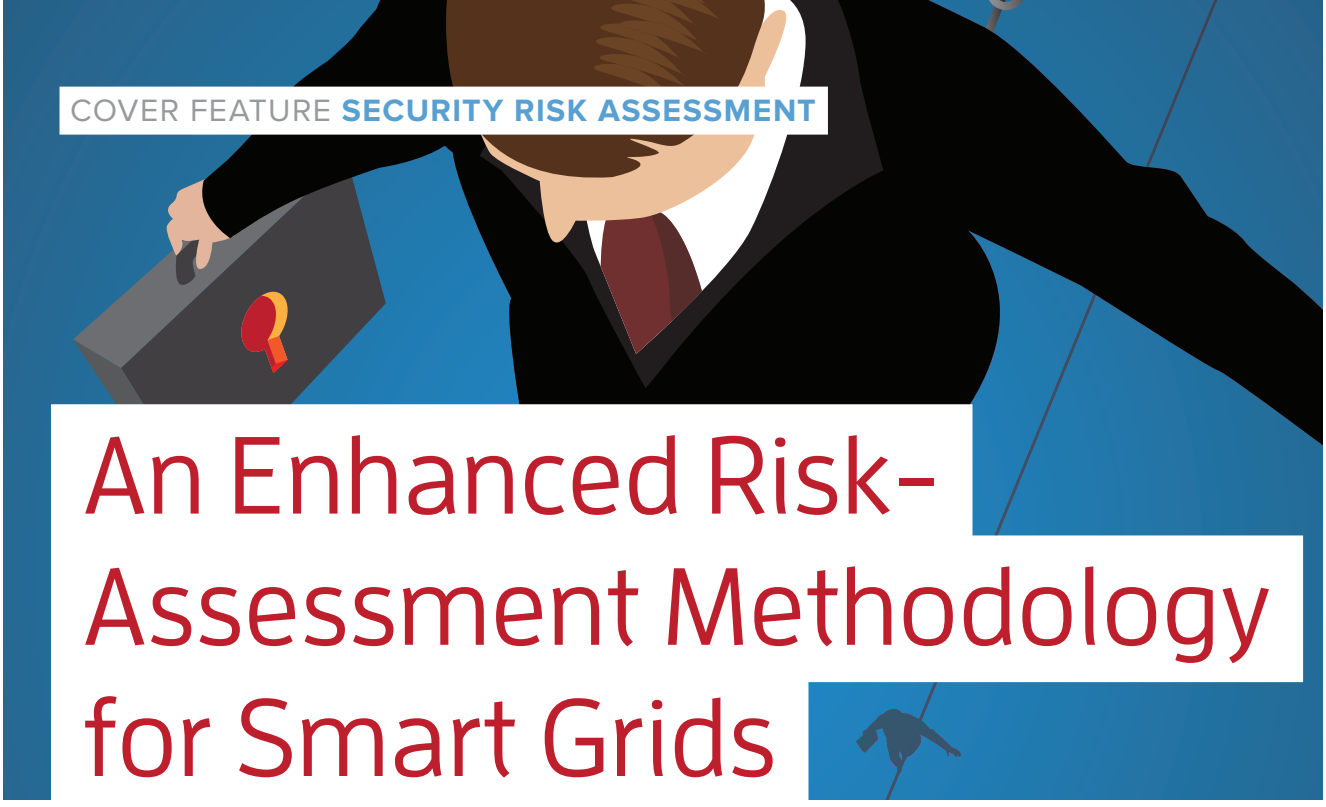


An Enhanced Risk-Assessment Methodology for Smart Grids

Judith E.Y. Rossebø, ABB Norway
Reinder Wolthuis and Frank Fransen, TNO
Gunnar Björkman, KTH Royal Institute of Technology
Nuno Medeiros, EDP Distribuição

Cyberattacks on power grids are pushing threat and risk assessment to another complexity level. As part of its scope, the EU's Security for Smart Electricity Grids (SEGRID) project was tasked with building on existing methods to address the interdependencies characteristic of a smart grid. The authors describe the resulting methodology.

As society's electrical needs evolve, smart power grids must be able to adapt to fluctuating demand from renewable voltage generation and innovations such as electric vehicles. To remain flexible, utilities need to rethink traditional operations, moving from the top-down hierarchical approach in supervisory control and data acquisition (SCADA) systems to a distributed approach with an increased heterogeneous level of observability, controllability, and automation.

In this new environment, distribution system operators (DSOs) will have more support in—and more responsibility for—controlling and influencing power flows in medium- and low-voltage grids. They will see more automatic functions such as self-healing networks, but the cost will likely be a dramatic increase in opportunities for large-scale cyberattacks, which will require deeper risk assessments. Indeed, sophisticated cyberattacks on control systems have already occurred, engineered by highly motivated threat sources and carried out by skilled attackers. For example, in 2010 industrial control systems at the nuclear enrichment facility in Naţanz, Iran, were damaged by Stuxnet malware,[1] and in 2015 a cyberattack on the Ukrainian electricity distribution network caused a regional blackout.[2,3] Given the world's heated political climate, such attacks can be expected to increase.

Smart power grids pose extreme challenges for risk assessment. The threat and vulnerability landscape continues to change unpredictably as new threat

0018-9162/17/$33.00 © 2017 IEEE

sources and attackers emerge with ever more complex and inventive ways of exploiting vulnerabilities. A large-scale smart grid is a system-of-systems involving a conglomerate of stakeholders, each representing their own interests and with different risk perceptions. Added to that mix is attackers' capability and motivation, which greatly influence both the likelihood of cyberattacks and their impact on the infrastructure. Because the grid is essential to critical infrastructure, any structured risk-management approach must include ways to identify, analyze, evaluate, and treat risks, including an assessment of how an attack will impact the infrastructure.

As part of the 7th Framework Programme of the European Community for research, technological development, and demonstration activities (FP7), the Security for Smart Electricity Grids (SEGRID) project is investigating how to enhance the protection of smart grids against cyberattacks. The project, which began in October 2014 and is scheduled to complete at the end of 2017, is a collaboration of industrial and academic partners, including DSOs with practical insights into the strengths and weaknesses of applying risk-assessment methods in the energy sector. One of the project's goals is to evaluate these current methods and further develop enhanced risk-assessment and risk-management approaches tailored for application to smart grids.

To meet that goal, the project team, of which we are members, established a set of requirements to compare existing risk-assessment methods developed for or applied in the energy sector. We then evaluated the candidate assessment methods and proposed a four-step approach to risk assessment that combined aspects of the three highest-scoring methods. We extended the four-step approach with components from these methods and applied the resulting methodology to a set of smart-grid use cases to explore its strengths and weaknesses. From this exploration and experience in practical risk assessment, we identified the need for a fourth method that could provide a risk-management framework. Our enhancements and this framework form the basis of the SEGRID Risk Management Methodology (SRMM), the primary objective of which is to provide DSOs with a structured, in-depth methodology for understanding potential threats and vulnerabilities, managing identified risks, and taking measures to contain and mitigate them.

ENHANCEMENTS IN THE SRMM AIM TO PROVIDE DSOs WITH TOOLS TO ANALYZE RISKS AND LINK THEM TO STAKEHOLDERS' BUSINESS OPERATIONS.

METHODOLOGY FOUNDATIONS

SRMM enhances existing risk-assessment methods in three ways. We used HMG Information Assurance Standard No. 1 (IS1)[4] as a foundation and extended it with the Network Risk Management (NRM) method[5] to include stakeholder interdependencies and risk propagation through value chains so that DSOs could better understand how risks affect stakeholder interests. We further extended this initial enhancement to include a practical approach for assessing societal impact in case of a power outage caused by a cyberattack. Because any power-supply disturbance could critically affect social structure, DSOs must be able to analyze risks in this context. Finally, because those who seek to compromise a smart grid generally are more skilled and driven than the average attacker, SRMM applies an enhanced version of the European Telecommunications Standards Institute's (ETSI's) Threat Vulnerability and Risk Analysis (TVRA) method,[6] which adds an assessment of the attacker's capability and motivation in the risk-estimation stage.

In addition to these enhancements, we included the risk-management framework given in the ISO/IEC 27005: 2011 Information Security Risk Management standard (ISO/IEC 27005).[7]

Feedback from the DSOs who participated in method evaluation was key in identifying the most frequently used risk-assessment methodologies for the energy sector and in recognizing the main gaps to close in completing the complex process of risk assessment. This analysis steered SRMM's design toward principles that would ensure smart-grid protection and to the risk-assessment methods that form the basis for SRMM.

HMG Information Assurance Standard No. 1

IS1 was developed as the UK government's technical risk-assessment methodology. Netbeheer Nederland (netbeheernederland.nl), the Dutch energy-grid operators' association, adapted IS1 for smart metering and other smart-grid use cases by simplifying its underlying methodology and extending its application in multiple-stakeholder environments. The enhanced IS1 includes support for graphical modeling standardized to the interoperability layers of the smart-grid architecture model (SGAM).[8] This modeling provides DSOs with an at-a-glance look at the technical aspects, business functions, and stakeholder interdependencies in a smart-grid use case.

Network Risk Management

NRM was designed to provide insight into stakeholder and system interdependencies, stakeholder responsibilities, and the propagation of risk through the business value chain. DSOs can then see clearly how the cybersecurity risk affects business operations. To make those impacts explicit, SRMM integrates elements from NRM to provide insight into dependencies and responsibilities between systems and stakeholders in a system-of-systems environment. In this way, SRMM furthers the multiple-stakeholder view of a smart grid by clarifying what responsibilities and obligations each stakeholder has to other stakeholders. This enhancement is important because a cyberattack's negative effects can easily spread from one stakeholder domain to another.

ETSI Threat Vulnerability and Risk Analysis

ETSI developed the TVRA method to aid information and communications technology (ICT) standards development by providing a structure for identifying security solutions and justifying their inclusion in a standard. Formally known as the ETSI TS 102 165-1 standard for analyzing the threats, vulnerabilities, and risks of an ICT system,[6] TVRA describes a series of steps for evaluating and estimating the factors that affect the risks a threat poses. ETSI has provided an Excel-based tool to automate risk estimation. TVRA is based on the Common Criteria for Information Technology Security Evaluation (CC),[9] which provides a strong basis for estimating an attack's likelihood—an aspect that IS1 does not address.

We enhanced TVRA to make it more suitable for impact and likelihood assessment and risk classification, and included an assessment of the attacker's capability and motivation in risk estimation.

> ANY IMPACT ASSESSMENT OF A POWER OUTAGE MUST INCLUDE ITS SOCIETAL CONSEQUENCES, INCLUDING ENVIRONMENTAL AND POLITICAL EFFECTS.

ISO/IEC 27005:2011 Information Security Risk Management

ISO/IEC 27005 provides a framework for managing risks that can compromise information security. Risk management includes establishing the risk assessment's context, evaluating and treating the risk, communicating the risk to stakeholders, monitoring the risk, and formally reviewing the risk-management process with the organization and its stakeholders.

RISK-MANAGEMENT STEPS

As Figure 1 shows, SRMM has seven main steps, which we explain in the context of the Ukraine cyberattack. The methodology is based on the ISO/IEC 27005 framework, but is tailored for the needs of smart grids. The enhancements aim to bridge the gap between technical threat, vulnerability, and risk assessment done at the technology and engineering level with risk management done at the business, company, and owner levels.

In each step, we assume that the DSO alone applies SRMM in a specific smart-grid use case. The DSO could also collaborate with stakeholders in using SRMM for a particular use case.

Context and scoping

In step 1, the DSO completes activities to prepare for risk assessment, including defining the criteria for performing the assessment and managing risks. A specification of the assessment's scope and boundaries is a central part of these activities.

To enhance scoping, SRMM uses NRM's notion of *scopes*. A scope has obligations to and expectations of other scopes, which can be a process,

system, or any other clearly defined entity. Each scope has one owner, who is responsible for ensuring that the obligations of its scope are satisfied and remain fulfilled.

The DSO begins scoping by modeling a smart-grid use case, employing NRM-based concepts to define scopes for each stakeholder and the attendant obligations and expectations, and verifying that obligations have matching expectations.

In a simplified view of the Ukrainian regional distribution grid, the stakeholders are the DSO, the energy supplier, the customer, and society. Figure 2 illustrates the NRM model, showing at a high level the DSO's obligations and expectations as owner of the distribution grid. The figure shows how these obligations and expectations connect—including internal (self-imposed) expectations such as the DSO's need to control the grid through the SCADA system—and the system's expectations of other elements.

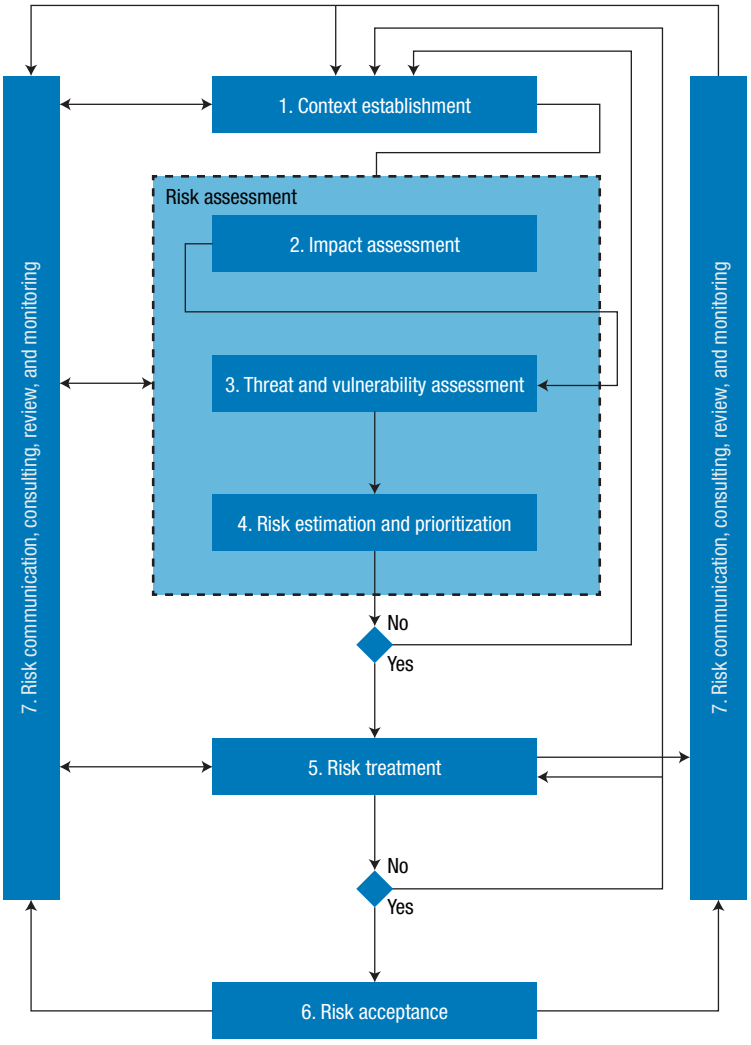


FIGURE 1. Security for Smart Electrical Grids (SEGRID) Risk Management Methodology (SRMM). SRMM's seven steps are based on the framework set forth in ISO/IEC 27005 but have been enhanced to align with a smart grid's interdependencies and complexities. The idea is to give distributed system operators (DSOs) a way to understand the potential threats, the business and societal impacts for the various stakeholders, and the likelihood that threats will occur.

Impact assessment

In this step, the DSO uses SRMM to assess a threat's potential impact on stakeholder assets and business processes, including obligation and societal impacts.

Obligation impact. An obligation is directly related to a scope and thus to its owner, the stakeholder responsible for the scope and for fulfilling the scope's obligations. For each stakeholder obligation, the maximum impact (worst-case scenario) if the obligation is not fulfilled is defined qualitatively as very low to very high. Existing impact analyses, such as the National Electric Sector Cybersecurity Organization Resource (NESCOR) impact analyses,[10] can be used as input to the obligation impact assessment. The assessment does not distinguish among aspects of confidentiality, integrity, and availability—only on determining what happens if the obligation is not fulfilled.

Societal impact. Society is increasingly dependent on the proper functioning of the electric power grid, which in turn supports most other critical infrastructures, such as potable water and food distribution, sewage handling, telecommunications, finance, and transportation. Most infrastructures can operate without electrical power for a short time, but longer outages can have devastating economic, humanitarian, and sociological consequences. Any impact assessment for a smart grid must include the assessment of a power outage and its societal consequences.

Typically, societal impact consists of human, economic and environmental, and political and social

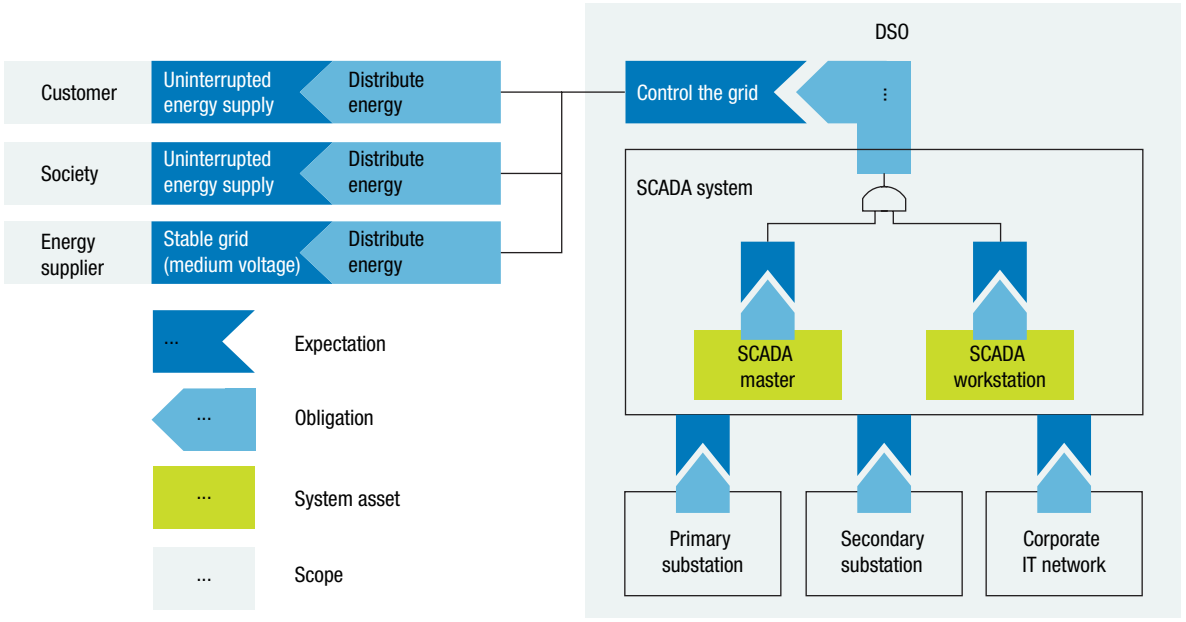


FIGURE 2. Simplified example of connecting obligations and expectations. Both the society and customer stakeholders expect the DSO to keep an uninterrupted energy supply, and the energy supplier expects the DSO to operate a stable grid and thus provide energy reliably. The DSO's internal expectation is that the supervisory control and data acquisition (SCADA) system can control the grid to fulfill its other obligations. The SCADA system, which consists of a SCADA master for grid supervision and control and SCADA workstations for grid operators, also has expectations of the substations and the corporate IT network.

impacts.[11] SRMM is concerned with impacts to internal stakeholder assets and business processes as well as the impact on obligation to other external stakeholders. However, combining these categories with the societal impact categories is not trivial. Moreover, societal impacts have a cascading effect on dependent infrastructures.[12] For example, a power outage will impact the telecommunications infrastructure, which will limit or prevent people from calling emergency response services, which could result in sick or injured people not getting the necessary help in time.

Calculating societal impact. The FP7 Viking project (2008–2011)—which investigated vulnerabilities and impacts from failing SCADA systems—used a different approach to evaluate the societal impact of a power interruption: social impact magnitude (SIM) is a logarithmic measure based on outage length, disturbance duration, and impact incidence (the number of people affected by the outage).[13] The SIM is calculated as

$$\mathrm{SIM} = \log_{10}(A_{\mathrm{people}} \times A_{\mathrm{length}}) = \log_{10}(A_{\mathrm{people}}) + \log_{10}(A_{\mathrm{length}}),$$

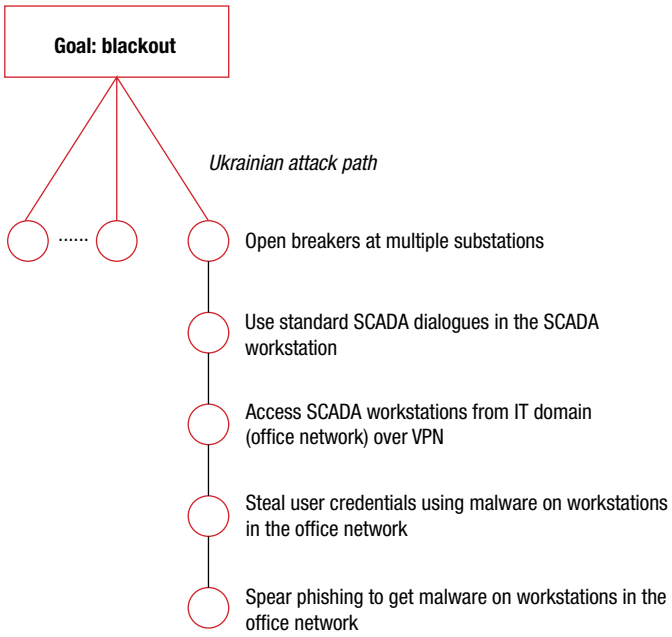
where A_{length} is the average disturbance duration in seconds and A_{people} is the number of people impacted divided by 1,000. Division by 1,000 is done to align the SIM value with the well-known Richter scale for measuring earthquakes to give an intuitive understanding of the significance of societal impacts from a power outage.

SRMM adopted the SIM approach to determine the impact on the society stakeholder identified in the scoping step, using it to determine the worst-case scenario for an outage and then mapping the results to the qualitative scale of very low to very high.

Rating impacts. During the Ukraine outage, 225,000 customers had no power for 1 to 6 hours. The outage's impact on the DSO can be related to three obligations:

- *DSO to customer.* The outage was relatively short, so depending on the contract between the DSO and its customers, the obligation impact rating would be low to medium.
- *DSO to society.* The SIM value is 6.3, which translates to a high societal impact. The regulator could launch an investigation of the outage and impose fines and additional regulations on the DSO. The estimation of the impact if this obligation is not fulfilled is high.
- *DSO to energy supplier.* The energy supplier cannot supply energy and loses income. Depending on the contract between the energy supplier and DSO, the obligation impact could be medium to high.

At this point, the DSO can decide to pursue the associated threat, vulnerability, and risk assessments only for a subset of obligations—excluding those that, when unfulfilled, result in a medium, low, or very low impact. These ratings are deemed acceptable and, to avoid unnecessary effort, are



Description of Threat & Vulnerability Scenario

- Threat: Unauthorized operation of medium-voltage breakers
- Assets: SCADA workstations, remote terminal units, breakers
- Existing controls: Access control (username/ password), firewalls
- Threat source: Unidentified group
- Threat actor: Team of highly skilled threat actors
- Threat vector: Phishing attacks to get credentials, remote access to SCADA workstations using virtual private network (VPN) access as corporate users
- Vulnerabilities exploited: Insufficient protection of credentials, insufficient training
- Threat scenario description: Attackers leverage legitimate credentials to obtain access to three DSOs, use remotely operated breakers to disconnect power, and wipe additional systems using KillDisk malware at the end of the attack. Firmware of serial-to-Ethernet devices at substations is corrupted, call centers are flooded, and follow-up attacks interfere with restoration efforts
- Unwanted incident or event: 225,000 customers lose power, energy supplier and DSOs' operations are impacted, and DSOs' reputations are damaged

FIGURE 3. Simplified attack tree for the 2015 Ukraine cyberattack attack along with the description of the threat and vulnerability scenario. Other attack paths with the same goal are possible and can be analyzed in a similar fashion.

omitted from the ensuing threat, vulnerability, and risk-assessment steps.

At the end of this step, the DSO will know the assets that a security breach will critically impact along with the effects on the stakeholders' obligations. These critical assets make up the *focus of interest* (FoI), which becomes input to the threat and vulnerability assessments.

In the example, the DSO obligations that, when unfulfilled, lead to an impact of at least high are DSO to society and DSO to energy supplier. Therefore, the assets related to these stakeholder obligations become the FoI input.

Threat and vulnerability assessment

During this step, the DSO uses SRMM to identify the attack paths and threat-attack scenarios for the assets in the FoI, taking into account the controls already implemented. The analysis includes identification of threat sources and actors and any exploitable vulnerabilities. SRMM provides guidance in this identification, but the DSO should also refer to known threat and failure scenarios,[10] threat lists,[14] and attack libraries such as the Common Attack Pattern Enumeration and Classification (CAPEC; capec.mitre.org). For detailed vulnerability analysis of the system design, the DSO can use automatic analysis tools such as the Cyber Security Modeling Language (CySeMoL).[15]

After identifying attack scenarios, the DSO links them to their impacts. Figure 3 shows an attack tree for the Ukraine example along with a description of the threat and vulnerability scenario.

Risk estimation and prioritization

For risk estimation, the DSO uses SRMM's enhanced TVRA along with results from the impact (step 2) and the threat and vulnerability (step 3) assessments to estimate the risk for each threat scenario. The risk estimate is a function of both the attack's likelihood and its impact. To prioritize risks, the DSO uses SRMM to relate each threat and vulnerability scenario plus its estimated risk to the relevant obligations.

Attack likelihood estimation. The TVRA version in SRMM includes an estimated likelihood that the potential attack will be successful. To estimate an attack's likelihood, the DSO first assesses the five factors in the attack-potential table in Figure 4 (top left). The resulting attack potential is the weighted sum of these factors, which indicates how difficult it would be to execute an attack. The attack-potential value is then mapped to a vulnerability rating from a rating range of basic to beyond high. The DSO then combines the vulnerability rating, which indicates the effort required to perform the attack, with the threat level to produce the attack likelihood.

As Figure 4 shows, the attacker's motivation and capability significantly influence threat level. Both the Stuxnet attack in Iran and the power outage in the Ukraine are examples of cyberattacks that required a highly coordinated effort involving extensive resources as well as advanced systems knowledge and expertise. If it is plausible that a highly motivated threat actor with access to considerable resources and with advanced skills will launch such a cyberattack, then the attack's likelihood should not be based solely on the required attack potential. This is the rationale for the SEGRID project team's decision to include the threat actor's capabilities and motivation in

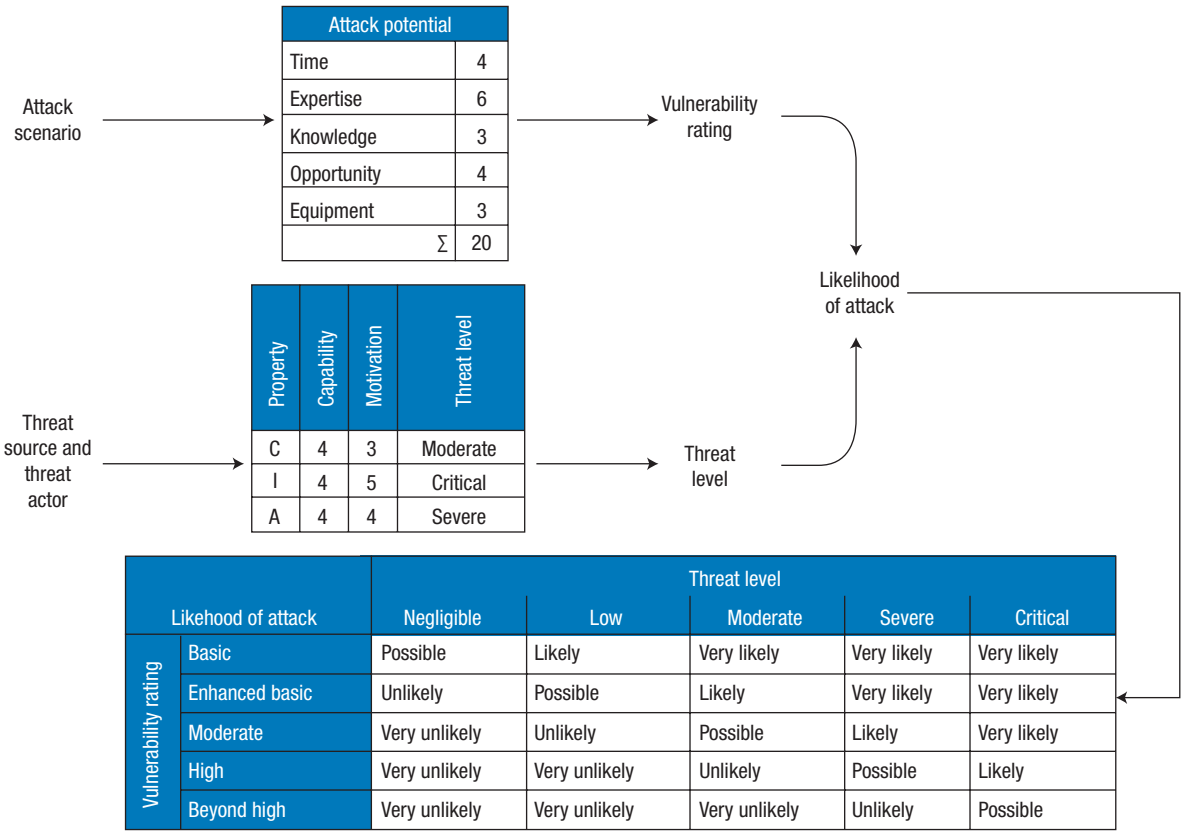


FIGURE 4. Estimation of an attack's likelihood. SRMM uses an enhanced version of the European Telecommunication Standards Institute's Threat Vulnerability and Risk Analysis (TVRA) method to assess a threat actor's capability and motivation, relate that to the threat level, and combine the threat level and vulnerability rating to produce the likelihood that a particular attack scenario will occur. The enhanced TVRA method accounts for the attacker's expertise and motivation level, which has an influence on the attack likelihood.

qualifying attack likelihood.[16] ETSI has already accepted this enhancement as a change to be incorporated in a future version of the TVRA standard.

Attack-impact estimation. To estimate an attack's impact, the DSO combines the results of the impact assessment (step 2) with the attack-intensity factor. To derive attack intensity, the DSO first obtains the attack-impact rating by combining the impact value from the impact assessment (step 2) with the intensity factor from the TVRA method. Attack intensity, which is included in the impact rating, can affect the degree to which a threat impacts a system.

An estimation example. Figure 5 gives an example for the Ukraine outage. In this case, attack potential is the combination of the opportunity to carry out the attack and the threat actor's required capability. Attack potential maps to a vulnerability rating of beyond high (f_1). In the original TVRA method, vulnerability rating was then mapped directly to attack likelihood. In the enhanced TVRA method, the vulnerability rating is mapped to the threat level (the motivation and capability of the threat source and threat actor), which is taken from the threat source and threat actor analysis. In the Ukraine attack, the threat source—an unidentified group who employed hackers and programmers—was highly motivated. Thus, the threat level was assessed to be severe. Adding threat level and the vulnerability rating yielded an attack likelihood of possible (f_2). The high impact rating, obtained from the impact assessment (step 2 of SRMM) is combined with attack intensity, which yields an impact of very high (f_3). Finally, the impact is combined with the likelihood to estimate the risk as critical (f_4) for this threat scenario.

These assessments align well with actual events: the attackers were skilled, the attack was intense and well-coordinated, and power was disrupted to an entire region.

Prioritizing risks. To prioritize risks, the DSO evaluates identified risks against the risk-evaluation criteria from the scoping step and prioritizes them according to obligations. The risk for each obligation is estimated by considering all of the expectations needed to fulfill an obligation. The identified risks that pass the risk-evaluation criteria are then mapped to the obligations. The threats with the highest risk become the risk in not fulfilling that obligation. The DSO repeats this process for each obligation.

Risks for each scope and subscope are then prioritized. For each

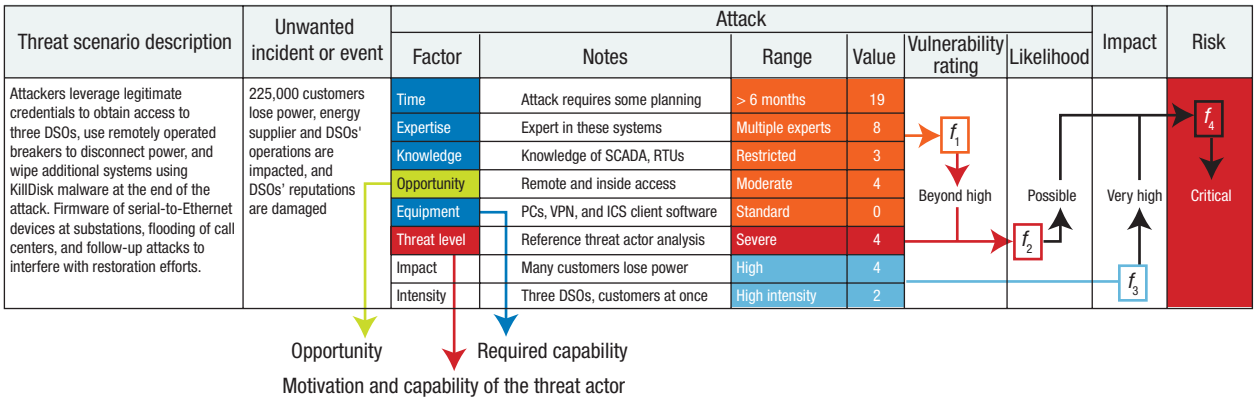


FIGURE 5. Estimating attack likelihood and impact with the enhanced TVRA method. A combination of estimating the required capability (time to plan the attack along with necessary systems knowledge and expertise), opportunity for the attack, and the attacker's motivation and capability enables the DSO to estimate the risk associated with an attack scenario.

obligation, the risk that this obligation is not fulfilled is passed up the ladder to the next scope, which assumes the responsibility for estimating the risk when the subscope's obligation is not fulfilled. In the Ukraine outage, for example, the DSO is at the scope level and the SCADA system is a subscope. If the individual responsible for estimating risk to the SCADA system determines that the risk of his inability to fulfill his internal obligation to control the grid exceeds the risk-evaluation criteria, the risk passes up to the DSO, who evaluates the extent to which his own expectation to control the grid can be met and then uses the results to estimate his risk that he cannot fulfill his obligations to the customer, society, and energy-supplier stakeholders. Those stakeholders, in turn, can pass this risk to others at the scope level, propagating risk through the value chain.

Risk treatment

The risks identified in the previous step must be treated according to their priority. The risk-treatment plan aims to reduce, retain, avoid, or share risks, taking into account an analysis of the obligations. The risk-treatment plan should include commonly accepted security controls. For reference, ISO/IEC 27002 provides guidance on selecting controls[17] and IEC 62443-3-3 specifies security requirements for industrial automation and control systems.[18] To protect the Ukrainian grid, a treatment plan might include improved access control, with roles and privilege management, audits and logs, security monitoring, vulnerability management (for example, scanning), and security-awareness education and training.

Risk acceptance

In risk acceptance—deciding which risks can be absorbed and which will need to be addressed—the DSO evaluates the risk-treatment plan and residual risks against the predefined risk-acceptance criteria. The party that must bear responsibility for accepting risk is clearly indicated because a risk is always associated with a scope and its owner.

Risk monitoring and review

In this SRMM step, the DSO documents assessment results and communicates them to relevant groups, particularly other stakeholders in the value chain (see also step 5). The technical risks have been connected to business obligations, which gives a scope's owner deeper insights into how technical risks influence business risk.

By applying SRMM to assess the risks in an actual cyberattack on the Ukrainian grid, we have shown how SRMM builds on state-of-the art risk-assessment methodologies while providing enhancements and guidance for use in smart grids. Initial experiences with SRMM on some of the SEGRID project use cases show that the methodology is suitable for risk assessment across multiple stakeholders, particularly for identifying critical threats and risk to the stakeholders. The SEGRID project team's enhancements to ETSI's TVRA method help bridge the gap between business and company management and technical threat and risk assessment.

We believe this methodology could become the risk-management approach of choice for smart-grid environments because it allows DSOs to understand the potential threats, the business and societal impacts for various stakeholders, and the likelihood of different attack scenarios. DSOs have a leading role in transforming the energy sector as facilitators of innovation, sustainability, and technological progress. Cybersecurity threats can result in severe consequences for DSOs that can easily extend to the other stakeholders in the energy value chain and in society as a whole. To prevent those outcomes and ensure that the power grid remains resilient and dependable, DSOs must clearly understand potential cyberattack risks.

ACKNOWLEDGMENTS

This work was funded by the EC as part of the EU FP7 SEGRID project under Framework 7 agreement 607109. The views expressed are purely those of the authors and may not in any circumstances be regarded as stating an official position of the EC.

ABOUT THE AUTHORS

JUDITH E.Y. ROSSEBØ is a cybersecurity specialist at ABB Norway and ABB's representative in ISA 99/IEC 6243 standardization. Her research interests include cybersecurity, industrial automation and control systems security, threat and risk assessment, and international standardization. Rossebø received a PhD in telematics from the Norwegian University of Science and Technology (NTNU). She leads the threat and risk-assessment working group in the EU's Security for Smart Electricity Grids (SEGRID) project and is a member of IEEE. Contact her at judith.rossebo@no.abb.com.

REINDER WOLTHUIS is a senior cybersecurity consultant and project manager in the Cyber Security & Robustness Group at TNO, the Netherlands. His research interests include risk management, security metrics and benchmarking, security automation, and usability of security solutions. Wolthuis received an MSc in electrical engineering from the University of Twente. He is the project coordinator of SEGRID. Contact him at reinder.wolthuis@tno.nl.

FRANK FRANSEN is a senior scientist in TNO's Cyber Security & Robustness Group. His research interests include emerging security technologies, cyberthreat intelligence sharing and use, security of mobile communication systems, information security and risk management, and the cybersecurity of smart energy grids. Fransen received an MSc in information technology from the Technical University of Eindhoven. Contact him at frank.fransen@tno.nl.

GUNNAR BJÖRKMAN is a doctoral student in the Electrical Power and Energy Systems Department at the KTH Royal Institute of Technology (KTH). His research interests include the security of supervisory control and data acquisition (SCADA) systems. Björkman received an MSc in electrical engineering from KTH. Contact him at gunnar.bjoerkman@outlook.com.

NUNO MEDEIROS is head of the Cyber Security department at EDP Distribuição. His research interests include cybersecurity and data protection. Medeiros received an MSc in electrical and computer engineering from the University of Porto (FEUP) and an MSc in information technology–information security (MSIT-IS) from Carnegie Mellon University. He is a member of the European Commission's Smart Grids Task Force—Stakeholder Forum (SGTF-SF) working group and the EC Smart Grids—Data Privacy Impact Assessments (DPIA) task force and a founding representative and current member of the European Energy—Information Sharing & Analysis Centre (EE-ISAC). Contact him at nuno.medeiros@edp.pt.

REFERENCES

1. N. Falliere, L.O. Murchu, and E. Chien, "Symantec Security Response: W32.Stuxnet Dossier," v1.4, Symantec, 2011.
2. "Cyber-Attack against Ukrainian Critical Infrastructure," IR-ALERT-H-16-056-01, 2016; ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.
3. R.M. Lee et al., *Analysis of the Cyber Attack on the Ukrainian Power Grid*, white paper, SANS Inst.—Industrial Control Systems and the Electricity Information Sharing and Analysis Center (E-ISAC), 18 Mar. 2016.
4. *HMG IA Standard Nos. 1 and 2—Supplement—Technical Risk Assessment and Risk Treatment*, UK Communications Electronics Security Group (CESG), Apr. 2012.
5. M. Hoeve et al., "El Metodo—Managing Risks in Value Chains," *Proc. Securing Electronic Business Processes—Highlights of the Information Security Solutions Europe 2011 Conf.* (ISSE 2011), 2011, pp. 214–223.
6. European Telecommunications Standards Inst., *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN), Methods and Protocols—Method and Proforma for Threat, Vulnerability, Risk Analysis* (ETSI TS 102 165-1, 2011); etsi.org/deliver/etsi_ts/102100_102199/10216501/04.02.03_60/ts_10216501v040203p.pdf.
7. Int'l Org. for Standardization, *Information Technology—Security Techniques—Information Security Risk Management (ISO/IEC 27005)*, 2011.
8. European Committee for Standardization, European Committee for Electrotechnical Standardization, and European Telecommunications Standards Inst. (CEN-CENELEC-ETSI) Smart Grid

Coordination Group, *Smart Grid Reference Architecture*, 2012.
9. Int'l Org. for Standardization, *Information Technology—Security Techniques—Methodology for IT Security Evaluation (ISO/IEC 18045)*, 2008.
10. Nat'l Electric Sector Cybersecurity Org. Resource, *Electric Sector Failure Scenarios and Impact Analyses*, v1.0, NESCOR Technical Working Group 1, 2013.
11. "Risk Assessment and Mapping Guidelines for Disaster Management," EC staff working paper 21.12.2010, 2010.
12. M. Theocharidou and G. Giannopoulos, *Risk Assessment Methodologies for Critical Infrastructure Protection, Part II: A New Approach*, tech. report EUR 27332 EN, EU Joint Research Centre, 2015.
13. M.B.O. Larsson, G. Björkman, and M. Ekstedt, "Assessment of Social Impact Costs and Social Impact Magnitude from Breakdowns in Critical Infrastructures," *Proc. Int'l Workshop Critical Information Infrastructures Security* (CRITIS 12), 2012, pp. 240–251.
14. EC Expert Group on the Security and Resilience of Communication Networks and Information Systems for Smart Grids, *Threat Analysis*, WP 1.2 EC Dir. Gen. for Info. Sec., 14 Mar. 2012.
15. T. Sommestad, M. Ekstedt, and H. Holm, "The Cyber Security Modeling Language: A Tool for Assessing the Vulnerability of Enterprise System Architectures," *IEEE Systems*, vol. 7, no. 3, 2013, pp. 363–373.
16. J.E.Y. Rossebø, F. Fransen, and E. Luiijf, "Including Threat Actor Capability and Motivation in Risk Assessment for Smart Grids," *Proc. Joint Workshop Cyber-Physical Security and Resilience in Smart Grids* (CPSR-SG 16), 2016, pp. 1–7.
17. Int'l Org. for Standardization, *Information Technology—Security Techniques—Code of Practice for Information Security Controls (ISO/IEC 27002)*, 2013.
18. Int'l Electrotechnical Commission, *Industrial Communication Networks—Network and System Security—Part 3-3: System Security Requirements and Security Levels (IEC 62443-3-3)*, 2013.