Cyber security analysis of Web-of-Cells energy architectures

Roberta Terruggia
RSE SpA
Italy
roberta.terruggia@rse-web.it

Giovanna Dondossola
RSE SpA
Italy
giovanna.dondossola@rse-web.it

Mathias Ekstedt
KTH
Sweden
mekstedt@kth.se

The evolution of the power grid toward a distributed architecture requires rethinking of the traditional control strategies. From a hierarchical structure the future grid moves on to a decentralized organization where the Distributed Energy Resources are spread over the whole infrastructure. The control strategies need to implement new functionalities where the ICT (Information and Communication Technology) components represent essential assets and the cyber security issues have to be addressed very carefully. This paper presents a methodology for the cyber security analysis of an ICT architecture implementing the Web-of-Cells (WoC) concept for the control of the future power grid as proposed by the ELECTRA EU project. Starting from a WoC architecture, a realistic Cell network topology is modelled by the securiCAD tool. The model comprises cells where the main ICT assets (hosts, network nodes, programs, services and data flows) contain vulnerabilities allowing that possible attack steps are deployed to perform a cyber attack. To contrast the attack process, specific cyber security measures can be included in the model. The cyber security analysis is performed by means of the securiCAD tool implementing the proposed methodology for the evaluation of the attack graphs and the computation of the TTC (Time To Compromise) indicator. TTC represents the expected time an attacker would take to compromise every single asset in the modelled ICT infrastructure. The methodology allows to perform a sensitivity analysis estimating the efficacy of the applied mitigation measures by comparing the TTC values in the different model setups. The cyber security analysis described in this paper addresses the cyber threat assessment of a sample multi phase attack process by evaluating the possible attack paths and obtaining the TTC values for the attack target assets.

Smart Grids, ICT Architectures, Cyber Security Assessment, Control Strategies, Distributed Energy Resources, Web-of-Cells.

1. INTRODUCTION

In the last years the power system is facing a strong transformation: it is changing from a hierarchical to a decentralized structure where the Distributed Energy Resources spread over the whole infrastructure. This new landscape requires the traditional control strategies to be reconsidered including new functionalities where the ICT assets become fundamental and the consequent cyber security concerns have to be considered very carefully.

Power transmission, distribution, aggregation and consumption domains are changing their infrastructure increasing the penetration of ICT components and communications in order to address the requirements of the new control functionalities. The adoption of the new technologies allows to improve the reliability of the grid and its hosting capacity, however at the same time the grid stability is becoming increasingly

dependent on the communications and ICT components status and behaviour.

The new scenario moves from specialized standalone systems, where in several cases the security is guaranteed by physical perimeters and private infrastructures, to interconnected outsourced digital infrastructures, often remotely controlled using public channels. The new technologies and connectivity bring benefits to the power grid operation, nevertheless new cyber security concerns have to be addressed. Significant risks never considered before have to be analysed because new vulnerabilities existing in the system could be exploited in order to perform malicious actions entering from the communication and ICT devices and able to compromise the physical process. A recent analysis of real malicious activities in terms of possible evidences of cyber kill chains to energy infrastructures is given by the US-CERT alert [24].

The paper addresses the analysis of the cyber security considering an attack process targeting an ICT architecture for the new decentralized power grid control strategies. The infrastructure focuses on the Web-of-Cells (WoC) concept as proposed by the ELECTRA EU project, where the infrastructure is split in several cells and locally controlled.

The analysis considers that an attack process is not a monolithic entity but even can be decomposed in several attack phases. Each phase is required for the execution of the whole attack chain.

The ICT infrastructure is modelled and analysed by securiCAD, a tool that allows estimations of attack likelihoods in relation to architecture variants. securiCAD is used to model the ICT architecture and each phase of the attack process, applying the evaluation more times it is possible to assess the entire attack chain.

The securiCAD based analysis presented in this paper can be viewed as a step of the whole cyber security analysis process described in [4]. Specifically, the securiCAD approach addresses the cyber threat assessment of the architectures by evaluating the possible attack paths and allows to obtain a Time To Compromise (TTC) probability distribution for the main assets of the infrastructure. TTC represents the expected time an attacker would take to compromise every single asset in the modelled ICT infrastructure. The ability to identify components that are critical in terms of security supports the selection of suitable countermeasures to be implemented and the evaluation of their effectiveness, i.e. the steps 4 and 5 of the mentioned security analysis process [4].

The structure of the paper is the following: Section 2 briefly describes some related works, then Section 3 introduces the operational context illustrating the concept of Web-of-Cells. Section 4 presents the securiCAD tool, that is the tool used to carry out the cyber security analysis, then Section 5 introduces the analysis methodology. Section 6 describes the WoC ICT architecture, modelled in Section 7 with securiCAD. The main results of the cyber security analysis of the WoC ICT architecture addressing a field test implementation of ELECTRA use cases are presented in Section 8. Then Section 9 provides some final remarks and future works.

2. RELATED WORKS

The assessment of the cyber security of critical infrastructures is an important task addressed by several studies [19], [20], [25]. The analysis can be performed using probabilistic methods estimating the infrastructure weaknesses as combination of

probabilities of basic events. Several formalisms with different capabilities can be applied for the analysis. The Attack Trees (AT), an evolution of the Fault Trees, is a technique that allows to model the attack process as a combination of attack steps starting from basic attack events (leaves of the tree). These are combined using boolean operators to represent the possibilities to reach the attack goal (the top event). Some studies [6], [21] present this formalism and [14], [15] use it for the assessment of critical infrastructures. The AT formalism has been extended for the inclusion of countermeasures nodes, components able to reduce the probability of the attack success. This enriched formalism is called Attack Defence Trees (ADT) and [16], [17] apply this technique for the analysis in different sectors including power systems.

In [22] the Weighted-ADT (WADT), an enriched version of the ADT formal method, is presented. The WADT allows to perform qualitative and quantitative analysis enhancing the formalism with cost and impact attributes. This technique has been applied to the power system environment in [23].

Another class of formalisms refers the techniques able to represent not only the combinatorial model, but also to address decision analyses including uncertainty. These methods are based on probabilistic graphical formalisms as Bayesian Networks and Decision Networks (or Influence Diagrams). Several studies have been carried out for the probabilistic analysis of the cyber security of different sector infrastructures including power systems [7], [12], [18]. These models allow to capture uncertainty and compute indicators using inference techniques. Moreover it is possible to select the best set of countermeasures to activate through decision approaches.

In the analysis presented in this paper combinatorial and Bayesian like formalisms have been deployed to study the cyber security of the ICT infrastructures for the future power grids.

3. OPERATIONAL CONTEXT: WEB-OF-CELLS

The prediction for the future power grid is an increase of the flexible energy resources in special way at distribution level. The future organization of power grid resources requires new control strategies able to address the challenges posed by their distributed topology. To answer to the new requirements the ELECTRA IRP EU project [1] proposes the Web-of-Cells concept that is a new distributed control paradigm of the power infrastructure.

The power system is split in several "Cells" and the control strategies are based on a cell-centric approach. A Cell is defined as a portion of the

power grid able to guarantee a predefined power exchange with its boundaries. The Cell stability is maintained controlling its internal resources, i.e. generators, flexible loads and storage systems [8].

Each Cell is physically connected with one or more neighbouring Cells by means of tie lines. A Cell can involve one or more voltage levels and cover different sizes in terms of geographical areas. Figure 1 presents an example of a Web-of-Cells power architecture.

Figure 1: Example of a Web-of-Cells power structure

The WoC concept proposes to solve local problems locally, using decentralized control strategies [5]. Cell stability is maintained by a cell controller, a component able to provide autonomous control of balance, frequency and voltage by means of specific control actions to the cell resources. This new paradigm requires to understand the cyber security implications of the deployed ICT architectures [9].

4. SECURICAD TOOL

securiCAD is a tool developed by foreseeti [2] to perform cyber security analysis of ICT infrastructures deployed in heterogeneous business sectors (financial as well as energy sectors). It falls into the category of quantitative and probabilistic assessment tools that formalise the estimation of threat likelihoods of system architecture designs. One of the distinguishing features of this tool is that it separates the architecture model construction from the cyber security analysis, the former is left to the tool user and the latter is widely automated by generating attack/defence graphs from a library of predefined potential attack steps and security measures.

From a predefined modelling language consisting of classes such as networks, firewalls, hosts, clients, servers, data flows, access control system

architecture models are built. All classes in turn have a number of attack steps and defence mechanisms, e.g. a host can be fully compromised or be down due to a denial of service attack, and the host can deploy defence mechanisms such as address space layout randomization, anti virus, and be up to date with patches. Also a hypothetical attacker (corresponding to a professional penetration tester) is placed in the system model. All the model properties are probabilistic in nature, so that the property of e.g. “being patched” is specified as a probability between 0-100%. From this information a large number of attack/defence graphs in the form of Bayesian-like networks [11] are generated. These networks are Monte Carlo simulated to provide a probabilistic overall assessment. This probabilistic approach is characterised by the high level of uncertainty due to the nature of the cyber security challenge in terms of threats, vulnerabilities and vulnerability exploitations [3] as well as uncertainties in the ICT infrastructure configuration. Concretely the attack/defence graphs in securiCAD are generating probability distributions of the TTC indicator [10] for each attack step and builds an attack path overview of the simulated attack graphs. The TTC is evaluated considering the propagation of the attack following the different paths of the attack graph and for each step of the path takes the elicited based probabilities into account. The individual probabilities of attack success is based on a mix of deterministic dependencies, such as that you need to have access to an asset before it is possible to run an exploit on it, and estimated TTC probability distributions, such as that it generally takes longer time to compromise a hardened and patched host, but it is not inherently impossible. The exact TTC probability distributions can be varied in securiCAD but it also comes with default values based on a number of previous research studies. In this work the default distributions were used.

5. ANALYSIS METHODOLOGY

A novel contribution of the paper is the definition of a methodology allowing to understand the securiCAD tool capabilities in the context of a wider assessment approach supporting the user in the evaluation of ICS (Industrial Control Systems) attack chains.

First of all, it is essential to identify the operational context under analysis in terms of functionalities and requirements. In this paper the operational context addresses the decentralized control strategies required by the Web-of-Cell concept. The selection of the context allows to identify the type of analysis to carry out. It is possible to deploy qualitative as well quantitative methods, depending on the information considered and on the accuracy

of the requested results. The analysis can be performed using an experimental setup, building models with different formalisms or with mixed methods where the model parameters come from laboratory or field sources. In this paper a mixed method is used as presented in the next sections.

The process requires to identify some relevant indicators able to provide evidences of the phenomenon under analysis. The study presented in this paper select the TTC of a given asset and the attack success probability as key indicators, moreover the information obtained by the post processing of the attack graph provide a valid direction for the progress of the analysis.

The evaluation of the indicators requires the selection of a suitable tool capable to model the information of interest and to compute the indicator values. For this analysis the identified tool is securiCAD, a tool able to model the ICT architecture and to perform quantitative probabilistic analysis for the computation of the attack success rates.

The definition of the relevant ICT architecture to be studied is an essential step of the analysis. In particular it is necessary to select the main components in terms of hosts, network devices and cyber security assets and how these communicate. Each tool captures different levels of abstraction and ensures diverse modelling power. For this reason it is important to select the right tool to be able to model the key infrastructural aspects for the analysis, whilst containing complexity and size explosion of the model.

The ICT architecture has to be represented by a model expressed by one or more formalisms. Moreover the model parameters need to be set, implementing the values that are more representative for the context. Some of the parameter values will be changed in the progress of the study, indeed a baseline and an enhanced scenarios are compared in the analysis to estimate the effects of the architectural and parameter changes as the effectiveness of the countermeasure implementation.

The baseline scenario comprises the default values and the enhanced one implements one or more security measures under study.

After the setup of the two models to be compared it is possible to perform the analysis and obtain the results in terms of indicators. Comparing the values coming from the baseline and enhanced models it is possible to highlight the effectiveness of the implemented measures.

In this paper the assessment of the cyber security of a smart grid architecture has been performed addressing quantitative evaluation methods implementing probabilistic and stochastic

formalisms. The scenario under analysis addresses an attack process involving IT (Information Technology) as well OT (Operational Technology) assets. An attack process can be decomposed in some phases, in turn each phase is structured in several attack steps. For sake of simplicity in this paper a two phase attack process is addressed, but the methodology can be applied to more complex multi-phase processes. For representing in the correct way the structure of the attack process the two phases have been modelled and analysed by two computation runs and the results combined for a wider analysis.

6. ARCHITECTURE

To perform a cyber security analysis, it is essential to identify an ICT architecture that includes all the relevant aspects of the environment under investigation. This could be a difficult task if the context of the analysis is complex and not all the architecture components are identified.

The concept of Web-of-Cells is instantiated in a high level architecture covering the low voltage field test facility in RSE, a typical field and enterprise ICT infrastructure, including the main ICT components required by the control functionalities [8]. Several areas involving different cyber security requirements can be identified: components connected through corporate as well as process networks have to communicate in a secure way through different domains.

The WoC control strategy requires communications inside a given cell or inter-cells. The different areas are interconnected by means of wired but also wireless channels possibly deploying heterogeneous network technologies.

Figure 2: Tested ICTArchitecture

Following the cell-centric approach emphasized by the WoC control scheme where the local problems are resolved locally, the focus of the paper analysis is on a cell area where a set of resources are controlled by a cell controller, which implements one or more control functionalities.

Figure 3: Field Cell C Model

In a more general view, the architecture involves a corporate network possibly connected with an external network (Internet) and with the process network. An overview of the WoC ICT architecture is presented in Figure 2.

7. SECURICAD MODEL

Figure 3 presents the securiCAD model of a single cell (cell C) of the specified architecture, where each cell control network includes the controllable resources, a cell controller, an HMI (Human Machine Interface) for the monitoring of the component status and an operator workstation which is connected also to the corporate network.

This model implements the main assets and the communications involved in a sample cell. Two different data flows are identified and modelled. The Cell controller communicates with the resources by means of the Modbus protocol, receives the measures and sends the control commands. The operator is able to monitor the status of the cell resources via a HMI deploying the HTTP protocol. For each resource these two data flows are implemented in order to allow the communication with the Cell controller and the HMI. Moreover the operator workstation communicates with other assets connected with the corporate

network, e.g. corporate employee hosts and servers. The securiCAD tool allows modelling the general behaviour of a communication protocol, but not the specific characteristics, neither the protocol stack details. Indeed, the objective of the analysis is to take into account the attack process as a set of possible attack steps and implemented countermeasures, without going deeply in the specific attack steps. Different types of attack processes can be analysed, involving many or a specific information flow or asset.

8. ANALYSIS OF THE ATTACK SCENARIO

The selected attack scenario comprises an external attacker that deploys the corporate network to inject a phishing message and obtain control of the operator workstation. Subsequently the attacker is able to intrude the control communication and compromise the cell controller asset. This selected scenario is quite representative of actually happened cyber kill chains to power control systems [26]. The attack process under analysis can be subdivided in two main phases: the first one comprises as target the access to the control network and the latter consists of the intrusion into the communications for the compromise of the cell controller. The two phases have been analysed in sequence where the success of the control network

Figure 4: Attack Graph – Phase 1

access (Man In The Middle) phase is a prerequisite for the achievement of the second phase (Intrusion in the control communications and cell controller compromise). In order to get specific results for each attach phase, two separate securiCAD runs have been executed.

Security analysis - First phase: Man In The Middle attack

The Man In The Middle (MITM) attack often represents a preliminary step in the attack process leading to perform a successive malicious action.

In this analysis the MITM attack refers the ability of an attacker to intercept a specific data flow, but not the possibility to modify the message contents.

The analysis reported in this section investigates the TTC of the MITM attack step, so explores possible attack paths leading to the MITM attack to the control network. Modbus does not natively provide any message protection measure, but it is possible to implement such extensions by means of a network wrapper.

securiCAD allows to model the existence of a malicious data flow between the attacker and a malicious service running on the user machine. Let us take the example of a phishing message that has been sent to the victim. After the victim opens

the malicious message it activates a service that is able to create a data flow with the attacker.

In this scenario the cell architecture comprises an operator workstation in the cell network where the operator is tricked to activate the malicious service. The operator workstation communicates with the corporate network as well as with the resources in the cell local area network, so through the corporate network and the operator workstation the attacker is able to reach the control network used by the cell controller and the resources to exchange process data.

Figure 4 presents the attack graph for the attack first phase where the attacker is depicted with a red circle and the target with a blue one (Modbus communication Man in the Middle). The green circles represent imperfect defence measures identified by the tool, including “Encryption” and “Authentication” (highlighted with a black circle), the security extensions considered in the analysis.

The attack graph contains the attack paths used to compute the TTC values. Figure 5 presents the MITM TTC values of the dataflow between the Lithium Battery (a cell resource of the field cell C) and the cell controller. The plain message exchange is implemented without authentication, encryption and nonce protocol protections (baseline scenario). From the tool estimations a

success rate of 86% is achieved in 20 days as displayed in Figure 5.

A valid countermeasure to reduce the MITM success is the implementation of authentication and integrity mechanisms on the Modbus data flow. In securiCAD such security mechanisms can be modelled as protocol parameters. Some variables can be set considering the protocol asset: the exchanged information may be **authenticated**, i.e. the information is assumed not be altered or substituted (reducing the success probability of MITM), and/or **encrypted**, where encryption prevents eavesdrop and reduces the MITM success probability ensuring that the ciphered text is not decrypted without authorization. The **nonce** prevents replay attacks, appending an unpredictable value ensuring that past legal messages cannot be reused.

Figure 5: Dataflow MITM - success rate with default security parameters

Figure 6 shows the TTC to achieve the MITM attack step in case the effectiveness of 80% of the authentication, encryption (imperfect measures in the attack graph of Figure 4) and nonce.

Figure 6: Dataflow MITM - success rate with probability protocol protection (authentication, encryption and nonce) set to 0.8

Comparing the results with those achieved in the previous case (Figure 5) the time increases for 50% of attackers from 6 to 10 days, and considering 95% of attackers from 51 days to infinity value. The probability of success of the

attack decreases from 71% to 53% within 10 days, from 86% to 73% within 20 days and from 95% to 88% within 50 days. Assuming perfect security measures in terms of authentication, encryption and nonce the results in Figure 7 have been obtained. The countermeasures are able to avoid the Man in The Middle attack: indeed, the TTC value is infinity and also in 50 days the probability is 0%. This last analysis is a limit case not achievable in the real world, since it is never possible to guarantee the effectiveness of 100% of any given security measure.

Figure 7: Dataflow MITM - success rate with protocol protection (authentication, encryption and nonce) set to "On"

Security analysis - Second phase: Intrusion in the control communications

The analysis presented in the previous section considers the ability of an attacker to perform a MITM attack to control data flows and represents the first phase of the attack process. Indeed, the MITM to TCP_Modbus_Li data flows can be considered as the first attack step in order to perform a more severe intrusion in the control communications. In this analysis an intrusion refers the ability of an attacker to modify the contents of the control messages, i.e. to intercept the data flow and to compromise the data flow source node (the Cell controller in our case). In this section the focus is on the attack second phase: the aim of the analysis is to evaluate the probability of an intrusion in the communications between the Cell controller and the resources (Modbus data flows) given the success of the MITM attack step, for this purpose the TTC value to the Cell controller node is estimated.

In Figure 8 is depicted the attack graph obtained from the analysis of the second phase. The attacker starting point is the Modbus communication Man in the Middle, the target step of the first phase. The target step of the next analysis is the Cell Controller Compromise (blue circle). Also in this case the security extensions considered in the analysis are highlighted with a black circle.

Figure 8: Attack Graph – Phase 2

Figure 9 presents the results where the infrastructure does not implement any specific security measure, only the default parameters are in place (baseline scenario). After 10 days the probability of cell controller compromise is 58% that becomes 77% after 20 days and 92% after 50 days.

Figure 9: Cell controller Compromise – success rate with default security parameters

Applying host based defences (e.g. patches at both client and host level) the TTC values increase and the success rate of the attack decreases as presented in Figure 10: 43% of attackers

compromise the cell controller after 10 days, 65% after 20 days and 85% after 50 days.

Figure 10: Cell controller Compromise – success rate with specific host based security management measures (patches)

By extending the infrastructure with all the host level security parameters set to “On”, i.e. by setting to “On” also the AntiMalware and the Data Execution Prevention parameters, a more secure setup is reached and this allows to obtain the results presented in Figure 11.

Figure 11: Cell controller Compromise – success rate with all host based security parameters set to “On”

The compromise probability of the cell controller is 31% after 10 days, 45% after 20 days and 59% after 50 days.

9. CONCLUSION

In summary, this paper presents a methodology for the cyber security analysis of attack processes carried out with the securiCAD tool. The selected operational context refers to the WoC concept developed in the ELECTRA IRP project. The ICT infrastructure considering the functional aspects of the WoC control strategies has been specialized and modelled. The attack process has been split in two main attack phases for the evaluation of the effectiveness of cyber security countermeasures performing a sensitivity analysis of the Time To Compromise (TTC) values.

The analysis addresses the cell architecture implemented in the RSE field test environment. A securiCAD model has been obtained for evaluating the TTC values and attack success rates in the two attack phases of the attack process: a Man In The Middle attack to (Modbus/TCP) control communications followed by an intrusion in those communications for compromising the cell controller. Several countermeasures have been included in the model and their effectiveness in terms of TTC and attack success rate estimated.

The analysis results presented in this paper show how an attack process can be addressed and the cyber security evaluated to identify the appropriate countermeasures. The effectiveness are measured in terms of attack graph examination and of time required to achieve the attack goal.

A key aspect of the attack process analysis is the time scale. The success rate of a given attack raises when a longer time for the evolution of the process is allowed. The analysis presented in this paper select the TTC as a key performance indicator of the attack process success, where the probability of attack success is measured as a function of time. The success rate is not only a simple percentage of the attack success, but a function of the number of days available to the attackers for carrying out the attack process. This is a driving principle of the cyber security analysis

allowing to understand the defence line power and limits, when compared to the behaviour of the offensive actions.

The analysis of the ICT infrastructure performed with securiCAD can be combined in a synergic and complementary way with other probabilistic analyses based on different formalisms as the decision networks [12]. This would allow to address the whole cyber kill chain [13] from the reconnaissance phase to the final action addressing more complete scenarios.

The next steps of the work will start from the results presented in this paper and consider them as input for an attack modelling study of the attack process considering the phases an attacker has to perform to compromise the target.

The advantage of this combined approach will be in terms of modelling power and ability to compute probabilistic indexes by means of basic inferences. Moreover it can help to select the countermeasures considering the objective function to be optimized.

ACKNOWLEDGMENTS

This work was partially supported by the EU ELECTRA IRP project funding from European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 609687 as well as the Swedish Civil Contingencies Agency through the research centre Resilient Information and Control Systems (RICS).

REFERENCES

- [1] ELECTRA IRP EU project, available at <http://www.electrairp.eu>
- [2] SecuriCAD Cyber Threat Modeling and Risk Management – securiCAD by foreseei. More information available and community edition of the tool at: <https://www.foreseei.com/>
- [3] M. Korman, M. Välja, G. Björkman, M. Ekstedt, A. Vernotte, R. Lagerström, “Analyzing the effectiveness of attack countermeasures in a SCADA system”, In: Proceedings - 2017 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids, CPSR-SG 2017, Association for Computing Machinery, Inc , 2017, p. 73-78
- [4] G. Dondossola, S. Fries, D. Engel, C. Neureiter, R. Terruggia, M. Uslar: “Smart Energy Grid - Coordination Group Cyber Security & Privacy (SEG-CG/CSP Report)”, CEN-CENELEC-ETSI - CCMC 1, 1-69, <ftp://ftp.cenelec.eu/EN/EuropeanStandardization/Fields/EnergySustainability/SmartGrid/CyberSecurity-Privacy-Report.pdf>

- [5] L. Martini, H. Brunner, E. Rodriguez, C. Caerts, T. I. Strasser, G. M. Burt "The grid of the future and the need for a decentralized control architecture: the Web-of-Cells concept" CIRED 2017 24th International Conference on Electricity Distribution Glasgow, 12-15 June 2017
- [6] B. Kordy, S. Mauw, S. Radomirović, P. Schweitzer, "Foundations of Attack-Defense Trees", In Formal Aspects of Security and Trust (FAST'10) , volume 6561 of LNCS, pages 80-95. Springer, 2011
- [7] T. Sommestad (2012), "A framework and theory for cyber security assessments", PhD Thesis, Industrial information and control systems, Royal Institute of Technology, Stockholm, Sweden
- [8] ELECTRA Deliverable 5.3, "The Web-of-Cells control architecture for operating future power systems", <http://www.electrairp.eu>
- [9] ELECTRA Deliverable 4.4 "ELECTRA Web-Of-Cells Cyber Security Analysis Report", <http://www.electrairp.eu>
- [10] M.A. McQueen, W. F. Boyer, M.A. Flynn, G. A. Beitel "Time-to-compromise model for cyber risk reduction estimation", Quality of Protection Workshop, ESORICS 2006
- [11] B. V. Cherkassky, A. V. Goldberg, T. Radzik, "Shortest paths algorithms: Theory and experimental evaluation" Mathematical Programming, 1996, Vol 73 n. 2 p. 129-174
- [12] D. Codetta Raiteri, L. Portinale, R. Terruggia, "Quantitative Evaluation of Attack/Defense Scenarios through Decision Network Modelling and Analysis", Proc. IEEE Intern. Carnhan Conference on Security Technology (ICCST 2014), pp. 432-437, 13-16 Oct, 2014
- [13] E. M. Hutchins, M. J. Cloppert, R. M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", 6th Annual International Conference on Information Warfare and Security, Washington, DC, 2011
- [14] J. Byres, M. Franz, and D. Miller. 2004. The use of attack trees in assessing vulnerabilities in SCADA systems. In Proceedings of the International Infrastructure Survivability Workshop. Lisbon.
- [15] P. Chee-Wooi Ten, G. Manimaran, and C. C. Liu. 2010. Cybersecurity for critical infrastructures: Attack and defense modeling. IEEE Trans. Syst. Man Cybernet., Part A 40 (2010), 853–65. Issue 4.
- [16] B. Kordy, S. Mauw, S. Radomirovic, and P. Schweitzer. Attack defense trees. The Journal of Logic and Computation, 2012.
- [17] A. Roy, D.S. Kim, and K. Trivedi. Scalable optimal countermeasure selection using implicit enumeration on attack countermeasure trees. In Proc. 42nd Int. Conf. on Dependable Systems and Networks, Boston, MA, 2012.
- [18] T. Sommestad, M. Ekstedt, and P. Johnson. Cyber security risks assessment with bayesian defense graphs and architectural models. In Proc. 42nd HICSS '09, pages 1 –10, 2009.
- [19] W. Shaw, SCADA system vulnerabilities to cyber attack. 2012 In Electric Energy online.com. Available at http://www.electricenergyonline.com/show_article.php?mag=&article=181.
- [20] W. Kroeger, Critical infrastructures at risk: a need for a new conceptual approach and extended analytical tools. Reliab. Eng. Syst. Safety, 93, 2008, 1781–1787.
- [21] B. Schneier, B. Attack trees. Dr. Dobbs Journal of Software Tools, 24(12), 1999, 21–29.
- [22] A. Bobbio, L. Egidi, R. Terruggia, A methodology for qualitative/quantitative analysis of weighted attack trees, IFAC Proceedings Volumes, Volume 46, Issue 22, 2013, Pages 133-138
- [23] A. Bobbio, L. Egidi, R. Terruggia,, E. Ciancamerla, M. Minichino, Weighted attack trees for the cybersecurity analysis of SCADA systems, 3rd International Defense and Homeland Security Simulation Workshop, DHSS 2013, Held at the International Multidisciplinary Modeling and Simulation Multiconference, I3M 2013, Pages 33-40
- [24] US-CERT, <https://www.us-cert.gov/ncas/alerts/TA18-074A>
- [25] G. Dondossola, L.P. Cambaceses, J. McDonald, M. Ekstedt, A. Torkilseng, 2011, "Modelling of cyber attacks for assessing smart grid security", Proceedings Cigré D2 2011 Colloquium, Buenos Aires 19-20 October 2011
- [26] E-ISAC SANS-ICS ICS Defense Use Case No. 6: Modular ICS Malware August 2017