Risk analysis of cyber-physical systems by GTST-MLD

Francesco Di Maio, *Senior Member, IEEE*, Roberto Mascherona, Enrico Zio, *Senior Member, IEEE*

***Abstract*— Cyber-Physical Systems (CPSs) must consider both components failures and cyber threats. In this work, we propose the Goal Tree Success Tree Master Logic Diagram (GTST-MLD) to analyze these within the same framework. The benchmark with a conventional Attack Tree (AT) - Bow Tie (BT) method of literature shows that GTST-MLD can overcome the limits of conventional AT-BT and requires less information to quantify the risk of a generic CPS, properly managing the scarcity of information on security threats. The method is applied to a CPS comprising of a chemical reactor and its control system that is exposed to cyber-attacks to the SCADA system.**

***Index Terms*— Risk analysis, cyber security, Goal Tree Success Tree, Master Logic Diagram, Attack Tree, Bow Tie.**

N_{BE}	Number of Basic Events (BEs)
λ_k	Failure rate of the component of the k-th BE
f_{SCADA}	Probability of BE "unauthorized access to SCADA"
X_k	k-th BE
$P_k(t)$	Probability of the k-th BE occurrence, before time t
$F(t)$	System unreliability
$\Phi(\boldsymbol{X})$	System structure function
N_M	Number of MCSs
i	Index of a MCS
$P[M_i](t)$	Probability of the i-th MCS occurrence before time t
$F_{ATBT}(t)$	Unreliability analytically obtained with AT-BT
n_f	Number of sub-functions in the GTST-MLD
G	Goal function in the GTST-MLD
F_f	f-th sub-function in the GTST-MLD
f	Index of a sub-function in the GTST-MLD
n_c	Number of main components in the GTST-MLD
C_c	c-th main components in the GTST-MLD model
c	Index of a main component in the GTST-MLD
n_p	Number of support components in the GTST-MLD
P_p	p-th support component in the GTST-MLD
p	Index of a support component in the GTST-MLD
n_d	Number of IFs in the GTST-MLD
D_d	d-th IF in the GTST-MLD
d	Index of an IF in the GTST-MLD
$n_{d_{safety}}$	Number of safety-related IFs in the GTST-MLD
$D_{d_{safety}}$	d-th safety-related IF in the GTST-MLD
d_{safety}	Index of a safety-related IF in the GTST-MLD
$d_{security}$	Index of a security-related IF in the GTST-MLD
$n_{d_{security}}$	Number of security-related IFs in the GTST-MLD
$D_{d_{security}}$	d-th security-related IF in the GTST-MLD
$CF_{c,f}$	Weight between C_c and F_f
$DF_{d,f}$	Weight between D_d and F_f
DG_d	Weight between the D_d and G
$PC_{p,c}$	Weight between the P_p and C_c
$DC_{d,c}$	Weight between D_d and C_c
$DP_{d_{security},p}$	Relationship weight between $D_{d_{security}}$ and C_c
$AB_{a,b}$	Weight between the a-th and the b-th element
$P[AB_{a,b}]$	Probability that the b-th element fails (or is unfulfilled) given that the a-th element is failed
$p_{d_{security}}^{attack}$	Attack probability of the $d_{security}$-th attack type
$difficulty_{d_{security}}$	Difficulty level of the $ds_{ecurity}$-th attack type
$P[D_d](t)$	Probability of occurrence of the d-th IF
$P[F_f](t)$	Probability of fulfillment of the f-th sub-function
$P[G](t)$	Probability of the top goal fulfillment in time
$F_{GTST}(t)$	Unreliability calculated with the GTST-MLD
N	Number of Monte Carlo iterations
$T_{mission}$	Mission time of the Monte Carlo simulation
dt	Time interval of the Monte Carlo simulation
$F_{GTST}^{min}(t)$	Lower bound unreliability by GTST-MLD
$F_{GTST}^{max}(t)$	Upper bound unreliability by GTST-MLD

I. Introduction

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 et al., 2015; Kumar et al., 2015; Zio 2016; Zio 2018;). For example, nowadays, Supervisory Control And Data Acquisition (SCADA) systems are commonly used in industrial I&C systems, consisting of hardware and software components, and of connecting network(s) that design an architecture of a centralized controller with several field devices, such as Programmable Logic Controllers (PLCs) (Cherdantseva Y. et al, 2016; Tsang, 2010; NIST, 2011).

While allowing for improved CPSs controllability (Alcaraz et al., 2011), connecting infrastructures introduce new threats (Lopez et al., 2013) and vulnerabilities to external cyber attacks that can alter the I&C systems functionalities (Cho et al., 2017; Shin et al., 2015; Zio 2016; Wang et al., 2018a; Wang et al., 2018b, Alcaraz and Lopez, 2016). Therefore, the risk analysis and management of CPSs is challenging, because traditional risk analysis must be complemented with cyber-security aspects (Kriaa et al., 2015; Subramanian et al., 2016; Amundrud et al., 2017) including information security (Nunez and Agudo, 2014; Wangen et al., 2017).

Safety and security have been indeed, traditionally analyzed separately, because the related risk sources are intrinsically different (Aven, 2009; Kriaa et al., 2015). Safety concerns (stochastic) components failures that can result in accidental scenarios, whereas security concerns (deterministic) malicious and intentional attacks that can compromise both the physical and cyber parts of the system. Developing an integrated risk

Francesco Di Maio is with the Energy Department of Politecnico di Milano, Via La Masa 34, 20156, Milano, Italy (francesco.dimaio@polimi.it)
Roberto Mascherona is with ARAMIS Srl, Bastioni di P.ta Nuova 21, 20121, Milano, Italy (roberto.mascherona@aramis3d.com)
Enrico Zio is with the Energy Department of Politecnico di Milano, Via La Masa 34, 20156, Milano, Italy (enrico.zio@polimi.it) and with Mines ParisTech, PSL Université Paris, Centre de Recherche sur les Risques et les Crises (enrico.zio@mines-paristech.fr)

analysis approach covering both safety and security aspects is needed (Zio, 2016; Zio 2018).

Two alternative perspectives (e.g., the "bottom-up" and the "top-down") can be adopted to conduct such risk analysis (Cherdantseva et al., 2016; The Open Group, 2012; Cho et al., 2018). The "bottom-up" perspective aims at inferring consequences of events and estimating likelihood of system failures following a cause-related logic, in line with the traditional risk analysis approaches (The Open Group, 2012), e.g., Fault Tree (FT) and Bow Tie (BT) methods. A "bottom-up" the Attack Tree Bow Tie (AT-BT) method for integrated safety and cyber security analysis has been recently proposed (Abdo et al., 2018), based on a combination of BT analysis (Ferdous et al., 2012), Fault Tree analysis (FTA), Event Tree Analysis (ETA), and a modified version of AT analysis (Schneier, 1999). This method uses ATs to expand the leaves of a BT that are breaches for security threats. The quantitative assessment requires defining the probability of an attack leaf, considering (McQueen et al., 2006; Cherdantseva et al., 2016; Schneier, 1999):

i) the probability that the system is attacked;
ii) the probability that the attack is successful, given that there is a breach in the CPS;
iii) the probability that the attack damages the CPS, given that the attack is successful.

Historical data should be used for the definition of leaf probabilities (The Open Group, 2012), but "accurate historical data on cyber impacts is badly lacking in the SCADA or process industries, thus making accurate risk assessment extremely difficult" by "bottom-up" approaches (Byres et al., 2007).

This can be overcome resorting to "top-down" approaches that consider components goals rather than failure modes, and the prerequisites to satisfy these goals. Among the advantages of these approaches are (The Open Group, 2012; Cherdantseva et al., 2016; Subramanian et al., 2018):

i) the easy and intuitive construction of the relationships between events, rather than figuring out the components failure modes and their mutual effects (as for "bottom-up" approaches);
ii) the capability of dealing with scarcity of data regarding the failure probability of components due to different failure modes.

In this work, the Goal Tree Success Tree Master Logic Diagram (GTST-MLD) is proposed as a goal-oriented alternative to failure-oriented approaches such as AT-BT. The GTST-MLD approach will be shown to be a powerful approach to model the relationships between components and functions in a system, and capable of accommodating uncertainty due to scarcity of information (Li et al., 2015; Ferrario et al., 2104; Brissaud et al., 2011).

The main original contributions can be summarized as:

- the development of a GTST-MLD framework for considering both safety-related failures and security-related threats in the risk analysis of CPSs;
- the demonstration that goal-oriented approaches, such as GTST-MLD, can overcome the limitations of the traditional failure-oriented approaches, such as the AT-BT, by properly treating uncertainty due to scarcity of information related to cyber threats.

For demonstration, AT-BT and GTST-MLD are developed, tailored and applied for the risk assessment of a chemical reactor (Abdo et al., 2018), whose control system components can fail due to both (stochastic) failures (e.g., failure of the automated safety valve) and (deterministic) cyber-attacks (e.g., Denial of Service attack).

The reminder of the paper is organized as follows. In Section 2, the chemical reactor case study is presented, and the risk analysis is performed by AT-BT; in Section 3, the GTST-MLD theoretical and methodological bases are described, and the results of application to the case study are presented. Finally, Section 4 draws some conclusions.

II. CASE STUDY

We consider a propylene oxide polymerization reactor controlled by PLCs and supervised by a SCADA presented in (Abdo et al., 2018). This serves as an example of a CPS supervised by a SCADA system and the considerations drawn on the GTST-MLD strengths and weaknesses (with respect to AT-BT) can also be extended to other CPSs.

The reactor runs a high exothermic chemical reaction at high pressure and is equipped with a cooling system, formed by two pumps (P1 and P2), a block valve (BV), a control valve (CV) and a power supply aimed at keeping the operation running under normal conditions. The uncontrolled increase of pressure in the system activates an Automated Safety Valve (ASV). The information collected by the SCADA system are accessible to the site managers on tablets, smartphones, etc. by wireless remote control.

The most threatening incident is overheating and overpressure leading to reactor explosion. This might be initiated by cyber-attacks to the SCADA and failures of the components, as modelled in the BT presented in (Abdo et al., 2018), whose $N_{BE} = 6$ Basic Events (BEs) are: ASV failure (k=1), BV failure (k=2), P1 failure (k=3), P2 failure (k=4), CV failure (k=5), Unauthorized access to SCADA (k=6).

For the BEs involving failures of components (k=1,2, …, 5), exponential distributions are assumed for the failure times, with failure rates (λ_k) (INERIS, 2015): λ_1=1E(-3) for the ASV, λ_2=1E(-3) for CV, λ_3=1E(-3) for BV, λ_4=1E(-4) for P1, and λ_5=1E(-4) for P2.

From the BT proposed by (Abdo et al., 2018), it can be seen that the only BE that can cause overpressure in the system is the stochastic failure of the Automated Safety Valve (ASV), whereas overheating is produced by the cooling system failure that, in turn, fails due to the stochastic failures of at least one of the two valves (BV or CV) or the pumping system. This latter is due to the failure of both Pump 1 (P1) and Pump 2 (P2).

The BT is complemented by the AT of Fig. 1, which models the logic of occurrence of the event "unauthorized access to SCADA" (k=6). Also, this event may lead to the cooling system failure (in this case, due to CPS cyber-security vulnerabilities): indeed, the SCADA system supervises the control systems of the chemical reactor and it might cause the reactor explosion, if successfully attacked.

The attack to the SCADA system can be manifested as:

- an attack to the communication network, viz:
  i) Key logger attack;
  ii) Man in the middle;
  iii) Message spoofing;

iv) Replay;
v) Denial of Service attack (DoS).

- an attack to computer software, viz:
  i) Buffer overflow attack;
  ii) Structured Query Language (SQL) injection attack;
  iii) STUXNET.

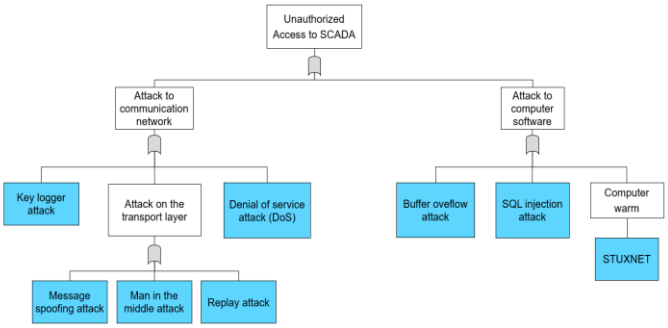

Fig. 1. Attack tree (adapted from Abdo et al., 2018).

TABLE I
LIST OF CYBER SECURITY ATTACKS

Cyber attack type	Difficulty	Vulnerability	Probability (Byres et al., 2004)
Key logger	Medium	High	N.A.
Message spoofing	Medium	Medium	N.A.
Replay	Trivial	Medium	N.A.
Man in the middle	Medium	Medium	N.A.
Denial of service	Trivial	High	N.A.
Buffer overflow	Very difficult	High	N.A.
SQL injection	Difficult	Medium	N.A.
STUXNET	Medium	High	N.A.
Unauthorized access to SCADA control center			$f_{SCADA} = 0.046/y$

Each one of the above-mentioned attacks is characterized by its difficulty, vulnerability and probability, as listed in Table I.
It is worth mentioning that in this work the attack modelling is focused on the effects of the attacks on the physical process and not on the effects on the ICT infrastructure, nor on the attitudinal behavior of the attacker.
Difficulty relates to the experience, time, resources and skills that are needed to perform the attack (Byres et al., 2004), whereas vulnerability refers to the defense strategies implemented in the system against each attack (in other words, the poorer the quality and lower the number of defenses, the higher the system vulnerability to the attack). For example, the key logger attack is characterized by medium difficulty (because of the little time, experience, resource and skills needed), but associated to high vulnerability, because breaching into the system is simple (when email surveillance is not implemented).
We assume that only the probability of "unauthorized access to SCADA" is known and equal to $f_{SCADA} = 0.046\ attacks/year$ (Byres et al., 2007), whereas the probabilities for each one of the listed attacks are not available (N.A., in Table I). Note that f_{SCADA} is estimated from the Industrial Security Incident Database (ISID), based on the reported security incidents in 2004 (i.e., 23 failures for 500 monitored SCADA systems). Even though the aim of ISID is that of creating an historical collection of industrial cyber security incidents, from which industry can gain a realistic understanding of the of cyber threats, the value of f_{SCADA} is probably an underestimation, mainly because it arbitrarily neglects:
i) statistical fluctuations (or even increases) in the years;
ii) the contribution of system vulnerability to the success rate of an attack.

In line with the above mentioned hypotheses, constant BE rates of occurrences, we assume exponential probability distributions for components failure times and SCADA attack times, so that the probability that the k-th BE occurs before time t is:

$$P_k(t) = \begin{cases} 1 - e^{-(\lambda_k t)}\ for\ k = 1, \dots, 5 \\ 1 - e^{-(f_{SCADA} t)}\ for\ k = 6 \end{cases} \quad (1)$$

The probabilities of the minimal cut sets (MCSs) of the system obtained from the AT-BT model described in (Abdo et al., 2018) are listed in Table II.

TABLE II
LIST OF THE MCSS

#MCS	Events (belonging to i-th MCS)	Probability $P[M_i](t)$
1	ASV failure, BV failure	$P_1(t)P_2(t)$
2	ASV failure, CV failure	$P_1(t)P_5(t)$
3	ASV failure, P1 failure, P2 failure	$P_1(t)P_3(t)P_4(t)$
4	ASV failure, Key logger attack ASV failure, Message spoofing attack ASV failure, Man in the middle attack ASV failure, Replay attack ASV failure, Denial of service attack ASV failure, SQL attack ASV failure, Buffer overflow attack ASV failure, STUXNET	$P_1(t)P_6(t)$

The MCSs $1, 2, 3$ are composed of stochastic components failures, whereas MCS 4 is due to "unauthorized access to SCADA".
We evaluate the system unreliability adopting the rare event approximation (Zio, 2007):

$$F(t) \cong P[\Phi(\boldsymbol{X}) = 1] \leq \sum_{i=1}^{N_M} P[\mathrm{M_i}](t) \quad (2)$$

where $\Phi(\boldsymbol{X})$ is the system structure function, which incorporates all the causal relationships among the BEs $= (X_1, X_2, \dots, X_{N_{BE}})$, which lead to the top event, N_M is the number of MCSs for the system under analysis and M_i is the i-th MCS. The unreliability $F_{ATBT}(t)$ analytically obtained with Eqs. 1 and 2 is shown in Fig. 2 (solid line): at $t = 1$ year, the probability of reactor explosion is equal to 4.7E-5, which falls within the range [1E(-5)-1E(-4)] reported in (Abdo et al., 2018) for the same case study. This numerical result is taken as baseline for the comparison with GTST-MLD. Moreover (see Fig. 2), comparing the system unreliability obtained by considering only safety-related MCSs (1. ASV failure, BV failure; 2. ASV failure, CV failure; 3. ASV failure, P1 failure, P2 failure), plotted in dashed line in Fig. 2, or considering both safety and cyber security-related MCSs (with addition of 4. ASV failure, unauthorized access to SCADA), plotted in solid line in Fig. 2, we see how the former is an order of magnitude lower than the latter, confirming, again, what reported in (Abdo et al., 2018) and highlighting the need of considering security-related aspects (and not only safety-related aspects) in the risk analysis

of CPSs, to avoid misleading risk results.

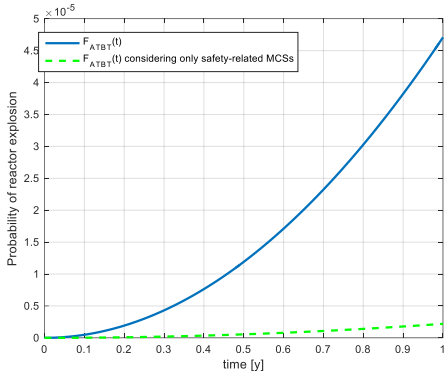

Fig. 2. Probability of reactor explosion considering safety and security-related MCS (continuous line) or only safety-related MCS (dashed line).

III. THE GTST-MLD APPROACH

GTST-MLD is a goal-oriented approach to logically and hierarchically decompose ("top-down") a system into functions and sub-functions, and for representing interactions between the different system components and their failures (Li et al., 2015; Brissaud et al., 2011). The Goal Tree (GT) hierarchically decomposes the system safety goal function into n_f sub-functions F_f, $f = 1, \dots, n_f$. The "top" function is the *goal function* and defines the principal purpose which the system is designed for. The hierarchy of the GT is built by answering the question "how" an upper level function is achieved, until the lowest level functions are reached (i.e., when the functions have been sufficiently decomposed according to the available knowledge and the scope of the study). Conversely, the functions should describe "why" the respective sub-functions of the lower level are needed.

The ST describes the relations between the physical elements of the system and is developed "top-down" looking at all levels in which the system can be decomposed. Practically, the physical elements are all the components of the system necessary to achieve any of the functions present in the GT. As for the ST, two types of components are distinguished (see Fig. 3): the n_c main components C_c, $c = 1, \dots, n_c$ and the n_p support components P_p, $p = 1, \dots, n_p$, i.e., those needed to fulfill the main function and those needed for the operation of the main components, respectively. Starting from the "system" element, ST is created by answering the question "what are the parts" in which the considered element can be decomposed into, until the basic components of the system are reached. The relationships between GT functions and ST main components is represented in a compact and transparent way by the MLD. In practice, a MLD maps the functions and components mutual influences into a matrix CF whose values $CF_{c,f}$ are the strength of the relationship between the c-th component and the f-th functions (rows and columns, respectively). Pictorially, the MLD is shown in Fig. 4: the strength values are represented by different shades of colors of the circles (usually, the darker the shade, the stronger the relation) connecting components (rows) with functions or sub-functions (columns).

The connections between main and support components are mapped in a MLD matrix, called PC, whose values $PC_{p,c}$ are the strengths of the relationships between the p-th support components and the c-th main components.

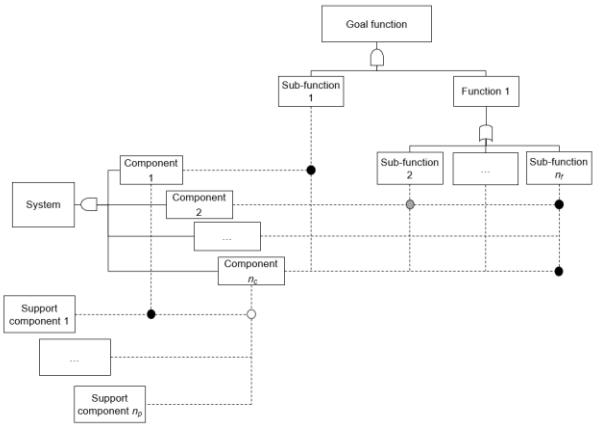

Fig. 3. Example of GTST-MLD structure.

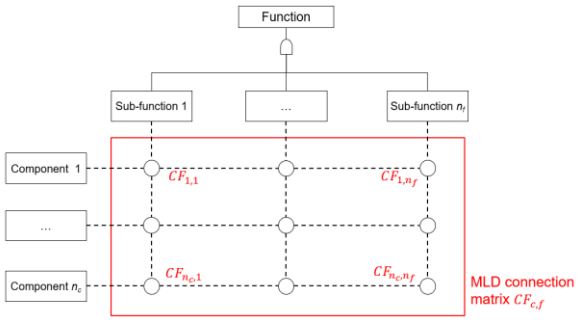

Fig. 4. MLD connections between GT and ST.

The n_d Influencing Factors (IFs) $D_d, d = 1, \dots, n_d$ are the dysfunctional aspects that can prevent the system to achieve the goal function and impair both the system safety and security.

The GTST-MLD here proposed originally considers as IFs not only the components stochastic failures but also the malicious attacks that may affect the system functionality, making it, as we will show, a suitable approach for integrating safety and security into the same framework of risk analysis.

To account for the different nature of the influencing factors connected to safety ($D_{d_{safety}}$, $d_{safety} = 1, \dots, n_{d_{safety}}$) and security ($D_{d_{security}}$, $d_{security} = 1, \dots, n_{d_{security}}$), occurrences of $D_{d_{safety}}$ are modeled according to the components failure times distributions and occurrences of $D_{d_{security}}$ are modeled according to the SCADA system attack times distribution.

For what concern the attack type selection, which type of attack occurs for the such CPS considered is modelled by assigning numerical values to the cyber-attacks difficulty levels in the range [0,1] (i.e., trivial, medium, difficult and very difficult are taken equal to 0.8, 0.6, 0.4 and 0.2, respectively). These values are assigned according to (Byres et al., 2004) and are related to the skills, experience and time necessary to perform each type of attack.

Then, attack type probabilities $p_{d_{security}}^{attack}$ are computed:

$$p_{d_{security}}^{attack} = \frac{difficulty_{d_{security}}}{\sum_{d_{security}}^{n_{d_{security}}} difficulty_{d_{security}}} \quad (3)$$

where $difficulty_{d_{security}}$ is the difficulty (Table I) of the $d_{security}$-th attack. Within a Monte Carlo sampling scheme for the numerical simulation of attacks, the $d_{security}$-th attack occurs if a random value ρ, sampled from a uniform distribution in [0,1], falls within the sub-range of [0,1] corresponding to its $p^{attack}_{d_{security}}$. 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 matrices can be defined (similarly to what shown in Fig. 4) for mapping the $n_{d_{safety}}$ IFs influence on the n_c main components, and of the $n_{d_{security}}$ IFs on the n_p supporting components.

Summarizing, the GTST-MLD relationships can be hierarchically listed as:

- the $d_{security}$-th cyber-attack implies the failure of the *p*-th support component;
- the d_{safety}-th stochastic failure implies the failure of the *c*-th main component;
- the failure of the *p*-th support component implies the failure of the *c*-th main component;
- the failure of the *c*-th main component implies a loss of the *f*-th function.

For the loss of the *f*-th function, a model $DF_{d,f}$ of the relationship between any *d*-th (either safety-related or security-related) and the *f*-th function is defined:

$$DF_{d,f} = \cup_c \left(DC_{d,c} \cap CF_{m,f}\right) \tag{4}$$

where $DC_{d,c}$ models the relationship between any *d*-th IF (either safety-related or security-related) and the *c*-th main component, viz:

$$DC_{d,c} = DC_{d_{safety},c} \cup_p \left(DP_{d_{security},p} \cap PC_{p,c}\right) \tag{5}$$

In general, the weight $AB_{a,b}$ can be seen as the probability that B_b occurs given that A_a occurred. For example, $P[CF_{c,f}]$ is the probability of a loss of the *f*-th function given that the *c*-th component is failed. In this way, it is possible to define the probability of fulfillment of the GT sub-functions $P[F_f](t)$:

$$P[F_f](t) = 1 - \cup_d \left(P[D_d](t) \cap P[DF_{d,f}]\right) \tag{6}$$

where $P[D_d]$ is the probability of occurrence of each *d*-th IF (either safety or security-related).

Considering the AND/OR gates that define the relationship between functions and the top goal function, we define the influence of IFs on the goal function:

$$P[DG_d] = \cup_f / \cap_f \left(P[DF_{d,f}]\right) \tag{7}$$

Therefore, the probability of the top goal fulfillment is:

$$P[G](t) = 1 - \cup_d \left(P[D_d](t) \cap P[DG_d]\right) \tag{8}$$

and the unreliability of the system is the complement to one of this probability:

$$F_{GTST}(t) = 1 - P[G](t) \tag{9}$$

For complex CPSs, estimate of $F_{GTST}(t)$ can be obtained by Monte Carlo simulation, enriching the approach proposed in (Ferrario and Zio, 2014) by rigorously complementing the IFs due to cyber-attacks to the IFs due to stochastic failures.

The simulation consists in two successive phases, namely initiation and propagation:

- the initiation step simulates the occurrence of IFs;
- the propagation simulates the IFs propagation to components and/or functions by GTST, according to the relationships expressed by the MLD.

In such simulation, counters for IFs, components and functions are defined and used to report, during the simulation, the occurrence of IFs, the failures of components and the fulfillment of functions.

IV. APPLICATION TO THE CASE STUDY

The GTST-MLD of Fig. 5 is built for the case study of Section 2 and the Monte Carlo simulation is performed with $N = 10^7$ and $T_{miss} = 1$ year.

The system *goal function* "explosion prevention", is guaranteed if the cooling system or the pressure control system are working properly, making "pressure control" ($f = 1$) and "overheating control" ($f = 2$) its related *sub-functions*.

As for the ST, we divide the control system of the chemical reactor in:

i) Pressure control system, made of up ASV ($c = 1$)
ii) Cooling system, made up of P1 ($c = 2$), P2 ($c = 3$), CV ($c = 4$), BV ($c = 5$) and the field devices of the SCADA for the cooling system ($c = 6$), which include sensors, actuators and a PLC;

We consider the SCADA system (which supports and supervises the control of temperature and pressure, but it is not physically embedded in the control systems) as support system P_p, decomposing it in n_p components: hardware ($p = 1$), software ($p = 2$) and communication network ($p = 3$).

The weights of the MLD, High (with a quantitative value of 1), Medium (with a quantitative value of 0.5) and Low (with a quantitative value of 0), are assigned based on technical considerations about the system. For example (see Table III), from the BT analysis we know that if the BV fails, then, the cooling system also fails and, consequently, $f = 2$ is not fulfilled. From this, the relationship between $c = 6$ and $f = 2$ can be set equal to "High". Similarly, all the weights between SCADA (*p*=1,2,3) and the *c*=6 main component, and between IFs (safety and security) and main components (*d*=1,2,3,4,5,6 with *c*=1,4,2,5,6, respectively) are all set equal to "High".

For validation purposes, $F_{ATBT}(t)$ (solid line) and the $F_{GTST}(t)$ (stars) are plotted in Fig. 6: the negligible discrepancy confirms that the GTST-MLD approach is a suitable goal-oriented alternative to the failure-oriented AT-BT. Moreover, as already pointed out in Fig. 2, the unreliability estimated using GTST-MLD considering only safety-related IFs is an order of magnitude lower than that obtained considering both safety and cyber security-related IFs

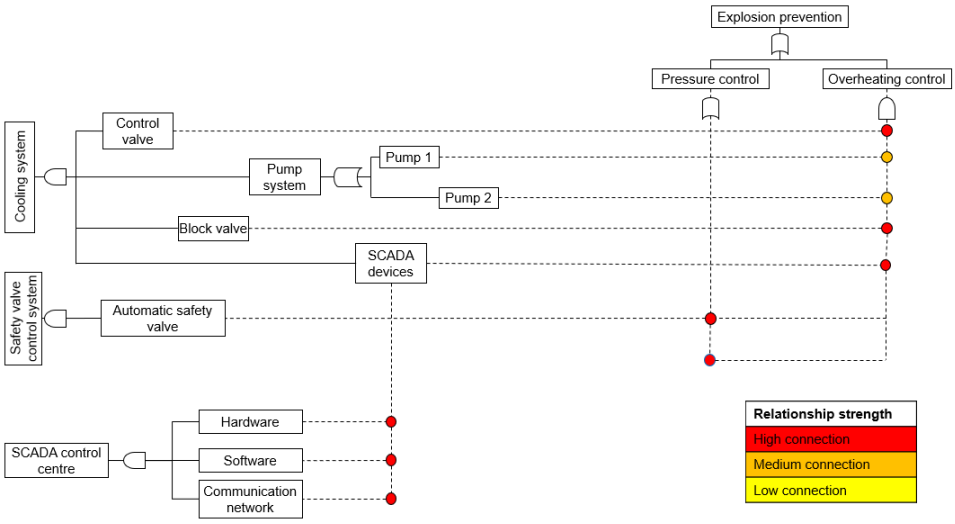

Fig. 5. GTST-MLD structure for the case study under analysis.

TABLE III
CONNECTION WEIGHTS BETWEEN MAIN COMPONENTS AND GOAL FUNCTIONS

$CF_{c,f}$	$f = 1$	$f = 2$
$c = 1$	High	/
$c = 2$	/	Medium
$c = 3$	/	Medium
$c = 4$	/	High
$c = 5$	/	High
$c = 6$	/	High

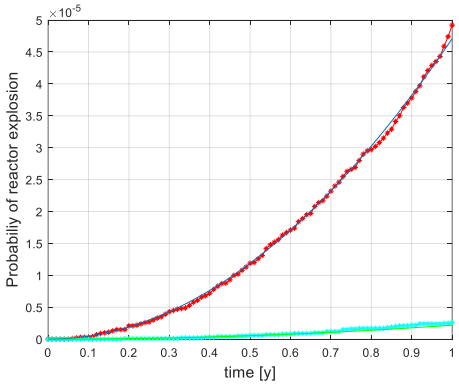

Fig. 6. Comparison between AT-BT analytical result (solid lines) and GTST-MLD simulated result (stars).

It is worth mentioning that, for the sake of the comparison:

1) Beside all the safety-related IFs, the only security-related IF that has been considered is "unauthorized access to SCADA" (with "High" connection weights to the $p = 1, 2, 3$ support components), neglecting the initialization of numerous types of cyber-attacks, that however should be modelled for a realistic risk analysis. As we will show in what follows, this can be overcome by GTST-MLD, even when there is scarcity of detailed information regarding each attack type probability;
2) Vulnerability of the system to the different types of attacks has been neglected;
3) Uncertainty has not been assumed neither on the IFs initialization frequencies, nor on the propagation weights.
4) Safety and security related risks are treated considering their different nature according to the theoretical approach detailed in (Abdo et al., 2018).

Let us now assume that all the types of attack listed in Table I are known, as well as their information regarding the difficulty of the attack and the vulnerability of the system to that attack. Key logger, message spoofing, replay, man in the middle, DoS, buffer overflow, SQL injection and STUXNET are the security-related IFs ($d = 6, \dots, 13$), all affecting directly the SCADA with a weight $DP_{d,p}$ inversely proportional to the countermeasures implemented in the system against each of them (i.e., the larger the weight, the larger the vulnerability, the lower the quality and the number of countermeasures usually implemented to counteract the specific attack, pictorially showed in Fig. 7).

Fig. 8 shows the comparison between the AT-BT analytical result for $F_{ATBT}(t)$ (solid line) and the GTST-MLD result (stars), when the vulnerability of the system to the different attacks is accounted for in the propagation of the IFs up to the goal function. It can be seen that AT-BT overestimates the risk related to cyber threats. This is due to the fact that, according to AT-BT assumptions, the BE_6 propagates up to the top event without accounting for any successful defense action, whereas GTST-MLD accounts for the probability of defense success to any attack that may be initiated.

The GTST-MLD flexibility to embed vulnerability into the weights assignment allows prioritizing defense strategies to maximize the system safety, by quantifying the influence on $F_{GTST}(t)$ of changing the weights (mimicking a change in the defense strategy to oppose a specific attack).

Despite that, we must consider:

i) the lack of data on the type and quantity of attacks,
ii) the leak of knowledge on the vulnerability of a system to such attacks,
iii) the awareness that the different defense strategies to oppose different attacks

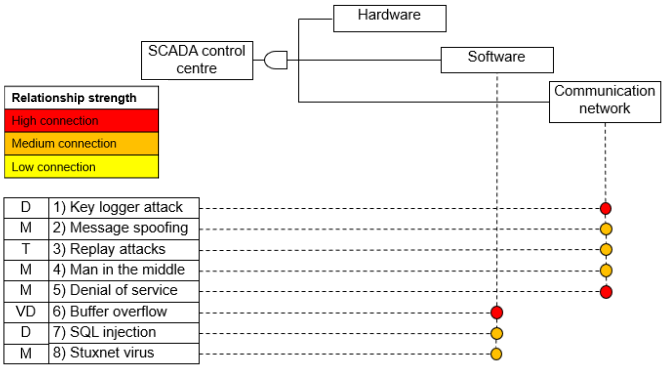

Fig. 7. GTST-MLD (connection between Security IFs and SCADA).

Accounting for these factors amounts to assigning uncertain weights between security-related IFs and the SCADA system, making it fundamental to consider the effect of the propagation of the uncertainty on the weights $DP_{d_{security},p}$ for the $F_{GTST}(t)$ estimation. The results obtained are shown in Fig. 8, where the bounds resulting from the uncertain weights originate the shadowed area that includes the GTST-MLD risk estimation, covering the uncertainties in the system modeling.

Let us, for example, assume that the weights of the MLD are assigned as intervals, as follows: High [0.75-1], Medium [0.25-0.75], Low [0-0.25]. Then, these intervals of weights uncertainty are propagated in the GTST-MLD model by a Monte Carlo Simulation, to obtain, at each time *t*, the bounding estimates of $F_{GTST}^{min}(t)$ and $F_{GTST}^{max}(t)$, where the former is calculated using the lowest values of the weights, whereas the latter using the largest values of the weights. In practice the procedure provides a bounded estimation for the system unreliability $\{F_{GTST}^{min}(t), F_{GTST}^{max}(t)\}$ due to the uncertain weights

As an example, one might argue that the types of attacks the system might be subjected to (see Table I) are not realistic because, in practice, the continuous improvement and evolution of digital technology accidentally exposes the system to new unknown threats. To show the robustness of the estimation of $F_{GTST}(t)$ to the lack of knowledge on all possible IFs that may impair the system functionality, the result is shown without considering Denial of Service among the potential IFs. It can be seen that the probability distribution of the (only) known types of attacks leading to the "unauthorized access to SCADA" allows covering the probability of occurrence of the unknown scenarios in the quantification of $F_{GTST}(t)$.

Adopting AT-BT modeling this is not possible: all the attack scenarios must be identified and included in the Basic Event "unauthorized access to SCADA" (see Section 2), and vulnerability is not considered (with its uncertainty). It is straightforward that the GTST-MLD allows covering lack of knowledge that can limit the AT-BT approach, which is constrained to assess the impact of SCADA induced failures when all "possible" cyber-attacks are considered.

V. CONCLUSIONS

GTST-MLD has been adopted for the first time as a goal-oriented approach for a quantitative risk analysis of a CPS, considering failures and cyber-security threats.

By application to the case study of the control system of a propylene oxide polymerization reactor, GTST-MLD has been shown to offer a fit alternative to conventional failure-oriented methods, such as AT-BT. In summary, the GTST-MLD:

- models the interdependencies between components;
- allows considering different cyber-attack types and their influence on different parts of the system;
- properly handles uncertainty due to the lack of information (typically related to cyber-security threats);
- provides an uncertainty management strategy to cover possible unknown cyber-threats.

The GTST-MLD weights assignment is expert dependent and efforts must be made to collect experimental data on threats and vulnerabilities, or to develop more complete and detailed databases of security incidents; on the other hand, the definition of a method for assigning weights integrating the heterogeneous sources of knowledge, information and data is needed, and will be the focus of future research work.

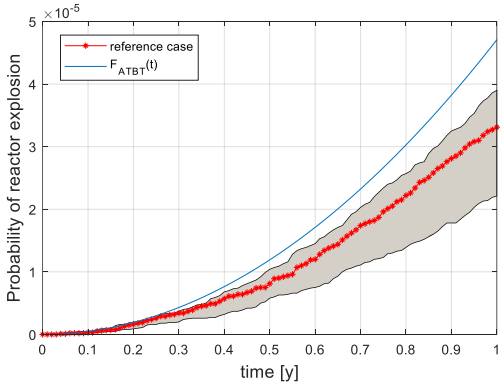

Fig. 8. Comparison between the AT-BT analytical result (solid line) and the GTST-MLD simulated result (stars), when vulnerability of the system to the different attacks is accounted for in the propagation of the IFs up to the goal function, and GTST-MLD simulation (without DoS scenario) considering uncertainties (shadowed area).

REFERENCES

(Abdo et al., 2018) H. Abdo, M. Kaouk, J.-M. Flaus, F. Masse, "A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie –combining new version of attack tree with bowtie analysis", 2018, computers & security 72 175–195

(Alcaraz et al., 2010) C. Alcaraz, J. Lopez, J. Zhou, R. Roman, "Secure SCADA framework for the protection of energy control systems", 2010, Concurrency and computation: practice and experience 23, 1431-1442

(Alcaraz and Lopez, 2016), C. Alcaraz, J. Lopez, "Safeguarding structural controllability in cyber-physical control systems", 2016, ESORICS 2016, part II, LNCS 9879, pp. 471-489

(Amundrud et al., 2017) Øystein Amundrud, Terje Aven, Roger Flage, "How the definition of security risk can be made compatible with safety definitions", 2017, Institution of mechanical engineers Vol. 231(3) 286-294

(Aven, 2009) Aven, T., "Identification of safety and security critical systems and activities", 2009, Reliability Engineering & System Safety, 94(2), pp.404-411.

(Brissaud et al., 2011) Florent Brissaud, Anne Barros, Christophe Berenguer, Dominique Charpentier, "Reliability analysis for new technology-based transmitters", 2011, Reliability Engineering and System Safety 96 299–313

(Byres et al., 2004) E.J. Byres, M. Franz, D. Miller, "The use of attack trees in assessing vulnerabilities in scada systems", 2004, Proceedings of the international infrastructure survivability workshop.

(Byres et al., 2007) Eric Byres, David Leversage and Nate Kube, "Security incidents and trends in SCADA and process industries", The industrial ethernet book, MAY 2007

(Cherdantseva et al., 2016) Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, Kristan Stoddart, "A review of cyber security risk assessment methods for SCADA systems", 2016, computers &

security 56 1–27
(Cho et al., 2018) C.-S. Cho, Wei-Ho Chung , and Sy-Yen Kuo, “Using Tree-Based Approaches to Analyze Dependability and Security on I&C Systems in Safety-Critical Systems”, IEEE SYSTEMS JOURNAL, VOL. 12, NO. 2, JUNE 2018.
(Ferdous et al., 2012) Ferdous R, Khan F, Sadiq R, Amyotte P, Veitch B. “Handling and updating uncertain information in bow-tie analysis”, J Loss Prevent Proc Indust 2012;25(1):8–19.
(Ferrario and Zio, 2014) E. Ferrario, E. Zio, “Goal Tree Success Tree–Dynamic Master Logic Diagram and Monte Carlo simulation for the safety and resilience assessment of a multistate system of systems”, 2014, Engineering Structures 59 411–433
(Hu and Modarres, 1999) Yu-Shu Hu, Mohammad Modarres, “Evaluating system behavior through Dynamic Master Logic Diagram (DMLD) modeling”, 1999, Reliability Engineering and System Safety 64 241–269
(INERIS, 2015) INERIS. “Agrégation semi-quantitative des probabilits dans les études de dangers des installations classées” – omega probabilités; 2015.
(Kriaa et al., 2015) Siwar Kriaa, Ludovic Pietre-Cambacedes, Marc Bouissou, Yoran Halgand, “A survey of approaches combining safety and security for industrial control systems”, 2015, Reliability Engineering and System Safety139 56–178
(Jiang et al., 2016) Y. Jiang, S. Yin, Y. Yang, “Comparison of KPI related fault detection algorithms using a newly developed MATLAB toolbox: DB-KIT”, IEEE, 2016
(Jiang and Yin, 2017) Y. Jiang, S. Yin, “Recent results on key performance indicator oriented fault detection using the DB-KIT toolbox”, IEEE, 2017
(Jiang et al., 2018a) Y. Jiang, K. Li, S. Yin, “Cyber-physical system based factory monitoring and fault diagnosis framework with plant-wide performance optimization”, IEEE, 2018
(Jiang et al., 2018b) Y. Jiang, S. Yin, O. Kaynak, “Data-driven monitoring and safety control of industrial cyber-physical systems: basics and beyond”, IEEE, 2018
(Kumar et al., 2015) S. Kumar Khaitan, J. D. McCalley, “Design Techniques and Applications of Cyberphysical Systems: A Survey”, IEEE SYSTEMS JOURNAL, VOL. 9, NO. 2, JUNE 2015.
(Li et al., 2015) Y.F. Li, S. Valla, E. Zio, “Reliability assessment of generic geared wind turbines by GTST-MLD model and Monte Carlo simulation”, 2015, Renewable Energy 83 222-233
(Lopez at al., 2013) J. Lopez, C. Alcaraz, R. Roman, “Smart control of operational threats in control substations”, 2013, Computers &Security xxx (2013) 1-14.
(Miles et al., 2006) Miles A. McQueen, Wayne F. Boyer, Mark A. Flynn, George A. Beitel, “Quantitative Cyber Risk Estimation Methodology for a Small SCADA Control System”, 2006, Proceedings of the 39th Hawaii International Conference on System Sciences
(Mueller and Yadegari, 2012) Mueller P, Yadegari B. “The stuxnet worm”, Département des sciences de linformatique, Université de l’Arizona; 2012.
(NIST, 2011) NIST special publication 800-82 guide to industrial control systems (ICS) security. 2011.
(Nunez and Agudo, 2014) D. Nunez and I. Agudo, “BlindIdM: A privacy-preserving approach for identity management as a service, International Journal Information Security, 13: 199-215, 2014
(Roy et al., 2010) Arpan Roy, Dong Seong Kim, Kishor S. Trivedi, “Cyber security analysis using attack countermeasure trees”, 2010, CSIIRW ’10 Proceedings of the sixth annual workshop on Cyber Security and Information Intelligence Research, Article No. 28
(Shin et al., 2010) Jinsoo Shin, Gyunyoung Heo, Hanseong Son, “Methodology on Cyber Security for Digital I&C System in Research Reactors”, 2010, Nuclear Engineering and Technology 49 517-524
(Schneier, 1998) Schneier B. “Modeling security threats”, In: Dr. Dobbs Journal; 1998.
(Tsang, 2010) Rose Tsang, “Cyberthreats, Vulnerabilities and Attacks on SCADA Networks”, 2010, University of California, Berkley.
(Subramanian et al., 2016) N. Subramanian, J. Zalewski, “Quantitative Assessment of Safety and Security of System Architectures for Cyberphysical Systems Using the NFR Approach”, IEEE SYSTEMS JOURNAL, VOL. 10, NO. 2, JUNE 2016.
(Ten et al., 2010) Chee-Wooi Ten, Student Member, IEEE, Govindarasu Manimaran, Senior Member, IEEE, and Chen-Ching Liu, Fellow, IEEE, “Cybersecurity for Critical Infrastructures: Attack and Defense Modeling”, IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART A: SYSTEMS AND HUMANS, VOL. 40, NO. 4, JULY 2010
(The Open Group, 2010) The Open Group. Dependency modeling (O-DM). “Constructing a data model to manage risk and build trust between interdependent enterprises”, Open Group Standard; 2012.
(Wang et al., 2018a) Wang W., Cammi A., Di Maio F., Lorenzi S., Zio E., “A Monte Carlo-based exploration framework for identifying components vulnerable to cyber threats in nuclear power plants”, Reliability Engineering and System Safety, 175, pp. 24-37, 2018.
(Wang et al., 2018b) Wang W., Di Maio F., Zio E., “Hybrid fuzzy-PID control of a nuclear Cyber-Physical System working under varying environmental conditions”, Reliability Engineering and Design, 331, pp. 54-67, 2018
(Wangen et al., 2017) G. Wangen, C. Hallstensen, E. Snekkenes, “A framework for estimating information security risk assessment method completeness”, Core Unified Risk Framework, CURF, International Journal Information Security, 2017
(Zio, 2007) Zio E., “An introduction to the basics of reliability and risk analysis”, 2007, World Scientific Publishing Co. Pte. Ltd. Vol. 13
(Zio, 2016) Zio E., “Challenges in the vulnerability and risk analysis of critical infrastructures”, 2016, Reliability Engineering & System Safety, 152, pp.137-150.
(Zio, 2018) Zio E., “The future of risk assessment”, Reliability Engineering and System Safety, 177, pp. 176-190, 2018.