TECHNOLOGY INDEPENDENT SECURITY REQUIREMENTS FOR SUCCESSFUL PROCUREMENT OF RTUS TO GET ACCEPTABLE RISK LEVELS AT DSOS

Maarten HOEVE
ENCS – The Netherlands
Maarten.Hoeve@encs.eu

Carlos MONTES PORTELA
Enexis – The Netherlands
Carlos.Montes.Portela@enexis.nl

Bart LUIJKX
Liander – The Netherlands
Bart.Luijkx@alliander.com

ABSTRACT

Security is becoming an important topic in distribution automation systems. Connecting these systems to enterprise IT networks for data sharing, has made them vulnerable to hackers from around the internet, as a recent incident in Ukraine has shown.

To make current and future distribution automation systems sufficiently secure against cyber-attacks, it is important to have good security requirements for procurement. Equipment is often procured in tenders, in which the requirements for security must be written down at the start. Mistakes in the requirements can lead to high costs or mismatches with the functionality actually needed. To address this problem, several grid operators have worked together within the community of the European Network for Cyber-Security (ENCS) to develop a harmonized set of security requirements for procuring distribution automation RTUs. This paper discusses how the requirements were developed, and what the benefits were of harmonizing them between grid operators.

The paper also discusses the use of the requirements in a tender for RTUs conducted by Dutch DSO Enexis in 2015. Enexis found that by using the requirements they obtained RTUs with much better security compared to tenders in the years before, while the selected RTUs selected were not significantly more expensive.

INTRODUCTION

With distribution automation, things that previously had to be done on-site in a substation, can now be done remotely in much less time. This includes sabotage. The connection of distribution automation networks to office networks for data sharing, changes the cyber security risks that distributions system operators (DSOs) face. An incident in Ukraine in December 2015 [1], has shown that by attacking the SCADA system hackers can create a black-out from anywhere on the internet.

Distribution system operators (DSOs) see these risks, and are looking for measures to mitigate them. Most measures are rightly aimed at protecting legacy systems, not designed to withstand cyber-attacks. Network architectures are changed to put critical systems behind several firewalls. SCADA operators and engineers are trained to be aware of the cyber-security risks.

But DSOs also need to address these risks when procuring new equipment. New equipment is bought every year. How do you make sure this new equipment is secure? And that it stays secure over its life-cycle? When buying new equipment, DSO need to follow strict rules in procurement processes. Most equipment is procured in tenders, in which requirements must be written down formally at the start. Asking for too much security will exclude vendors from the tender, and lead to high initial costs or equipment with inferior non-security functionality. Asking for too little security leads to high costs when structural vulnerabilities found later, during testing or operations.

Setting the right security requirements in a tender is therefore important in cost-effectively securing future distribution automation systems. Based on a project to develop security requirements for distribution automation RTUs, we want to show here that setting up good requirements is possible, and their effectiveness increases when they are harmonized between DSOs.

PROCUREMENT REQUIREMENTS

Setting security requirements during procurement processes, including tenders, is a common recommendation in many organizational security standards. The ISO 27002 standard [2] for instance has a control on information security requirements analysis and specification, which specifies that security requirements should be included in the requirements for new information systems. The IEC 62443 (or ISA 99) standard [3] also has a control on defining and testing security functions and capabilities of new components.

In the past, most DSOs have been developing their own set of security requirements. There are however benefits in harmonizing security requirements, so that different DSOs use the same, or largely the same set. One benefit is that harmonization reduces the cost of developing the requirements by sharing it between the DSOs. Another benefit is that by developing the requirements in advance, they are ready when they are needed. In this way, security concerns do not delay the tender process, which is often run under time pressure. This benefit helps to get security established in the standard way of working of DSOs.

The biggest benefit however comes from presenting a common set of requirements to manufacturers. In this way, DSOs can provide a clear signal to manufacturers about what security measures they want to have on a device.

Manufacturers can then implement these once for all DSO, and distribute the implementation costs over different DSOs.

AVAILABLE STANDARDS

With these benefits, it seems logical to ask if a set of security requirements for procurement is not already available. In other domains, such sets have indeed been available for a long time. The US government published the Orange Book [4] with their requirements for military systems already in the 1980s. These requirements have since evolved into the Common Criteria standard [5], which provides a toolkit for setting security requirements, and evaluating components against them.

Attempts to apply Common Criteria to the smart grid components have however failed up to now. In Germany, a Common Criteria protection profile was developed that specifies the security requirements for smart meter gateways. This approach to security is however thought to have raised the cost of the smart meter significantly, and delayed their roll-out. The Common Criteria prescribe a formal approach to security, which requires buyers and vendors to have a background in abstract security concepts. They require manufacturers to do a lot of paperwork. And, Common Criteria evaluation results in a certificate that is only valid for one specific version and configuration of a component. Any change to the component requires complete recertification. So, even though Common Criteria provide a good way to think about component security, it is difficult to apply them to distribution automation components.

The German Bundesverband der Energie- und Wasserwirtschaf (BDEW), has developed a whitepaper [6] with a more practical approach. This whitepaper includes security requirements based on ISO 27002, and can be used as an attachment to tender documents. The requirements are however on system level. They are written generically to apply to different systems. So, they cannot be used word for word for procuring components such as RTUs.

Component-level requirements are being developed as part of the IEC 62443 standard. Part 4-2 of this standard [7], which will contain the requirements, is however still in draft. It is too early to use it for procurement.

The US Department of Homeland Security has also released a document with procurement language [8]. The requirements in the section on RTUS however mostly concern the documentation that manufacturers should provide. It does not specify what security measures should be taken on a technical level.

So, the existing standards do not offer a set of requirements that can be directly used in a tender request for proposals document for RTUs. To fill this gap, several DSOs decided to join forces to develop a set of their own, based on the best practices from the existing standards.

DEVELOPING THE REQUIREMENTS

To develop the requirements, the DSOs decided to work within the community of the European Network for Cyber-Security (ENCS). ENCS is a non-profit company founded in 2012 to improve the security of DSOs. It is a cooperative, that currently has ten European DSOs of various countries. It provided a natural platform for collaboration in a non-commercial setting. A project was started, funded by the ENCS members Alliander, EDP, Enexis, E.ON, EVN, and Stedin, in which experts from ENCS worked with security officers from the involved DSOs to write a set of security requirements for procuring RTUs.

The main challenge in the project was balancing risk reduction with costs. RTUs play a critical role in monitoring and controlling the electricity grid. Security officers at DSOs want to put strong security measures on the RTUs to reduce the risk of compromise. But if the required security measures are too far from those implemented on RTUs in the market, there will be problems in the tender. Few manufacturers will be willing to implement the required measures, so that there is less competition. Those that will implement them, will ask a price premium for the implementation. Ideally, the requirements reduce the risks to an acceptable level without increasing the costs of the RTUs much.

To find a set of requirements that meets this goal, two steps were taken. On the one hand, a risk assessment was performed on distribution automation systems, based on

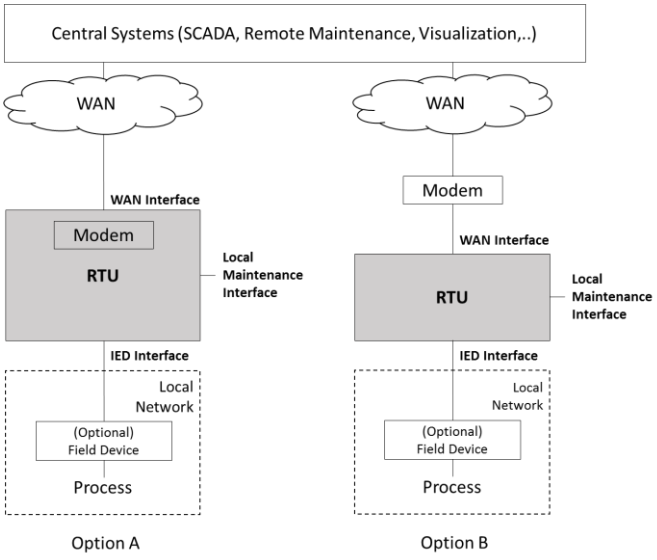

Figure 1: Reference architecture for distribution automation used in the development of the requirements.

the experience at the participating DSOs. The risk assessment allowed the effect of security measures to be estimated. On the other hand, a market survey was performed to determine which measures were already implemented on existing RTUs, and which measures were on the manufacturer's roadmaps. Based on these two activities a set of requirements was selected that counters the major risks, and could be fulfilled by sufficiently many manufacturers.

The requirements were written with the overall system architecture in mind. Some risks are more efficiently mitigated at in the system's architecture. For instance, to prevent attackers that break into a substation and open the RTU from getting encryption keys would require specially secured chips. Most available RTUs do not have these. To mitigate this risk, it is more efficient to take an architectural measure, and use a different key for each RTU. If in this case attackers would obtain key from one RTU, the impact would be low, because they cannot use it to compromise other RTUs. A reference architecture was developed to take such architectural measures into account (see Figure 1). The component level measures for RTUs were chosen to complement the system level measures.

REQUIREMENTS STRUCTURE

The requirements developed cover all aspects of RTU security. Figure 2 gives the different requirement categories included.

- RTU Security Requirements
  - Future-Proof Design
  - Cryptographic Algorithms and Protocols
  - Communication Security
  - System Hardening
  - Resilience
- Support for Secure Operation
  - Access Control
  - Logging
- Product Lifecycle and Governance
- Assurance

Figure 2: Categories includes within the distribution automation RTU security requirements.

The category with RTU security requirements contains the measures to protect the RTU itself against compromise. It contains functional requirements on the use of encryption for communication security, and quality requirements on the use of modern cryptographic algorithms, the level of system hardening, and the resilience to rough handling, both physically and over the network. To ensure that the RTU can be kept secure through its entire lifetime, future-proof design requirements are included that specify that it should be possible to update all security features remotely, and that there is enough memory and processing power for such updates.

The category on support for secure operation contains requirements for functionality that the RTU should have to keep the distribution automation system as a whole secure. This category includes requirements on supporting centralized access control, so that unique accounts can be created for each user instead of each role. It also includes requirements for logging security events, and exporting the logs to a central log management server. Such functionality allows for better security monitoring of the distribution automation system.

A separate category, product lifecycle and governance, is dedicated to what a manufacturer should do to secure their development and manufacturing processes. Manufacturers handle confidential information about the RTUs: detailed design documents, the source code of the firmware, initial keys provisioned to the RTU, and reports on vulnerabilities discovered. So, the manufacturer should set up a good security management system to protect this information.

Moreover, manufacturers should set up good processes for handling vulnerabilities. To keep RTUs secure in the long run, vulnerabilities need to be patched as quickly as possible after they have been discovered. So, manufacturers must have efficient processes to learn about vulnerabilities, and create patches for their RTUs. The project showed that manufacturers use more and more off-the-shelf libraries in the RTU firmware. For instance, many use the OpenSSL library [9] for cryptographically secure connections. Vulnerabilities that affect such libraries, such as Heartblead [10], will hence also affect many RTUs. The details of exploiting the vulnerabilities are often available online, because they are encountered in many websites and enterprise IT systems. Hackers can exploit them without any specific knowledge about RTUs. Manufacturers must therefore actively track vulnerabilities in third party libraries, by following mailing lists and security notifications.

Finally, there is a section on assurance. It contains different measures manufacturers must take to assure DSOs that the requirements are implemented correctly: security testing, providing documentation on how security is implemented, and following secure development processes.

To allow for innovation, the requirements are formulated in a technology independent way. For instance, the requirement on communication integrity in Figure 3 does not specify which communication protocol must be used. The requirement can be fulfilled using VPN technology (IPSec or OpenVPN), using TLS, or using application layer protocol measures. In this respect, it is different from communication protocol level standards, such as IEC 62351 [11] (which specifies the use of TLS for IEC 104

SCR.02 Message Integrity	
Minimum Requirements	1. The RTU SHALL verify the integrity of application layer messages received on the WAN and Local Maintenance interface using a message authentication algorithm allowed by SPR.01. 1. If the RTU detects that a message has been modified or if it cannot verify the integrity of the message, it SHALL reject or drop the message. 2. The RTU SHALL allow parties it communicates with on the WAN or Local Maintenance Interface to verify the integrity of application layer messages it sends by using a message authentication algorithm allowed by SPR.01.
Awarding Criteria	3. The RTU SHOULD verify the cryptographic integrity of messages received on the IED interface. 4. The RTU SHALL allow parties it communicates with on the IED Interface to verify the integrity of application layer messages it sends by using a message authentication algorithm allowed by SPR.01.
Recommended Assurance	• Analysis of the design documentation provided by the Vendor. • Functional tests can be used to verify that the RTU supports the required functionality. • Carrying out a penetration test can be used to determine if the RTU verifies message integrity under all conditions.

Figure 3: The requirements for protecting the integrity of communication.

traffic).

Technology independent requirements are used to give manufacturers freedom in the implementation. They know their own platform best, and can take the best decision on how to implement security measures. Moreover, in this way the requirements allow for new developments, such as the use of communication protocols such as JSON and SOAP that originate from the internet.

TESTING

Requirements only work well if they are tested. Only by having structural testing and auditing of all requirements, can a DSO be sure that they are implemented. Testing is therefore a control in all organizational standards (section [ref ISO 27002] control 14.2.8, [ref IEC 62443-2-1] control 4.3.4.3.1). Therefore, technical requirement categories contain guidance on how to test each requirement. See the recommended assurance part in Figure 3. The assurance category also contains requirements to the vendor about what tests should be performed.

Enforcing the assurance requirements is however proving difficult. The requirements follow the approach recommended in most standards: the manufacturer should perform the functional tests., and the purchaser then has an independent party review the test method and results, and possibly perform an independent penetration test ([5], [3] section A.3.4.3.5.3). But in practice, it is difficult to get good functional test results from the manufacturers. The responsibility for verifying the requirements then falls completely with the third party that does the penetration test. Most penetration tests are however time-boxed and focus on the most critical vulnerabilities. Creating a more structured test process would improve the requirements assurance process significantly. ENCS will work on this activity with its member DSOs and hopefully achieve a set of test cases, harmonized in the same way as the security requirements.

EXAMPLE PROJECTS

The requirements have been used in several tenders. One was a tender for new medium to low voltage distribution transformer station RTUs, conducted by Dutch DSO Enexis in 2015. The tender concerned the strategic medium to low voltage transformer substation, about 10% of the total medium to low voltage substations of Enexis.

Although manufacturers were surprised by the stricter, and extensive security requirements, a sufficient number could meet the requirements to have a competitive tender. Enexis has had the impression that the stricter security requirements did not lead to a much higher price.

What surprised Enexis team evaluating the offers on security, was that many manufacturers could implement advanced security features in a short time. Enexis had run a tender for similar RTUs a year before, and had received proposals from many of the same manufacturers. In the time between both tenders, many manufacturers were however able to implement features such as firmware signing, and centralized authentication using RADIUS. Manufacturers could implement such features quickly, because most RTUs were Linux-based, and could use open source software libraries and tools.

Besides in getting stronger security measures implemented, the requirements also helped in ensuring a more structured evaluation of the manufacturer proposals. They provided a set of objective criteria to score the manufacturers against.

CONCLUSION

With the ongoing development of the smart grid, many new IT components will be added in the grids in the coming years. The security requirements we set to these components during procurement will determine if the smart grid we have in five or ten years is secure or not. By harmonizing these requirements, DSOs can give a clear signal to manufacturers that security is a priority.

The project on distribution automation RTUs run by ENCS members has shown that the harmonized approach works in practice. The same approach to security requirements has also been successfully been applied for Smart Meters, in a project for Oesterreichs Energie [12], and to electric vehicle charging poles in a project for ElaadNL [13]. By consistently applying the approach throughout the smart grid, DSOs can without large extra costs make a large step forward in security.

REFERENCES

[1] R.M. Lee, M.J. Assante, and T. Conway, 2016. "Analysis of the Cyber Attack on the Ukrainian Power Grid - Defense Use Case." *SANS and E-ISAC report.*

[2] ISO/IEC 27002: *Information technology - Security techniques - Code of practice for information security controls.* International Organization for Standardization, Geneva, Switzerland.

[3] IEC 62443-2-1:2010: *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program.* International Electrotechnical Commission, Geneva, Switzerland.

[4] National Computer Security Center, 1983, *Trusted Computer Evaluation Criteria.*

[5] National Information Assurance Partnership, 2012, *Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model* - Version 3.1 Revision 4.

[6] BDEW Bundesverband der Energie- und Wasserwirtschaft e.V., 2015, *White Paper Requirements for Secure Control and Telecommunication Systems.*

[7] ISA WD 99.04.02, 2011, *Security for industrial automation and control systems – Technical Security Requirements for IACS Components*, Draft 1, Edit 1. International Society for Automation, Research Triangle Park, United States.

[8] Department of Homeland Security, 2009, *Cyber Security Procurement Language for Control Systems*.

[9] OpenSSL Foundation, "OpenSSL Cryptography and SSL/TLS Toolkit", www.openssl.org.

[10] Common Vulnerabilities and Exposures, 2014, *CVE-2014-0160*.

[11] IEC TS 62351-3:2007, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*. International Electrotechnical Commission, Geneva, Switzerland.

[12] European Network for Cyber Security, 2014, *Requirements Catalog - End-to-End Security for Smart Metering.* Oesterreichs Energie, Vienna, Austria.

[13] European Network for Cyber Security, 2016. *EV Charging Systems Security Requirements.* Elaad, Arnhem, The Netherlands.