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection [1]) compliance and address industry standards such as IEC 62351 and IEEE 1686. The capabilities include granular access control (including role-based access control), logging and reporting of security events (locally or to an available Security Information and Event Manager, or SIEM) and support for secure tunneling of communications through an integrated IPsec VPN client.

The product life cycle is of course not limited to product capabilities and the support of products, but it also encompasses the secure delivery of projects. An excellent example in which cyber security was

2 Safe remote access through ABB Service Desk

One of the big challenges in oil and gas production is that remaining reservoirs are increasingly difficult to exploit. Thus more advanced technology and expertise are required for production. However, it is prohibitively expensive to maintain all the necessary expertise on-site at remote locations such as offshore production facilities. At the Ormen Lange gas field and the Draugen offshore rig, ABB and Norske Shell have collaborated to establish a Service Environment™ that enables remote access to the sites, thereby taking advantage of expert knowledge while saving on travel costs. Cyber security concerns are of course paramount in all remote access scenarios and thus a solid security architecture was developed. One key success factor in this endeavor was the integration of Shell's own Process Control Domain security concept with ABB's security technology and services. Another was the early implementation of cyber security, ie, during the plant design and construction.

ABB performs and assists in the system operations to match Shell information security policy. Remote system monitoring is integrated with the site inventory so historical data can also be considered. Secure client server management, loop tuning, process optimization and preventive maintenance are all part of ABB's remote capabilities and responsibilities. The Service Desk, which is both manned and automated, is the heart of information collection. Here the cases are recorded and dispatched to the correct team within a defined timeframe. The team leader assigns each case to a specialist, who could be any one of a variety of ABB experts all over the world. Important aspects of Service Desk functionality include configuration, field alert and overall change management – all facilitated remotely.

The scope of these services is not limited to new projects. While the Ormen Lange project provided the opportunity to embed cyber security at the project design phase, the Draugen platform already existed before remote access and ABB's cyber security services were added.

integrated throughout the project life cycle is the development of Norske Shell's Ormen Lange gas field and Draugen offshore platform ➔ 2.

Cyber security embedded in the organization

ABB has identified cyber security as a strategic initiative and therefore established a formal cyber security organization led by the ABB Group Cyber Security Council. The council ensures a continuous strengthening of ABB's operational readiness and actively works to maintain the internal cyber security awareness and expertise throughout the company. The ABB cyber security organization comprises experts from various backgrounds including R&D, IS infrastructure, legal and communications in order to properly address the multifaceted challenges of cyber security. In addition, ABB complements and enhances its internal expertise and scope not only through collaborations with customers and government organizations but also through a strategic partnership with Industrial Defender, a company dedicated to ensuring the availability, reliability and security of critical infrastructure.

The future of industrial-control-system cyber security is comparable to the enterprise IT domain, where security has become a part of daily life with automated software updates, security patches and antivirus updates in order to thwart a growing number of threats. ABB is prepared to constantly enhance the security features of its offerings through technological advances and organizational readiness so it can continue to provide products and services that meet the security needs of its customers' critical infrastructure.

Collaboration across industry

To establish a high industry-wide cyber security level, standards are required. Standardization initiatives by IEEE, IEC and ISA were established with ABB playing an active role in defining and implementing cyber security standards for power and industrial control systems ➔ 3. The main objective of these initiatives is to establish and maintain the necessary levels of cyber security, while preserving the availability and functional interoperability of systems. In addition, ABB has participated in EU projects, eg, ESCoRTS and VIKING , and continues to invest in initiatives that bring together all stakeholders, including private companies, governments, academia and other research organizations.

ESCoRTS

ESCoRTS[2] was a joint endeavor among EU process industries, utilities, leading manufacturers of control equipment, and research institutes to foster progress toward the cyber security of control and communication equipment in Europe. It

Extended Automation System 800xA has a substantial set of security capabilities to support the secure operation of process automation solutions.

Footnotes

1 See www.nerc.com

2 See www.escortsproject.eu

3 ISA99 / IEC 62443

ISA99 is the Industrial Automation and Control System (IACS) Security Committee of the International Society for Automation (ISA), which is developing a multipart series of standards and technical reports*. Work products from the ISA99 committee are also submitted to the International Electrotechnical Commission (IEC) as standards and specifications in the IEC 62443 series. In order to avoid confusion and to demonstrate the alignment, the ISA will relabel the standard series from ISA99 to ISA 62443.

The standards and technical reports are organized into four general categories that identify the primary target audience for each group:
- General: includes general information such as concepts, models and terminology.
- Asset Owner: addresses various aspects of creating and maintaining an effective IACS security program for asset owners and operators as well as the necessary organizational support from suppliers of products and services.
- System Integrator: provides technical system design guidance and imposes security requirements on the integration of control systems by using a zone and conduit design model.
- Component Provider: describes the specific product development and technical requirements of control system products.

ABB has verified the applicability of IEC 62443 in the ESCoRTS EU project and supports the work of the committee by active participation and contribution.

* ISA99, Industrial Automation and Control Systems Security, www.isa.org/isa99

4 Cyber security is an essential component in today's power grids, enabling a reliable supply of power by protecting against attacks.

Collaboration with reputable universities is also a key element of ABB's research strategy.

addressed the need for standardization and developed a dedicated roadmap for standardization and research directions.

ESCoRTS has been a leading force for:
- Disseminating best practice on security of SCADA systems
- Hastening and ensuring convergence of SCADA standardization processes worldwide
- Paving the way to establishing cyber security testing facilities in Europe

The ESCoRTS project included a field evaluation of the available cyber security standards. ABB and the Italian energy utility ENEL jointly performed a cyber security assessment of an ENEL power generation plant that was redesigned in 2003. The assessment was based on the current status of the IEC 62443 standard at the time. The results included a positive assessment of the standard's applicability and utility in securing an industrial control system and also demonstrated that, with the commitment of and collaboration among the vendor, system integrator and asset owner/operator, an industrial control system's security posture can be improved within cost and resource constraints typically applicable to existing plants.

VIKING

VIKING[3] was a cyber security project that investigated vulnerabilities in state-of-the-art SCADA systems used for the supervision and control of electrical grids ➔ 4. The VIKING consortium was led by ABB and consisted of members from utilities, industry and academia. The objectives of VIKING were to:
- Develop calculation models for SCADA system security
- Estimate the societal costs and consequences of blackouts generated by failing SCADA systems
- Propose mitigation strategies for the vulnerabilities identified

These objectives were fulfilled by developing a security analysis language and a virtual society model, and by investigating vulnerabilities in power applications and proposing countermeasures for these vul-

Footnote
3 See www.vikingproject.eu

5 Research case study: Advanced Anomaly Detection and Security Configuration (ANADS)

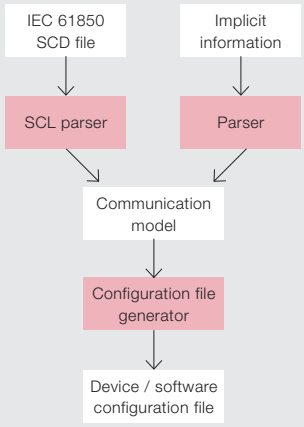

ABB is actively researching new ways of identifying intruders. The following example from its research labs shows what the future of cyber security in industrial control systems may look like.

In an IEC 61850 based substation automation system, intelligent electronic devices (IEDs) are sending out GOOSE (generic object-oriented substation events) messages at a certain frequency (eg, 200 Hz) to other IEDs. These GOOSE messages are meant to inform the receiving IEDs that the sender is active and ready to take part in providing particular logical functionality (eg, an interlocking function or a protection function). In this setup the substation automation system should ensure that the GOOSE messages reach the correct recipient within a given timeframe. Failure to deliver the GOOSE message to the correct recipient at the correct time may result in the failure of the particular function(s). Although these types of anomalies (missing or delayed sampling messages) will be passed on to the control center, the system lacks information about the primary cause of the anomaly, which may be a security incident.

ABB has developed a new approach for anomaly detection that takes the expected traffic into account and can issue an alert if traffic is not sent. For this, the substation configuration is enriched with implicit information that allows the generation of a detailed communication model as illustrated above. This model is then analyzed, and appropriate rules for configuring a firewall or an intrusion detection system are automatically generated. This allows for comprehensive monitoring of the complete data traffic in order to detect intruders at an early stage.

nerabilities. The results have been summarized in a number of story boards where possible cyber attacks on SCADA systems are described, and they include the likelihood of success for these attacks as well as their social and economic impact. Also included are possible mitigation methods and their potential to improve security.

An ongoing research topic

Collaboration with reputable universities is also a key element of ABB's research strategy. In 2006, eg, ABB began a three-year research project, "Threat Modelling," in cooperation with the University of St. Gallen and the Swiss Commission for Technology and Innovation (CTI). In this project, a methodology for threat modeling of embedded devices was successfully developed. The methodology allows for assessment and documentation of the actual security of the developed system throughout product development [1, 2]. On several occasions this methodology has been used within ABB to conduct security assessments as part of the development process.

> ABB played an active role in defining and implementing cyber security standards for power and industrial control systems.

ABB is committed to technology leadership and significantly invests in internal research as well – looking at, for instance, new innovative ways to protect industrial control systems [3,4]. ABB has and continues to address current and future needs by developing new approaches for cyber security in industrial control system. Examples include novel approaches for anomaly detection → 5 and the design of authentication architectures that allow the use of a single password per user throughout a complete plant.

For more information about cyber security at ABB, please visit www.abb.com/cybersecurity or email cybersecurity@ch.abb.com.

Sebastian Obermeier
Sascha Stoeter
ABB Corporate Research,
Industrial Software Systems
Baden-Dättwil, Switzerland
sebastian.obermeier@ch.abb.com
sascha.stoeter@ch.abb.com

Ragnar Schierholz
Markus Braendle
ABB Group Cyber Security Council
Zurich, Switzerland
ragnar.schierholz@ch.abb.com
markus.braendle@ch.abb.com

References

[1] Köster, F., Nguyen, H. Q., Klaas, M., Brändle, M., Obermeier, S., Brenner, W., Naedele, M. (2009, April). Information security assessments for embedded systems development: An evaluation of methods. 8th Annual Security Conference, Las Vegas, United States.
[2] Köster, F., Nguyen, H. Q., Brändle, M., Obermeier, S., Klaas, M., Brenner, W. (2009, April). Collaboration in security assessments for critical infrastructures. 4th International CRIS Conference on Critical Infrastructures, Linköping, Sweden.
[3] Brändle, M., Koch, T. E., Naedele, M., Vahldieck, R. Strictly no admittance: Keeping an eye on IT security in the plant. *ABB Review 1/2008*, 71–75.
[4] Naedele, M., Dzung, D., Stanimirov, M. (2001, September). Network security for substation automation systems. Safecomp 2001, Budapest, Hungary.