Simulation-Based Goal Tree Success Tree for the Risk Analysis of Cyber-Physical Systems

Francesco Di Maio
Department of Energy, Politecnico di Milano, Via La Masa 34, 20156 Milano, Italy. E-mail: francesco.dimaio@polimi.it

Roberto Mascherona
Aramis Srl, Milano 20121, Italy

Wei Wang
Department of Energy, Politecnico di Milano, Via La Masa 34, 20156 Milano, Italy. E-mail: wei.wang@polimi.it

Enrico Zio
Department of Energy, Politecnico di Milano, Via La Masa 34, 20156 Milano, Italy
Aramis Srl, Milano 20121, Italy
MINES ParisTech / PSL Université Paris, Centre de Recherche sur les Risques et les Crises (CRC), Sophia Antipolis, France
Eminent Scholar, Department of Nuclear Engineering, Kyung Hee University
E-mail: enrico.zio@polimi.it

Cyber-Physical Systems (CPSs) can be subjected to random failures of hardware components and to intentional breaches in cyber components. In a previous paper, the authors have proposed the Goal Tree Success Tree Master Logic Diagram (GTST-MLD) as a framework to jointly treat these aspects in the risk analysis of CPSs. In this work, a simulation-based method is proposed to assign the values of the weights of the GTST-MLD.
An application is carried out considering the digital Instrumentation and Control (I&C) system of the Advanced Lead-cooled Fast Reactor European Demonstrator (ALFRED)). A number of simulations are run for different types of cyber attacks at random times and magnitudes, and the critical parameters of different failure scenarios are collected, and properly manipulated to estimate the weights of the GTST-MLD.

Keywords: Risk analysis, Cyber-Physical System, Goal Tree Success Tree Master Logic Diagram, weights inference, simulation, Advanced Lead-cooled Fast Reactor European Demonstrator.

1. Introduction

Safety typically concerns stochastic components failures and human actions that can result in accidental scenarios leading the system towards unacceptable consequences, whereas, security concerns malicious and intentional attacks that can impair both the physical and cyber parts of the system, and lead to unacceptable consequences.

Extensive use of digital technologies for systems Instrumentation and Control (I&C) has led to highly connected and remotely controlled Cyber-Physical Systems (CPSs) (Shin, Son, Ur, & Heo, 2015; Zio, 2016, 2018). The connected infrastructures allow for an improved CPSs controllability but can introduce vulnerabilities i.e., weaknesses which can be exploited by skilled and willing attackers to breach all devised security measures (Cho, Chung, & Kuo, 2018; Wang et al., 2018; Zio, 2016). Thus, to evaluate the risk of CPSs, the risk analysis must address both safety and security issues, because not only failures of hardware and software can cause damages and harms, but also cyber attacks can breach the CPS security and lead to serious consequences (Kriaa, Pietre-Cambacedes, Bouissou, & Halgand, 2015).

To this aim, a Goal Tree Success Tree Master Logic Diagram (GTST-MLD) framework has been proposed by the authors to jointly treat safety and security aspects in the risk analysis of CPSs, allowing effectively modeling interdependencies between CPS components and managing the scarcity of information related to cyber security threats (Di Maio, Mascherona, & Zio, 2018). The illustration on a chemical CPS case study shows the expected modelling benefits by use of the GTST-MLD (Di Maio et al., 2018). In this latter GTST-MLD version, weights assignment is expert dependent. To gain

Proceedings of the 29th European Safety and Reliability Conference.
Edited by Michael Beer and Enrico Zio
 Published by Research Publishing, Singapore
ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0 esrel2019-paper

realism in the modeling, efforts must be made to collect experimental data on threats and vulnerabilities, develop more complete and detailed databases of security incidents, or define a method for assigning weights integrating the heterogeneous sources of knowledge, information and data, as proposed in this work, by developing a simulation method for assessing weights based on physical models mimicking the CPS behavior under attacks. For example, cyber attacks aiming at damaging different components of the CPSs have been explored by Monte Carlo (MC) simulation (Wang et al., 2018).

In this sense, we develop a simulation-based inference method for setting the weights of the GTST-MLD that is used to perform the risk analysis of a CPS. An approach is originally undertaken, based on Order Statistics (OS) (Nutt & Wallis, 2004; Wilks, 1941, 1942), for estimating probabilistically the GTST-MLD weights.

Without loss of generality and for demonstration purposes, we present the application of the approach on a nuclear CPS, specifically, the digital I&C system of the Advanced Lead-cooled Fast Reactor European Demonstrator (ALFRED)) (Frogheri et al., 2013), whose previously developed object-oriented DYMOLA simulator with a multi-loop PI control scheme is utilized (Ponciroli et al., 2014). Simulations are run for different types of cyber attacks at random times and magnitudes, and the critical parameters evolution of different scenarios are collected and used for estimation of the GTST-MLD weights by OS.

The reminder of the paper is organized as follows. Section 2 presents the main characteristics of the ALFRED reactor, with its control scheme at full power nominal conditions, and the MC engine of cyber breaches generating cyber attack scenarios. In Section 3, the GTST-MLD weights are quantified by OS with respect to different failure modes and fed into the GTST-MLD model developed for the ALFRED control system. Results of the case study are presented in Section 4. In Section 5, conclusions are drawn.

2. ALFRED

2.1 System description

ALFRED is a small-size (300 MW) pool-type fast reactor, cooled by molten lead (Frogheri et al., 2013). At full power nominal conditions, the dynamic process of the ALFRED primary and secondary cooling systems is controlled by both feedforward and PI (Proportional and Integral) SISO (Single Input Single Output) feedback control schemes (Ponciroli et al., 2014). This control process is supervised by a Supervisory Control and Data Acquisition (SCADA) system (which collects the information and makes them available to the site managers) (Figure 1).

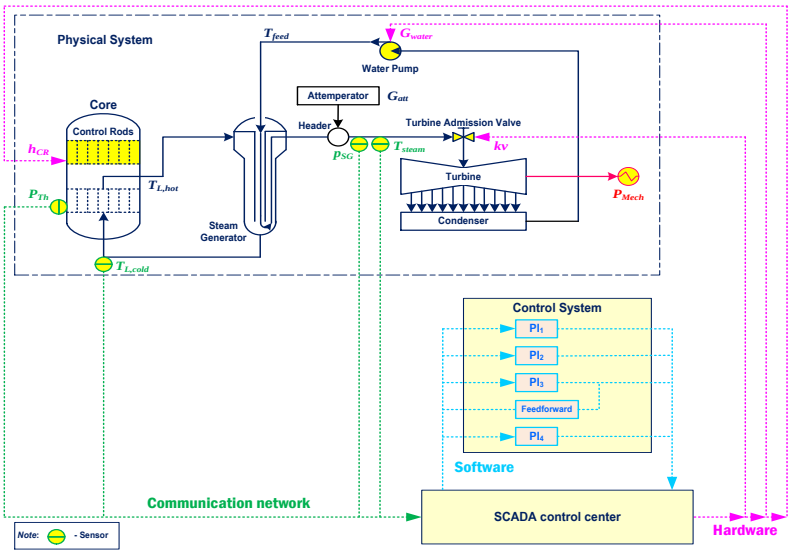

Figure 1. ALFRED reactor control system

The control aims at keeping the controlled variables (steam temperature T_{steam}, SG pressure p_{SG}, cold leg lead temperature $T_{L,cold}$ and thermal power P_{Th}) approximately at the steady state values, for outputting a mechanical power P_{mech}. The values y_{ref} shown in Table 1 are the optimal setting of the controlled variables at full power nominal condition. Each variable y is kept above (and below) the safety threshold L_y (and U_y), to ensure safe NPP operation conditions. For example, the $T_{L,cold}$ must be kept above 350°C to avoid the embrittlement of the structural materials in aggressive environments enhanced by fast neutron irradiation.

Table 1 Safety thresholds of critical variables

Variable, y	Reference value at full power nominal condition y_{ref}	Lower safety threshold (L_y)	Upper safety Threshold (U_y)
T_{steam} (°C)	450	/	550
p_{SG} (Pa)	180E5	170E5	190E5
$T_{L,cold}$ (°C)	400	350	/
P_{Th} (W)	300E6	270E6	330E6

2.2 The MC engine of cyber breaches injection

To test the effects of cyber attacks on system functionality and collect the critical parameters evolution under a generic *j*-th accidental scenario a_j, a MC engine is integrated with the ALFRED model for injecting cyber breaches at random times and magnitudes (see (Wang, Cammi, et al., 2018)). In particular, attacks are foreseen to occur on:

(i) Sensors measuring $T_{steam}, p_{SG}, T_{L,cold}$ and P_{Th}: in this case, four types of cyber attacks preventing the controllers from receiving legitimate measurements (equivalent to typical Denial of Service (DoS) attacks) are simulated to occur at a random time t_R, namely: (a_1) bias, (a_2) drift, (a_3) wider noise and (a_4) freezing, all mimicking stochastic failures (Boskvic & Mehra, 2002).

(ii) Actuators: in this case, malicious attacks consist in forcing the actuators to fail stuck to a random magnitude of actuation $A(t)$, namely: (a_5) control rods that regulate the rod heights h_{CR}, (a_6) water pump that regulates the feedwater mass flow rate G_{water} and (a_7) turbine admission valve *kv* that regulates the steam inlet mass flow rate.

(iii) PI controllers: in this case, cyber attacks can be considered equivalent to a deception attack maliciously injecting a false message to the controller, PI gains, namely, (a_8) K_p and (a_9) K_i) and (a_{10}) controlled variables set points $y_{set,ref}$ are randomly sampled from uniform distributions.

3. GTST-MLD for ALFRED

In Section 3.1, the GTST-MLD for the risk assessment of the multi-loop ALFRED control system that can fail due to both stochastic failures of its components and cyber attacks is introduced. In Section 3.2, a simulation-based inference method is originally proposed for setting the weights of the GTST-MLD model.

3.1 GTST-MLD structure

The GTST-MLD of Figure 2 has been developed for the ALFRED control system, whose four SISO control loops assolve the n_f sub-functions in the Goal Tree (GT): T_{steam} control $(f = 1)$, p_{SG} control $(f = 2)$, $T_{L,cold}$ control $(f = 3)$ and P_{Th} control $(f = 4)$. For each control loop, the respective n_c main components C_c are represented in the Success Tree (ST) (Modarres & Cheon, 1999):

- Steam temperature control loop: the sensor measuring steam temperature ($c = 1$) and the PI_1 controller ($c = 2$);
- Steam Generator (SG) pressure control loop: the sensor measuring SG pressure ($c = 3$), the PI_2 controller ($c = 4$) and the turbine admission valve actuator ($c = 5$);
- Cold leg lead temperature control loop: the sensor measuring cold leg lead temperature ($c = 6$), the PI_3 controller ($c = 7$) and the water pump actuator ($c = 8$);
- Thermal power control loop: the sensor measuring thermal power ($c = 9$), the PI_4 controller ($c = 10$) and the control rod actuator ($c = 11$).

The relationships between GT functions and ST main components are represented in a compact and transparent way by the Master Logic Diagram (MLD) (Hu & Modarres, 1999; Papazoglou & Aneziris, 2003). As shown in

Proceedings of the 29th European Safety and Reliability Conference.
Edited by Michael Beer and Enrico Zio
 Published by Research Publishing, Singapore
ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0 esrel2019-paper

Figure 2, MLD maps the influences among functions and components into a matrix CF (diamonds) whose values $CF_{c,f}$ are the strengths of the relationships between the c-th component and the f-th functions and are typically assigned by expert judgment.

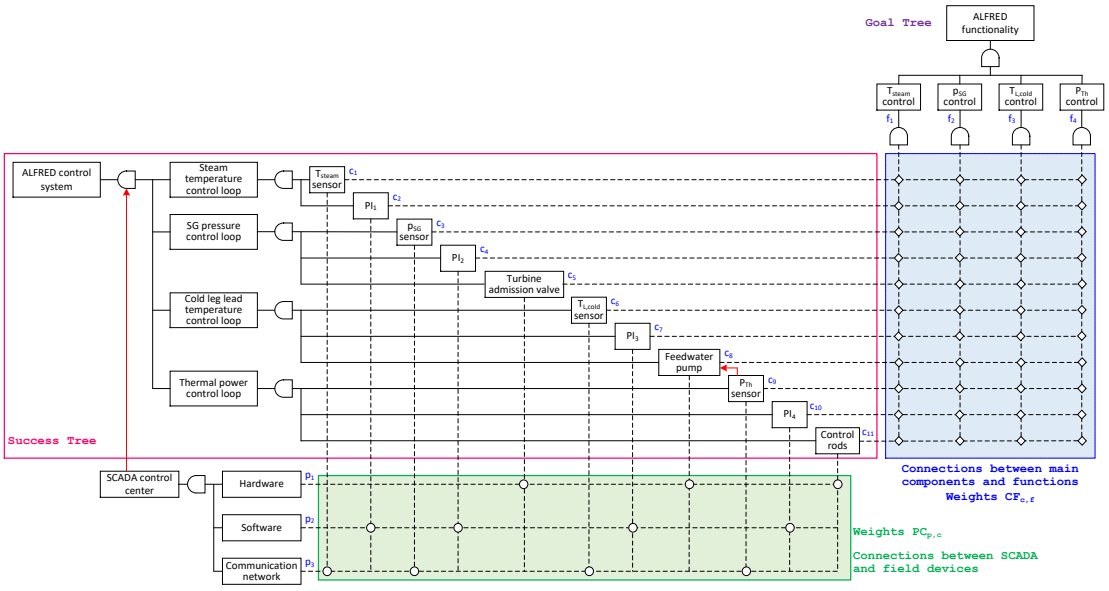

Figure 2. The GTST-MLD model for ALFRED

The SCADA system (which supports and supervises the control of the critical parameters, but it is not physically embedded in the control system) is decomposed in n_p supporting components: hardware ($p = 1$), software ($p = 2$) and communication network ($p = 3$). As it can be seen in Figure 1, the communication network has the task of delivering the sensor measurements to the control center, the software manages the Programmable Logic Controllers (PLCs) and the hardware supervises the actuator action. Then, the connections between main and support components are also mapped into a MLD matrix, hereafter called PC (dots in Figure 2), whose values $PC_{p,c}$ are the strengths of the relationships between the p-th support components and the c-th main components, as (typically) assigned by expert judgment as shown in Appendix A.

Then, Influencing Factors (IFs) $D_d, d = 1, \dots, n_d$ are identified as the dysfunctional aspects that can prevent the system from achieving the goal function. The GTST-MLD here proposed originally distinguishes safety-related IFs ($D_{d_{safety}}$, $d_{safety} = 1, \dots, n_{d_{safety}}$), that refer to stochastic failures of sensors, actuators and PIs, from security-related IFs ($D_{d_{security}}$, $d_{security} = 1, \dots, n_{d_{security}}$), that refer to different cyber malicious attacks that may affect the system functionality. The $n_{d_{safety}}$ safety-related IFs directly affect the n_c main components state, whereas the $n_{d_{security}}$ security-related IFs, affecting the SCADA functionality, relate to the n_p supporting components. IFs can impair both the n_c main components and the n_p supporting components that, finally, affect the n_f functions. MLD maps the connections between the $n_{d_{safety}}$ IFs and the n_c main components by weights $DC_{d_{safety},c}$, and the connections between the $n_{d_{security}}$ IFs and the n_p supporting components by weights $DP_{d_{security},p}$, again, typically assigned by expert judgment as shown in Appendix B.

Considering the AND/OR gates that define the relationships among functions and the top goal function, setting a CPS mission time T_{miss} and a simulation step dt, the probability of the top goal "fulfillment of the ALFRED functionality" $P[G]$ can be calculated, and, correspondingly, the system unreliability F_{GTST}

(the interested reader may refer to (Di Maio et al., 2018; Ferrario & Zio, 2014)):

$$F_{GTST}(t) = 1 - P[G](t) \quad (1)$$

3.2 Simulation-based inference method for setting the weights $CF_{c,f}$

To overcome the subjectivity of expert judgment in assigning the weights $CF_{c,f}$ of the GTST-MLD, in this Section, a simulation-based inference method is originally proposed. The rationale is that $CF_{c,f}$ can be defined as the probability that the *c*-th main component failure induces the *f*-th function unfulfillment, $CF_{c,f} = \Pr(f = 0|c = 0)$. The method starts by considering any *j*-th accidental scenario a_j among those described in Section 2.2 and simulates it *N* times over the mission time T_{miss}, for collecting the corresponding maximum and minimum values of the critical safety parameter *y* ($y_{max,a}$ and $y_{min,a}$, respectively). Then, the estimates $\hat{y}^{\gamma,\beta}_{max,a}$ and $\hat{y}^{\gamma,\beta}_{min,a}$ of $y^{\gamma}_{max,a}$ and $y^{\gamma}_{min,a}$, respectively, the (true) γ-percentile of the distributions of $y_{max,a}$ and $y_{min,a}$, can be calculated with confidence β (Lehmann & Casella, 2006), viz:

$$\gamma = \Pr(y_{max,a_j} < y^{\gamma}_{max,a_j}) \text{ or } \gamma = \Pr(y_{min,a_j} < y^{\gamma}_{min,a_j}) \quad (2)$$

$$\beta = \Pr(y^{\gamma}_{max,a_j} < \hat{y}^{\gamma,\beta}_{max,a_j}) \text{ or } \beta = \Pr(y^{\gamma}_{min,a_j} > \hat{y}^{\gamma,\beta}_{min,a_j}) \quad (3)$$

The value $\hat{y}^{\gamma,\beta}_{max,a_j}$ (or $\hat{y}^{\gamma,\beta}_{min,a_j}$) can be estimated by a Bracketing Order Statistics (OS) approach (Nutt & Wallis, 2004), which guarantees that the first element (out of *N*) in the descending (ascending, for $\hat{y}^{\gamma,\beta}_{min,a_j}$) sorted sample y^1_{max,a_j} (y^1_{min,a_j}) has a certain probability β of exceeding (subceeding) the unknown true γ-percentile. The number *N* can be calculated with γ and β selected by the analyst as in Eq. (4) (Nutt & Wallis, 2004):

$$\beta = 1 - \gamma^N \quad (4)$$

Finally, if the distribution of y_{max,a_j} (or y_{min,a_j}) is assumed to be a Gaussian $N\left(\mu_{y_{max,a_j}}, \sigma_{y_{max,a_j}}\right)$, with its mean and standard deviation values calculated as in Eqs. (5) and (6):

$$\mu_{y_{max,a_j}} = \frac{\sum_{i=1}^{N} y^i_{max,a_j}}{N} \quad (5)$$

$$\sigma_{y_{max,a_j}} = \frac{\hat{y}^{\gamma,\beta}_{max,a_j} - \mu_{y_{max,a_j}}}{\sqrt{2}\psi^{-1}(2\gamma - 1)} \quad (6)$$

where,

$$\psi(x) = erf(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-\mu^2} d\mu \quad (7)$$

With respect to a specific failure scenario a_j, the value of $CF^{a_j}_{c,f}$ can be taken equal to the probability that the distribution of y_{max,a_j} (or y_{min,a_j}) overcomes the upper (or lower) safety threshold U_y (or L_y) (i.e., the *c*-th component induces the *f*-th function unfulfillment):

$$CF^{a_j,N}_{c,f} = \Pr\left(y_{max,a_j} > U_y\right) = 1 - F_U(y_{max,a_j}) \quad (8)$$

In practice, since the *c*-th main component can be subjected to multiple attack scenarios (e.g., a_1, a_2, a_3 and a_4 for the *c*-th sensor, a_8, a_9 and a_{10} for the *c*-th PI controller of ALFRED in Section 2.2), we calculate $\Pr\left(y_{max,a_j} > U_y\right)$ and/or $\Pr\left(y_{min,a_j} < L_y\right)$ for each scenarios a_j, and consequently set:

$$CF^{N}_{c,f} = \arg\max_{a_j} CF^{a_j,N}_{c,f} \quad (9)$$

It is worth mentioning that if we fix β and select different batches of *N* simulations, the lower $CF^{L}_{c,f}$ and upper $CF^{U}_{c,f}$ bound of $CF_{c,f}$ can be found as in Eqs. (10) and (11) below:

$$CF^{U}_{c,f} = \arg\max_{N} CF^{N}_{c,f} \quad (10)$$

$$CF^{L}_{c,f} = \arg\min_{N} CF^{N}_{c,f} \quad (11)$$

where, $CF^{N}_{c,f}$ are found with different β values, leading to different *N*.

4. Results

As discussed in Section 2.2, the estimation of the γ-th percentile of y_{max,a_j} (or y_{min,a_j}) (i.e., weight bounds of $CF_{c,f}$) by resorting to OS (see Eq. (4)) for each type of cyber attack scenario *a*, where $a = a_1, a_2, \ldots, a_{10}$, proceeds by fixing β equal to 0.9 as in (Wang, Cammi, et al., 2018) and alternatively setting *N*=30, 29, 28, 27, 25, 22, 20 and 15. Results are listed in Table 2.

Considering a three-level risk metric (low [0.0, 0.2), medium [0.2, 0.8), high [0.8, 1.0]) (as traditionally done in (Wang, Cammi, et al., 2018)) for ranking the strengths of the weights estimates, the most vulnerable function is

P_{Th} $(f = 4)$ control, followed by p_{SG} $(f = 2)$ control and T_{steam} $(f = 1)$ control (shadowed $CF_{c,f}$ in Table 2).

Table 2. Weights $CF_{c,f}$ between main components and functions considering uncertainties

$CF_{c,f}$	$f = 1$	$f = 2$	$f = 3$	$f = 4$
$c = 1$	0	0	[0, 6.03E-265]	0
$c = 2$	0	[0.70, 0.85]	[1.06E-30, 4.95E-22]	[5.77E-45, 4.39E-23]
$c = 3$	[0.26, 0.37]	[0.63, 0.72]	[1.54E-5, 2.20E-3]	[0.12, 0.15]
$c = 4$	0	[0.46, 0.51]	[0.02, 0.07]	[0.74, 0.88]
$c = 5$	0	0	[0, 1.69E-307]	0
$c = 6$	0	[0.09, 0.18]	[0, 3.09E-258]	0
$c = 7$	[6.36E-8, 6.12E-5]	[1.95E-17, 2.05E-12]	[2.23E-5, 8.66E-4]	[3.39E-6, 5.10E-4]
$c = 8$	0	0	0	[2.50E-3, 0.02]
$c = 9$	[0.05, 0.21]	[0.62, 0.73]	[1.05E-14, 1.55E-8]	[0.90, 0.98]
$c = 10$	[0.40, 0.44]	[0.31, 0.34]	[3.08E-5, 1.10E-3]	[0.42, 0.45]
$c = 11$	[6.17E-8, 0.07]	[0.52, 0.59]	[0, 4.91E-22]	[0.01, 0.08]

Results of Table 2 can be useful to propagate the uncertainty on $CF_{c,f}$ to the system ALFRED uncertainty (see (Di Maio, Mascherona, & Zio, 2018)) within the GTST-MLD: the lower and upper bounds of the ALFRED uncertainty (shadowed area in Figure 3) result from a MC simulation scheme that enables propagating uncertainties to the ALFRED unreliability estimates.

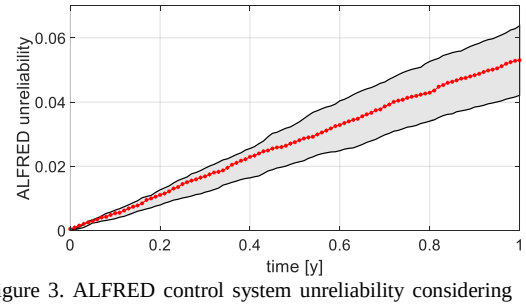

Figure 3. ALFRED control system unreliability considering uncertainties (shadowed area) and average unreliability (star-line) obtained by feeding the GTST-MLD model with the mean values of the intervals of $CF_{c,f}$ of Table 2

Figure 4 shows the bounded probabilities of unfulfillment for $f = 1, 2, 3$ and 4 functions, respectively. We can see that p_{SG} $(f = 2)$ control (see Figure 4(b)) and P_{Th} $(f = 4)$ control (see Figure 4(d)) at the mission time T_{miss} = 1 year, turn out to be equal to 0.0452 and 0.0449, respectively. These values are much larger than those of T_{steam} $(f = 1)$ control (see Figure 4(a)) and $T_{L,cold}$ $(f = 3)$ control (see Figure 4(d)) (equal to 0.0148 and 0.6E-3, respectively). This means that, on one side, the main components failures are more likely to have adverse impacts on the p_{SG} $(f = 2)$ control and P_{Th} $(f = 4)$ control fulfillments, as already pointed out; on the other side, this points out that the simulation-based method for assigning weights allows, not only limits the subjective and expert-dependent nature of weights, but also plays an important role in prioritizing the most vulnerable functions to cyber attacks, which can inform the analysts on possible mitigation strategies.

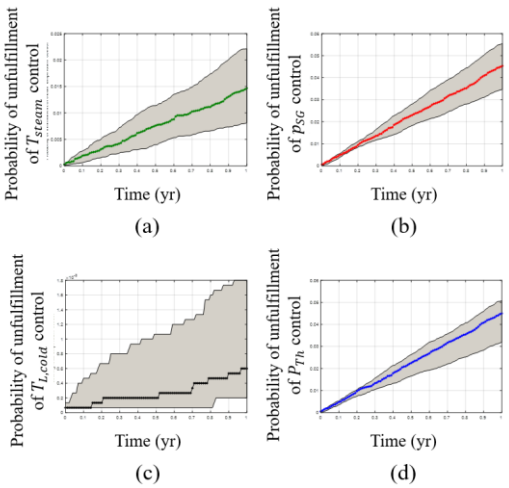

Figure 4. ALFRED control system sub-functions fulfillment: bounded probabilities of unfulfillment of (a) T_{steam} $(f = 1)$ control; (b) p_{SG} $(f = 2)$ control; (c) $T_{L,cold}$ $(f = 3)$ control; and (d) P_{Th} $(f = 4)$ control

5. Conclusions

In this work, we have proposed a simulation-based inference method for assigning the weights of a Goal Tree Success Tree Master Logic Diagram (GTST-MLD) framework, when performing the risk analysis of Cyber-Physical Systems (CPSs) jointly treating safety and security aspects. An approach based on the Order Statistics (OS) has been originally undertaken for

restructuring the parameters distributions and assigning the GTST-MLD weights.

We have taken the multi-loop control system of the Advanced Lead-cooled Fast Reactor European Demonstrator (ALFRED) as case study, in which cyber breach events aiming at attacking the embedded CPS components are injected by a Monte Carlo sampling procedure, at random times and of random magnitudes. The results also show that the method allows identifying the main components failures which are more likely to have adverse impacts on the p_{SG} $(f = 2)$ control and P_{Th} $(f = 4)$ control fulfillments.

Appendix A MLD Matrix of $PC_{p,c}$

The weights $PC_{p,c}$, between support and main components, of the MLD are shown in Table A.1 and assigned by expert opinion.

Table A.1. Weights between support and main components

$PC_{p,c}$	Sensors ($c = 1,3,6,9$)	PIs ($c = 2,4,7,10$)	Actuators ($c = 5,8,11$)
$p = 1$	Low(=0)	Low(=0)	High (=1)
$p = 2$	Low(=0)	High (=1)	Low(=0)
$p = 3$	High (=1)	Low(=0)	Low(=0)

Appendix B MLD Matrixes for $DC_{d_{safety},c}$ and $DP_{d_{security},p}$

Safety-related IFs $n_{d_{safety}}$ (stochastic failures of sensors, PIs and actuators) are identified for the *c*-th main components with historical failure rates. Weights $DC_{d_{safety},c}$ between IFs and main components are all set, by expert judgment, to "High" (equal to 1) because directly and strongly impacting on the component availability, irrespectively of the failure mode. For example, a sensor freezing, once verified, necessarily produces the sensor functional failure, as well as any other failure mode.

On the other side, the weights $DP_{d_{security},p}$ between security-related IFs $n_{d_{security}}$ and support components are shown in Table B.1, derived from the expert-assessed vulnerability levels.

Table B.1. Weights between security-related IFs and support component

$DP_{d,p}$, d=	$p = 1$	$p = 2$	$p = 3$
Key logger	/	/	High [0.75,1.00]
Message spoofing	/	/	Medium [0.25,0.75]
Replay	/	/	Medium [0.25,0.75]
Man in the middle	/	/	Medium [0.25,0.75]
Denial of service	/	/	High [0.75,1.00]
Buffer overflow	/	Medium [0.25,0.75]	/
SQL injection	/	Medium [0.25,0.75]	/
STUXNET	/	High [0.75,1.00]	/
Doorknob rattling	High [0.75,1.00]	/	/

Reference

Boskvic, J. D., & Mehra, R. K. (2002). Stable adaptive multiple model-based control design for accommodation of sensor failures. *3*, 2046-2051 vol.2043.

Cho, C.-S., Chung, W.-H., & Kuo, S.-Y. (2018). Using Tree-Based Approaches to Analyze Dependability and Security on I&C Systems in Safety-Critical Systems. *IEEE Systems Journal, 12*(2), 1118-1128.

Di Maio, F., Mascherona, R., & Zio, E. (2018). Goal-oriented risk analysis of cyber-physical systems. *IEEE Systems Journal*.

Ferrario, E., & Zio, E. (2014). Goal Tree Success Tree–Dynamic Master Logic Diagram and Monte Carlo simulation for the safety and resilience assessment of a multistate system of systems. *Engineering Structures, 59*, 411-433.

Frogheri, M., Alemberti, A., & Mansani, L. (2013). *The Lead Fast Reactor: Demonstrator (ALFRED) And ELFR Design.* Paper presented at the International Conference on FAST Reactors and Related Fuel Cycles: Safe Technologies and Sustainable Scenarios.

Hu, Y.-S., & Modarres, M. (1999). Evaluating system behavior through dynamic master logic diagram (DMLD) modeling. *Reliability Engineering & System Safety, 64*(2), 241-269.

Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., & Halgand, Y. (2015). A survey of approaches combining safety and security for industrial control systems. *Reliability Engineering & System Safety, 139*, 156-178.

Lehmann, E. L., & Casella, G. (2006). *Theory of point estimation*: Springer Science & Business Media.

Modarres, M., & Cheon, S. W. (1999). Function-centered modeling of engineering systems using

the goal tree–success tree technique and functional primitives. *Reliability Engineering & System Safety, 64*(2), 181-200.

Nutt, W. T., & Wallis, G. B. (2004). Evaluation of nuclear safety from the outputs of computer codes in the presence of uncertainties. *Reliability Engineering & System Safety, 83*(1), 57-77.

Papazoglou, I., & Aneziris, O. (2003). Master Logic Diagram: method for hazard and initiating event identification in process plants. *Journal of hazardous materials, 97*(1-3), 11-30.

Ponciroli, R., Bigoni, A., Cammi, A., Lorenzi, S., & Luzzi, L. (2014). Object-oriented modelling and simulation for the ALFRED dynamics. *Progress in Nuclear Energy, 71*(71), 15-29.

Shin, J., Son, H., Ur, R. K., & Heo, G. (2015). Development of a cyber security risk model using Bayesian networks. *Reliability Engineering & System Safety, 134*(134), 208-217.

Wang, W., Cammi, A., Di Maio, F., Lorenzi, S., & Zio, E. (2018). A Monte Carlo-based exploration framework for identifying components vulnerable to cyber threats in nuclear power plants. *Reliability Engineering & System Safety, 175*, 24-37.

Wilks, S. S. (1941). Determination of sample sizes for setting tolerance limits. *The Annals of Mathematical Statistics, 12*(1), 91-96.

Wilks, S. S. (1942). Statistical prediction with special reference to the problem of tolerance limits. *The Annals of Mathematical Statistics, 13*(4), 400-409.

Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety, 152*, 137-150.

Zio, E. (2018). The future of risk assessment. *Reliability Engineering & System Safety, 177*, 176-190.