Securing Cyber-Physical Systems: an Optimization Framework based on OSSTMM and Genetic Algorithms

Alessandro Giuseppi[1], Andrea Tortorelli[1], Roberto Germanà[1], Francesco Liberati[1] and Andrea Fiaschetti[1]

Abstract— **This paper presents an optimization framework, based on Genetic Algorithms, for the control of the "security level" of a Cyber-Physical System (CPS). The security level is a quantity that has been studied in several industrial standards, among which we selected the *Open Source Security Testing Methodology Manual* (OSSTMM). The proposed optimization solution is validated on scenarios representative of real operations of a security evaluator, and numerical simulations report the performances obtained by the algorithm.**

Keywords: ***Security, Cyber-Phisycal systems, Optimal Planning***

I. INTRODUCTION

In recent years, the study of Cyber-Physical Systems (CPSs) has become a topic of great interest for control system researchers, as CPSs bring together problems derived from classical control theory with concerns related to computer science and cyber-security [1]. In their most general definition, CPSs can be considered as interconnected systems that integrate both physical capabilities and computing power [2] and have found application in several fields, spacing from manufacturing [3], healthcare [4], telecommunication [5]–[7] and transportation [8] networks, power systems [9], [10] and aerospace [11].

Several works available in literature focus on real-time control of CPSs [12]–[14], and their real-time monitoring [15], [16], in order to detect attacks or anomalies that may be affecting the system dynamics. Consequently, a significant amount of effort was spent for identifying suitable models and modelling frameworks by the authors and other researchers in the field [17]–[21].

Another research direction in the field of CPSs is the one related to their security assurance [22], as, for such complex systems, assuring their controlled operation may not be sufficient to protect them against engineered attacks, such as data-altering attacks that corrupt/delay sensor readings or control signals [23]–[25] or attacks that target the system control logic itself, as stuxnet [26].

The H2020 project ATENA [27], in which this work was developed, deals with Critical Infrastructures (CIs) protection and focuses on both of the aforementioned research directions, mapping them on the "prevent, detect, mitigate" paradigm for security. In the context of the project ATENA, the partners proposed several solutions for adverse event mitigation [28], attack and anomaly detection [29], [30], and for the secure design of CI sub-systems [31], [32].

The project ATENA was designed having in mind the distinction between two different processes for the secure operation of CPS:

- Risk Mitigation, i.e., the process of reconfiguring a CI in order to mitigate "risk", a quantity that captures the likelihood of having a service disruption caused by detected adverse events or attacks;
- Vulnerability Management, i.e., the process of addressing the known vulnerabilities affecting protected system so that an eventual attacker would face a secured system.

The present work deals with the process of vulnerability management, and proposes an optimization framework to control what we will define as the security level of the protected CI.

The idea of measuring the security of a system is a concept that is already broadly investigated by industrial standards, as the *Common Vulnerability Scoring System* (CVSS) [33], [34] and the *Common Criteria for Information Technology Security Evaluation* (CC) [35]. The modalities applied and quantities measured in these various industrial standards are different, but they all share a common idea: *security* is something that should evaluate a frozen "snapshot" of the system, without taking into account ongoing attacks or threats that affect it.

Among the various industrial standards, the one that is the most suitable for the purpose of evaluating the security of a CPS in its wholeness was identified by the consortium of the ATENA project in the Open Source Security Testing Methodology Manual (OSSTMM) [36], a methodology that identifies a procedure, along with several security-related quantities, that is recognized by the industry as a proper method for security assessment. The whole methodology behind OSSTMM is built around the simple concept of having a balance between the number of *interaction points* present in the system (e.g., a PLC that interacts with a field sensor thought a communication bus), their *limitations* (e.g., the vulnerabilities and weaknesses affecting a encrypted communication channel between a SCADA server and a RTU) and the number of active security *controls* (e.g., data integrity checks conducted by a PLC before actuating its controls) put in place to address the identified limitations.

[1] A. Giuseppi, A. Tortorelli, R. Germanà, F. Liberati and A. Fiaschetti are with the Department of Computer, Control, and Management Engineering "Antonio Ruberti" at "La Sapienza" University of Rome, Via Ariosto, 25, 00185 Rome, Italy, e-mail: {giuseppi,tortorelli,germana,liberati,fiaschetti}@diag.uniroma1.it.

This work has been carried out in the framework of the ATENA project [Grant Agreement 700581] partially funded by the EU. This work reflects only the authors' view, the EU Commission is not responsible for any use that may be made of the information it contains.

Such a balance introduces the concept that too many controls may be counterproductive for CPS security, as they may introduce new limitations and vulnerabilities to the system, as well as higher maintenance and deployment costs.

The interested reader can find a complete description of the methodology and its related quantities in [36]; we report here, for the sake of presentation, the two main indicators selected for the studies conducted in project ATENA:

- *Actual Security*, the main indicator of OSSTMM, is a quantity that measures the aforementioned balance between limitations and controls. For the sake of readability for the evaluator, it is reported in a number that resembles a percentage, but in reality it has a logarithmic nature, meaning that even a slight improvement in its score could have significant implications on the security of the system;
- *True Protection* is a more informative indicator that measures the same balance as Actual Security but also considering the *category* of the implemented controls, identified by OSSTMM as Authentication, Indemnification, Resilience, Subjugation, Continuity, Non-Repudiation, Confidentiality, Privacy, Integrity and Alarm, which describe all aspects of the CPS and the protection against all types of attacks.

The purpose of this paper is to develop an optimization framework able to act as a controller for the process of vulnerability management in CPSs. We note that the proposed solution, described in the remainder of the paper, can be considered as an off-line planner (and not a real-time controller). The effectiveness of vulnerability management will be measured in terms of its repercussions on the OSSTMM-identified measures of the security level, and, due to the heavily nonlinear nature of the two selected security indicators, the optimization will be performed utilising a Genetic Algorithm (GA).

The remainder of the paper is structured as follows: Section II reports the needed preliminaries on GAs; Section III introduces the problem of vulnerability management as studied in the ATENA project; Section IV describes the reference scenarios used for testing the presented approach; Section V reports some numerical results in order to validate the proposed solution; finally, Section 6 draws the conclusions and highlights possible future research directions.

II. Preliminaries on Genetic Algorithms

This section reports a brief introduction to GAs to provide the reader with the needed background to understand the optimisation method selected for the vulnerability management problem. The interested reader can find more detailed discussions in the surveys [37], [38].

GAs are evolutionary algorithms useful when searching for the solution in a very wide range of alternatives. They are inspired by natural evolution and, therefore, the terminology used in this framework is directly taken from that field. A candidate solution is considered as an *individual* of the *population*. Basically, the evolution is regulated by the processes of *natural selection* and *reproduction*. The reproduction operator enforces the recombination of the genetic information of the *parents*, i.e., individuals of the former generation, mimicking the biological systems, to build a new individual. The natural selection operator selects the best individuals of the current generation of the population (according to the considered cost function, which is also called fitness function) which will survive in the next generation, resulting in an evolution towards the “fittest” *genotype*. A classical example from the literature is a population of butterflies that evolves toward the colour that makes it harder to be spotted by predators.

GAs constitute a powerful optimization framework because of their relatively simple implementation and because, in general, they can provide near-optimal solutions in otherwise intractable optimization problems. Also, they can be applied to problems coming from different domains and extract local-optimal solutions even in very complex problems. Due to their nature, it is very common to find GAs in the resolution of constrained nonlinear optimization problems and, for this reason, they are a good candidate for our framework.

The three fundamental operations that most GAs implement are:

- *selection*, in which the candidates which return the largest values of the fitness function are selected, as in the "survival of the fittest" law of nature;
- *crossover*, whose aim is the recombination of the genetic information of the parents such that the offspring belonging to the new generation can inherit traits of both parents;
- *mutation*, whose purpose is to maintain diversity within the population. We induce a mutation to have a probability that the new chromosomes will have some of their genes randomly mutated after the crossover. Mutation is used to achieve a better exploration of the space of admissible solutions and to try to avoid local optima of low quality.

Each of the three operators can be customised depending on the problem peculiarities. For instance, the selection operator may be a simple "stochastic uniform selection", in which the probabilities of being selected depend on the attained fitness value, or a "tournament selection" procedure, as in our case, in which the algorithm selects the best element of a randomly chosen subset of the population, multiple times in a row, in order to form the set suitable for reproduction. Full implementation details on our solution will be given in the following section.

In the proposed framework, the security maximisation problem will be modeled as a large-scale binary optimisation problem, making the choice of standard Genetic Algorithms natural, as they were proven to be both efficient and effective in such scenarios [38]. It is worth noting that more refined solution that benefit from other optimisation domains, as fuzzy logic control systems [39]–[41] or neural networks [42] and network/scenario decompositions [43], may prove useful for particularly large scenarios or when dealing with security metrics characterised by a more complex mathematical structure than OSSTMM.

In the following section we are going to formulate the problem of optimal vulnerability management in an optimisation form that is compliant with the application of GAs.

III. Problem Formulation

The problem of security assessment is usually conducted by a certified security evaluator who follows a strict procedure, analysing and reporting on checklists and spreadsheets various characteristics and properties of the studied CPS.

In order to offer a Decision Support System, driven by an optimization solution, to the evaluators, the crucial requirements that the proposed algorithm should be able to meet should be identified. In general, whichever is the methodology selected for assessing the security level of the CPS, what the security evaluator seeks is a way to increase the measured value by an amount that it considers to be satisfactory for the needs of the client and also attainable with the available controls. Furthermore, the client may have several specifications to meet, as, for example, the maximum deployment cost of the new controls or the need of having a particular type of control device in place in order to meet a certification.

On the ground of these considerations, the optmization problem that is required to be solved assumes the following structure:

$$\begin{aligned} &\max_{x \in X} F(x) \\ &s.t. \\ &x \in S \cap D \end{aligned} \tag{1}$$

where $x \in X = \{0,1\}^N$ represents a decision vector formed by N binary variables indicating whether the corresponding available control is to be deployed or not; the cost function $F : X \to \mathbb{R}$ represents the selected metric for the security level assessment; S is the subset of X that contains all the security configurations that have a security level, for the selected metric, above the desired one, denoted with $desired\_level$; D is the set containing all the configurations that meet additional requirements that may be imposed by the client.

The vector x can be considered as the security configuration of our system, containing a complete description of controls already present in the system (whose corresponding variables are set to 1) along with the new controls which can be activated. X is then the set of all possible security configurations. Hereinafter, we will denote the i-th element of vector x with x_i and with $X^m \subset X$ the population at the m-th iteration. For the cost function $F(x)$, we selected in the study the Actual Security and True Protection metrics from OSSTMM - in general, it can be any of the quantities identified by OSSTMM or a compliant industrial standard. The set S is defined as

$$S = \{x \in X | F(x) \geq desired\_level\}.$$

Note that the inequality constraint in the definition of S shares the nonlinearity with the cost function. Finally, examples of additional requirements imposed by the client and included in the set D are listed below:

- a maximum number n_{max} of active controls, i.e., $x^T x \leq n_{max}$;
- the presence of at least a control from a specific set K, i.e., $\sum_{i \in K} x_i \geq 1$;
- the mutual exclusivity of two or more controls from a specific set H, i.e., $\sum_{i \in H} x_i \leq 1$;
- a maximum configuration cost C_{max}, i.e., $cost^T x < C_{max}$ in which $cost$ is the vector of the N costs of the corresponding controls.

Several other requirements can be included in the proposed framework, under the sole condition that they can be captured with a constraint that depends on the security configuration x.

Being the problem formulated so far an heavily constrained one, we decided to follow the approach presented in [44], that consists in modifying the cost function $F(x)$ so that it captures also the constraint violation of the various configurations x. The augmented cost function assumes the form:

$$F_m(x) = \begin{cases} F(x), & if x \in D \cap S \\ f_m^w + \sum_{j=1}^{L} D_j(x) & otherwise \end{cases}, \tag{2}$$

where $D_j(x)$ is an increasing penalty function related to the violation of the j-th constraint/requirement, L is the number of constraints, m is the current generation of the algorithm and

$$f_m^w = \begin{cases} \min_{x \in X^m \cap S \cap D} F(x), & if X^m \cap S \cap D \neq \emptyset \\ 0 & otherwise \end{cases}. \tag{3}$$

In other words, f_m^w represents the worst fitness value attained by the feasible configurations of generation m. The described approach reduces the probability of reproduction of the configurations that violate some constraints by penalising their fitness values.

The associated selection procedure is "Tournament Selection". The mutation rate follows a fixed probability of 2% for the switch of each component x_i of the configurations x. The crossover mixes the components of the parents, picking either of their values for x_i with equal probability. The parameters were tuned after several testings, but as a general consideration, it is desired to keep the mutation rate relatively high so that the exploration of the scenario, whose dimension is exponential in the number of available controls, is encouraged.

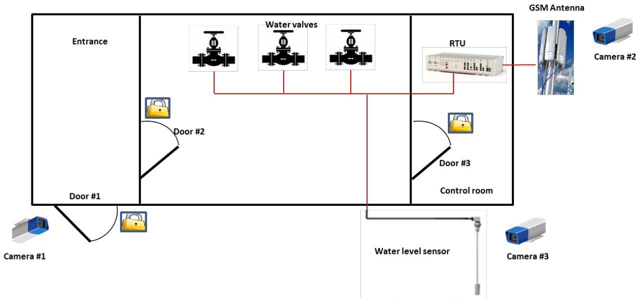

Fig. 1. First generation room, facility located at the dam.

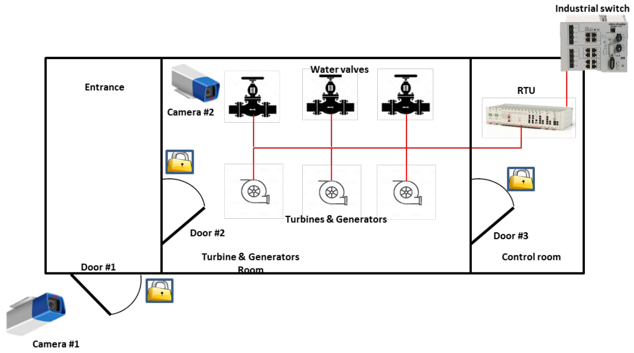

Fig. 2. Second generation room, turbine facility.

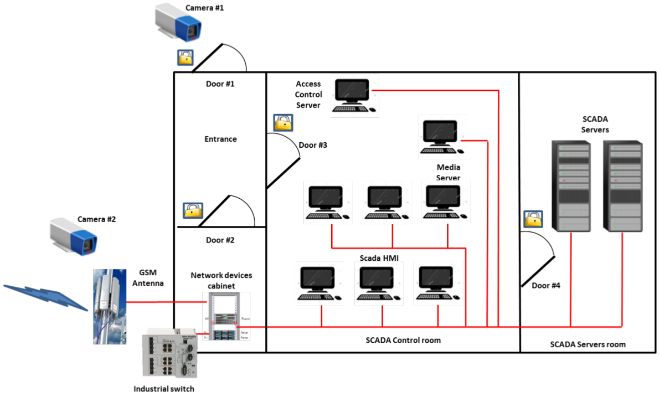

Fig. 3. Control room.

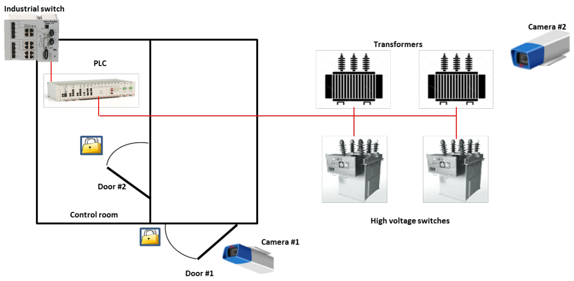

Fig. 4. Transformation System

IV. Reference Scenarios

In order to evaluate the performance of the proposed algorithm, we considered the scenario described in this section, defined by means of a questionnaire provided to a certified CC evaluator and his staff working in the ATENA project. The validation process starts by the modelling of the scenario in a form compliant with the proposed optimisation framework. In the second phase of the validation, the GA is tested on the model and its results are evaluated in both optimisation related performances (e.g., computational time, number of required generations, optimality of the solutions) and security aspects (e.g., level of security, exactness of the OSSTMM evaluation). The considered scenario is a simplified model of a Hydroelectric plant, described from the viewpoint of an evaluator for security assessment. We can divide such a system into four different subsystems:

- First generation room located at the dam;
- Second generation room located at the turbine facility;
- Control room;
- Transformation system.

In Figure 1, we report the first generation room we identified in a typical hydroelectric scenario, located near the dam that forms the water reservoir. In the generation room we can find a RTU controlling a set of valves and their sensors, needed to regulate the water flow into the turbines of the next generation room. The room is guarded by cameras, whereas all the communications between the RTU and the SCADA passes thought a GSM Antenna.

A similar setup is found for the second generation room, see Figure 2, where we find flow-controlling valves and the water turbines that produce electric power. This time, communications are supported by an industrial switch.

Figure 3 reports the control room, in which the SCADA servers are located. Here, we find several HMI positions for the operators, as well as the communication channels that connect the control centre with the other systems.

The last subsystem we considered is the transformation system, where the devices responsible for the power conversion are located. Once again, an RTU controls the transformers and the switches, that are located outside of the plant.

In Figure 5, the interconnected system is reported. In order to run the proposed GA algorithm on this scenario, we needed to provide a formal framework for its modelling, based on the representation depicted in Figure 6. Here, we modeled the assets that compose the various systems as blue squares, their interfaces as grey circles and their limitations and vulnerabilities as red triangles. The green hexagons represent the available controls that may be deployed, depending on the optimization outcome, whereas the yellow triangles represent the limitations that affect them.

V. Simulations

As mentioned in the introduction, we decided to validate the approach proposed by testing the proposed algorithm with the two OSSTMM indices "Actual Security" and "True Protection". The reader may find interest in the manual of the ATENA tool which implements the solutions presented in this paper and was used for the simulations, namely the Composer [45]. For the first two simulations we set a desired

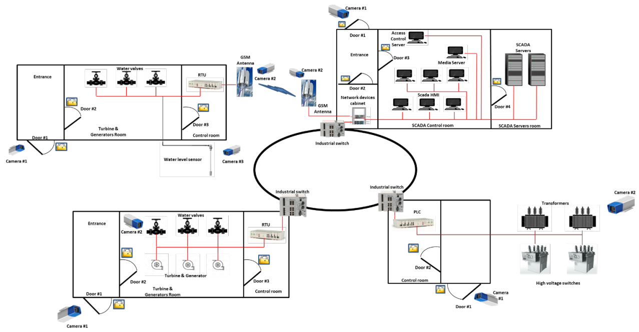

Fig. 5. Complete Hydroelectric system

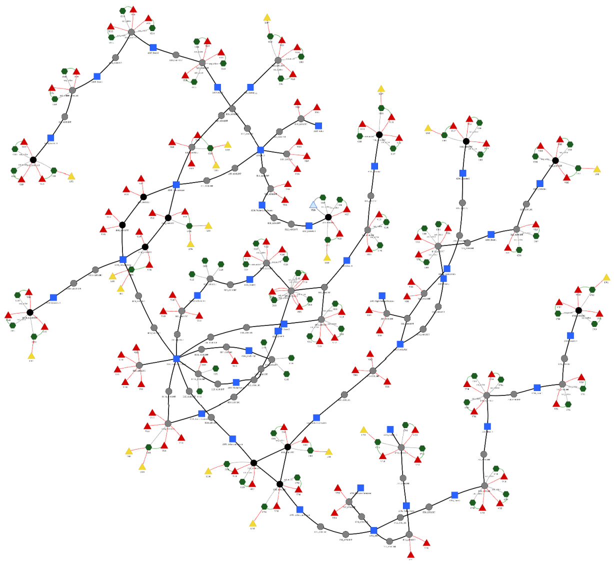

Fig. 6. Graph Model of the Complete Hydroelectric system

security level to 74.00, a value higher than the *starting score*, defined as the configuration with no additional controls (i.e., the one reported in Figure 6 without any of the green hexagons or yellow triangles active) but valuated as feasible by the security experts. In the following graphs, we report in blue lines the mean average value of the selected security indicator for the current generation and with the black lines the best value obtained by any configuration in the current generation.

In the first simulation, whose results are reported in Figure 7 and whose starting score for actual security was 72.76, we tested the algorithm on the generation system of Figure 1. We can observe how the actual security increases with generations, up to the point of having the mean value of the security level close to the best value. This condition usually happens when the algorithm finds a (local) minimum (hopefully close to the global one), as the final population collapses to similar values.

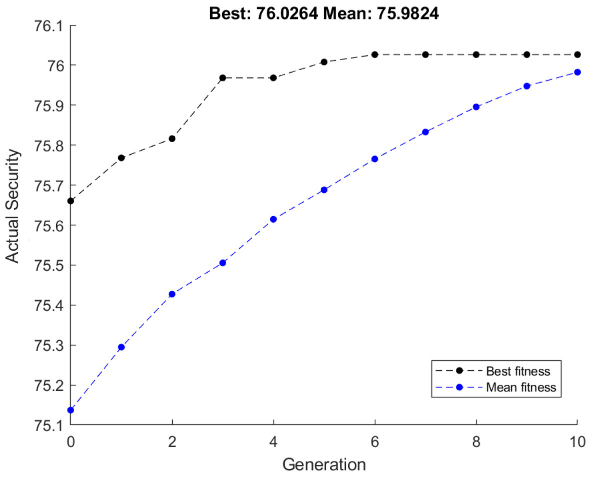

Fig. 7. Actual Security evolution, first simulation

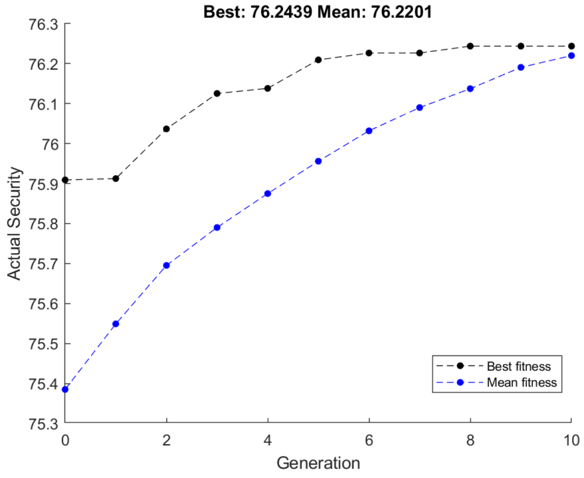

Fig. 8. Actual Security evolution, second simulation

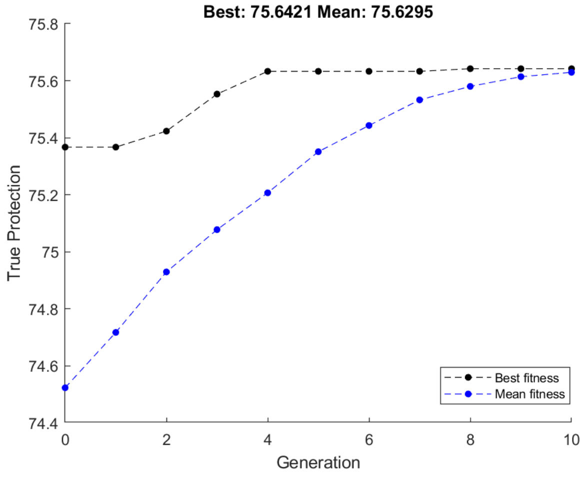

Fig. 9. True Protection evolution, second simulation

In the second simulation, we considered the complete system of Figure 5, for which the starting scores of initial Actual Security and True Protection levels were 64.94 and 61.31, respectively. The lower values with respect to the former case are due to the much higher imbalance between

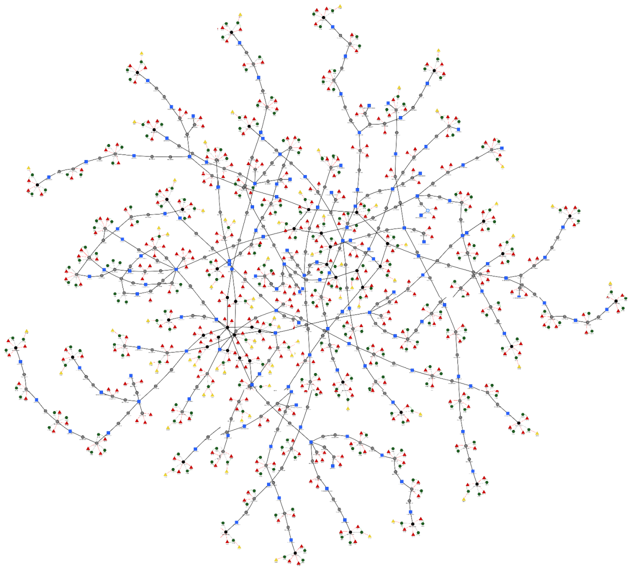

Fig. 10. 5x Hydroelectric scenario

vulnerabilities and (inactive) controls. However, as reported in Figures 8 and 9, after the optimization the system still attains results comparable with the previous simulation. It is interesting to notice how True Protection is slightly lower than Actual Security, due to the fact that it considers also the category, or type, of the implemented controls. The best performing configurations, in all cases, did not implement all the available controls due to the presence of limitations on the controls themselves; we also consider that the number of selected control would be even lower if considering their cost in the optimization.

For the final and third simulation we decided to test the scalability of the proposed approach. For the simulations reported so far, the generations required approximately 40s each on a 3GHz single core processor. We considered a scenario in which we connected 5 times the number of each subsystem, save for the control room. The scale of the scenario is reported in Figure 10. The starting score of True Protection in this case was 50.83, and we set a desired level of 61.00. Figure 11 shows that the optimization procedure still manages to handle such a scenario - with lower convergence speed. The desired security level is once again met very rapidly; each generation took less than 4 minutes, highlighting that, as an off-line controller, the proposed approach is suitable for the process of vulnerability management.

VI. Conclusions and Future Works

In this paper, we presented a solution for controlling the "security level", as defined in the industrial standard OSSTMM, of a CPS. We presented a framework based on genetic algorithms and validated the proposed approach on a scenario identified by real security evaluators. Simulations results proved the soundness of the approach as an off-line controller in a Decision Support System for security evaluators.

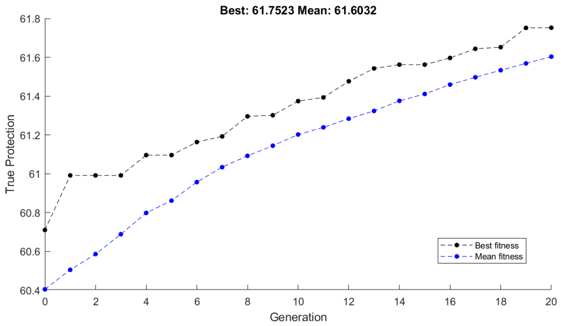

Fig. 11. 5x Hydroelectric scenario

A possible extension of the presented work would be covering more in detail and extending the utilised security metrics, as well as testing the approach over a more complete set of different scenarios coming from different sectors of the CPS. Scenarios in which the domain of application plays a more crucial role (e.g., power system in which power flow determines the degree of freedom of the available controls [13]) will also be explored, as the addition of physical-based constraints to the GA optimisation could lead to non-trivial aspects and concerns.

VII. Acknowledgements

The authors desire to acknowledge all the partners involved in the ATENA project and the CRAT team, in particular Professors F. Delli Priscoli, A. Pietrabissa, A. Di Giorgio and V. Suraci for their valuable contribution. Furthermore, the authors also acknowledge Pete Herzog, main developer of OSSTMM and co-founder of ISECOM, for his precious feedback.

References

[1] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: the next computing revolution," in *Design Automation Conference (DAC), 2010 47th ACM/IEEE*. IEEE, 2010, pp. 731–736.

[2] R. Baheti and H. Gill, "Cyber-physical systems," *The impact of control technology*, vol. 12, no. 1, pp. 161–166, 2011.

[3] J. Lee, B. Bagheri, and H.-A. Kao, "A cyber-physical systems architecture for industry 4.0-based manufacturing systems," *Manufacturing Letters*, vol. 3, pp. 18–23, 2015.

[4] Y. Zhang, M. Qiu, C.-W. Tsai, M. M. Hassan, and A. Alamri, "Health-cps: Healthcare cyber-physical system assisted by cloud and big data," *IEEE Systems Journal*, vol. 11, no. 1, pp. 88–95, 2017.

[5] C. Bruni, F. Delli Priscoli, G. Koch, A. Palo, and A. Pietrabissa, "Quality of experience provision in the future internet," *IEEE Systems Journal*, vol. 10, no. 1, pp. 302–312, March 2016.

[6] A. Pietrabissa, F. Delli Priscoli, A. Di Giorgio, A. Giuseppi, M. Panfili, and V. Suraci, "An approximate dynamic programming approach to resource management in multi-cloud scenarios," *International Journal of Control*, vol. 90, no. 3, pp. 492–503, 2017.

[7] F. Caldeira, M. Castrucci, M. Aubigny, D. Macone, E. Monteiro, F. Rente, P. Simões, and V. Suraci, "Secure mediation gateway architecture enabling the communication among critical infrastructures," in *2010 Future Network & Mobile Summit*. IEEE, 2010, pp. 1–8.

[8] S. Canale, A. Di Giorgio, F. Lisi, M. Panfili, L. R. Celsi, V. Suraci, and F. Delli Priscoli, "A future internet oriented user centric extended intelligent transportation system," in *2016 24th Mediterranean Conference on Control and Automation (MED)*. IEEE, 2016, pp. 1133–1139.

[9] S. Sridhar, A. Hahn, M. Govindarasu, *et al.*, "Cyber-physical system security for the electric power grid." *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2012.

[10] A. Di Giorgio, F. Liberati, R. Germanà, M. Presciuttini, L. R. Celsi, and F. Delli Priscoli, "On the control of energy storage systems for electric vehicles fast charging in service areas," in *2016 24th Mediterranean Conference on Control and Automation (MED)*. IEEE, 2016, pp. 955–960.

[11] D. Winter and B. P. Works, "Cyber physical systems-an aerospace industry perspective," *Boeing Management Company, Seattle, WA, USA*, 2008.

[12] T. Facchinetti and M. L. Della Vedova, "Real-time modeling for direct load control in cyber-physical power systems," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 689–698, 2011.

[13] A. Giuseppi, R. Germanà, and A. Di Giorgio, "Risk adverse virtual power plant control in unsecure power systems," in *2018 26th Mediterranean Conference on Control and Automation (MED)*. IEEE, 2018, pp. 1–9.

[14] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 6, pp. 1454–1467, June 2014.

[15] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, Nov 2013.

[16] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Computing Surveys (CSUR)*, vol. 46, no. 4, p. 55, 2014.

[17] A. Di Giorgio and F. Liberati, "A bayesian network-based approach to the critical infrastructure interdependencies analysis," *IEEE Systems Journal*, vol. 6, no. 3, pp. 510–519, 2012.

[18] ——, "Interdependency modeling and analysis of critical infrastructures based on dynamic bayesian networks," in *2011 19th Mediterranean Conference on Control & Automation (MED)*. IEEE, 2011, pp. 791–797.

[19] E. Lee, "The past, present and future of cyber-physical systems: A focus on models," *Sensors*, vol. 15, no. 3, pp. 4837–4869, 2015.

[20] P. Derler, E. A. Lee, and A. S. Vincentelli, "Modeling cyber–physical systems," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 13–28, Jan 2012.

[21] A. Fiaschetti, F. Lavorato, V. Suraci, A. Palo, A. Taglialatela, A. Morgagni, R. Baldelli, and F. Flammini, "On the use of semantic technologies to model and control security, privacy and dependability in complex systems," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2011, pp. 467–479.

[22] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry, *et al.*, "Challenges for securing cyber physical systems," in *Workshop on future directions in cyber-physical systems security*, vol. 5, 2009.

[23] G. Hug and J. A. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012.

[24] M. Mattioni, S. Monaco, and D. Normand-Cyrot, "Nonlinear discrete-time systems with delayed control: A reduction," *Systems & Control Letters*, vol. 114, pp. 31–37, 2018.

[25] A. Mercurio, A. Di Giorgio, and P. Cioci, "Open-source implementation of monitoring and controlling services for ems/scada systems by means of web services—iec 61850 and iec 61970 standards," *IEEE Transactions on Power Delivery*, vol. 24, no. 3, pp. 1148–1153, 2009.

[26] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, Nov 2011, pp. 4490–4494.

[27] F. Adamsky, M. Aubigny, F. Battisti, M. Carli, F. Cimorelli, T. Cruz, A. Di Giorgio, C. Foglietta, A. Galli, A. Giuseppi, *et al.*, "Integrated protection of industrial control systems from cyber-attacks: the atena approach," *International Journal of Critical Infrastructure Protection*, 2018.

[28] C. Foglietta, D. Masucci, C. Palazzo, R. Santini, S. Panzieri, L. Rosa, T. Cruz, and L. Lev, "From detecting cyber-attacks to mitigating risk within a hybrid environment," *IEEE Systems Journal*, pp. 1–12, 2018.

[29] V. Graveto, L. Rosa, T. Cruz, and P. Simões, "A stealth monitoring mechanism for cyber-physical systems," *International Journal of Critical Infrastructure Protection*, vol. 24, pp. 126 – 143, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874548218300672

[30] I. Frazão, P. Henriques Abreu, T. Cruz, H. Araujo, and P. Simoes, "Denial of service attacks: Detecting the frailties of machine learning algorithms in the classification process:," 12 2018, pp. 230–235.

[31] M. Panfili, A. Giuseppi, A. Fiaschetti, H. B. Al-Jibreen, A. Pietrabissa, and F. Delli Priscoli, "A game-theoretical approach to cyber-security of critical infrastructures based on multi-agent reinforcement learning," in *2018 26th Mediterranean Conference on Control and Automation (MED)*. IEEE, 2018, pp. 460–465.

[32] A. Fiaschetti, V. Suraci, and F. D. Priscoli, "The shield framework: How to control security, privacy and dependability in complex systems," in *2012 Complexity in Engineering (COMPENG). Proceedings*. IEEE, 2012, pp. 1–4.

[33] "Cvssv3.0," 2015. [Online]. Available: https://www.first.org/cvss/

[34] "CVE-2014-0160." 2013. [Online]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160

[35] "Common criteria v3.1. release 5," 2017. [Online]. Available: https://www.commoncriteriaportal.org

[36] ISECOM, "Osstmm 3 - the open source security testing methodology manual (2010)."

[37] Y. Xi, T. Chai, and W. Yun, "Survey on genetic algorithm," *Control theory and applications*, vol. 13, no. 6, pp. 697–708, 1996.

[38] M. Srinivas and L. M. Patnaik, "Genetic algorithms: A survey," *computer*, vol. 27, no. 6, pp. 17–26, 1994.

[39] F. Valdez, P. Melin, and O. Castillo, "An improved evolutionary method with fuzzy logic for combining particle swarm optimization and genetic algorithms," *Appl. Soft Comput.*, vol. 11, no. 2, pp. 2625–2632, Mar. 2011. [Online]. Available: http://dx.doi.org/10.1016/j.asoc.2010.10.010

[40] R.-C. David, R.-E. Precup, E. M. Petriu, M.-B. Rădac, and S. Preitl, "Gravitational search algorithm-based design of fuzzy control systems with a reduced parametric sensitivity," *Information Sciences*, vol. 247, pp. 154 – 173, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025513004222

[41] S. Vrkalovic, E.-C. Lunca, and I.-D. Borlea, "Model-free sliding mode and fuzzy controllers for reverse osmosis desalination plants," *Int. J. Artif. Intell*, vol. 16, no. 2, pp. 208–222, 2018.

[42] J. Saadat, P. Moallem, and H. Koofigar, "Training echo state neural network using harmony search algorithm," *Int. J. Artif. Intell*, vol. 15, no. 1, pp. 163–179, 2017.

[43] C. Bruni, F. Delli Priscoli, G. Koch, A. Pietrabissa, and L. Pimpinella, "Network decomposition and multi-path routing optimal control," *Transactions on Emerging Telecommunications Technologies*, vol. 24, no. 2, pp. 154–165, 2013.

[44] K. Deb, "An efficient constraint handling method for genetic algorithms," *Computer methods in applied mechanics and engineering*, vol. 186, no. 2-4, pp. 311–338, 2000.

[45] [Online]. Available: https://www.atena-h2020.eu/wp-content/uploads/2019/04/Composer-User-Manual_v1.1_CRAT.pdf