Safety and Security Interactions Modeling Using the BDMP Formalism: Case Study of a Pipeline

Siwar Kriaa[1,2], Marc Bouissou[1,2], Frederic Colin[1],
Yoran Halgand[1], and Ludovic Pietre-Cambacedes[1]

[1] Electricité de France (EDF) R&D
[2] Ecole Centrale Paris
{siwar.kriaa,frederic-ep.colin,yoran.halgand,
ludovic.pietre-cambacedes}@edf.fr, marc.bouissou@ecp.fr

Abstract. The digitalization of industrial control systems (ICS) raises several security threats that can endanger the safety of the critical infrastructures supervised by such systems. This paper presents an analysis method that enables the identification and ranking of risks leading to a safety issue, regardless of the origin of those risks: accidental or due to malevolence. This method relies on a modeling formalism called BDMP (Boolean logic Driven Markov Processes) that was initially created for safety studies, and then adapted to security. The use of the method is first illustrated on a simple case to show how it can be used to make decisions in a situation where security requirements are in conflict with safety requirements. Then it is applied to a realistic industrial system: a pipeline and its instrumentation and control system in order to highlight possible interactions between safety and security.

Keywords: Safety, security, interdependencies, modeling, industrial control systems.

1 Introduction

Modern industrial control systems are becoming increasingly complex and interconnected due to the integration of new information and communication technologies. The remote supervision and control of infrastructures means that these control systems are increasingly connected to external networks. Moreover, the migration towards standard communication protocols such as TCP/IP and the use of off the shelf components enables cost reduction, faster deployment and provides more flexibility. This radical transformation of control systems however introduces many security-related vulnerabilities such as software design flaws or vulnerabilities in publicly available protocols; that may endanger the overall infrastructure safety.

Safety and security risks converge when industrial infrastructures are supervised and controlled by digital control systems such as SCADA systems. It is consequently important to consider possible interdependencies between safety and security for a complete risk assessment and management. Typically we are interested in demonstrating how security issues impact safety and vice versa.

A. Bondavalli and F. Di Giandomenico (Eds.): SAFECOMP 2014, LNCS 8666, pp. 326–341, 2014.

In this paper, we propose to model safety and security interdependencies for an industrial case study using the Boolean logic Driven Markov Processes (BDMP) formalism. The approach used in this paper was first introduced in [12] where it was illustrated on a pedagogical use case. In this paper we apply it on a realistic industrial case study taking into account the system architecture. We discuss in Section 2 the convergence of security and safety issues in industrial control systems and their possible interdependencies. We give in Section 3 an overview of the BDMP formalism and the associated KB3 platform. We explain in Section 4 the benefits of BDMP on a simple example where safety and security are in contradiction. We provide in Section 5 the description of a pipeline case study architecture, the associated BDMP model and give qualitative and quantitative results obtained from it. Section 6 concludes the paper and introduces future work.

2 Safety and Security Interdependencies in ICS

2.1 Scope and Definitions

Safety and security can have different meanings according to the context and the technical communities; for instance safety is not defined in the same manner in the aerospace and nuclear communities. Consequently, it is important to clarify the signification of these terms in each context to avoid ambiguities. The SEMA referential proposed in [16] enables to frame the use of the terms “safety” and “security” based on two distinctions: System vs. Environment (S-E) and Malicious vs. Accidental (M-A). The first distinction is based on the origin of the threat or event leading to the considered risk and what it impacts (whether risk originates in the system and impacts the environment or vice-versa). The second distinction defines the nature of the threat or event giving birth to the considered risk, whether it is malicious or accidental. A system to system dimension is added to complete the coverage. In the frame of this paper, security is related to risks originating from or exacerbated by malicious intent, independently from the nature of the related consequence, whereas safety addresses accidental ones, i.e. without malicious intent, but with potential impacts on the system environment.

2.2 Related Work

In the literature, many authors raise awareness about the new security risks introduced by digitalized control systems and their potential impact on critical infrastructures safety in different industrial areas: aerospace [1], automotive [7], rail [17], building [10], energy [3]. These risks are also considered in emerging and dedicated industrial standards, like the IEC 64443 international standards series.

Historically separated, safety and security have long been treated by two different communities and with different methodologies. The need for a common framework integrating both safety and security issues is today becoming urgent with the increasing number of cyber-attacks targeting critical infrastructures. A common framework was addressed by Eames and Moffet in 1999 [4]. Much research has recently been carried-out triggering multiple cross-fertilizations between the two domains [13] but also several new approaches that propose to combine safety and security analysis in risk assessment [10,9,18,12,6].

2.3 Types of Safety and Security Interdependencies

In the literature some papers [4,10] outline possible interactions between safety and security requirements that can be either synergies or conflicts. In [12], Pietre-Cambacedes identifies four kinds of interdependencies:

- Conditional dependency: fulfillment of security requirements conditions safety or vice-versa;
- Mutual reinforcement: safety requirements or measures contribute to security, or vice-versa. Such situations enable resources optimization and cost reduction;
- Antagonism: safety and security requirements or measures lead, when considered together, to conflicting situations (cf. example in Section 4.1);
- Independence: no interaction.

These four kinds of relationship will be the basis of our study in the sequel.

3 Presentation of the BDMP Formalism and the KB3 Modeling Platform

The BDMP formalism enables graphical modeling of safety [2] and security [11,14,15,8]. BDMP models integrating both aspects are introduced in [12]. Visually similar to fault trees (or attack trees), BDMP provide good readability and a hierarchical representation. BDMP model the different combinations of events (leaves of the tree) that lead to the top event (system failure/damage). Additionally BDMP enable dynamical modeling with a special type of link called a “trigger”. Each basic event of a BDMP is associated with two distinct Markov processes corresponding to two possible modes of the basic event. The mode chosen for a given leaf at a given instant depends on the realization of other leaves, which is modeled with triggers (see example in Section 4.1). BDMP have interesting mathematical properties enabling an efficient processing for BDMP that specify Markov processes with very large state spaces [2]. The relevance of using Markov processes for security modeling is discussed in [11].

The KB3 platform [14] enables to input graphically BDMP models and generates textual models (in the Figaro modeling language) describing them. These latter are used as input to the KB3 quantification tools (FigSeq and Yams) in order to compute the probability of the top event and the different possible scenarios leading to it, sorted by decreasing contribution to the top event probability.

Table 1. Basic BDMP leaves for safety modeling

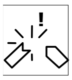
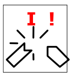
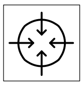
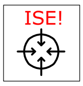
Representation	Modeled behavior
	This leaf is used to model a failure in operation, when the modeled component is active. Failure occurs after a time exponentially distributed (parameter λ) and can also be repaired in a time exponentially distributed (parameter μ).
	This leaf is used to model a failure on demand, likely to arise instantaneously when the leaf changes of mode (activated or not), with a probability γ. Failure can be repaired in a time exponentially distributed (parameter μ).

Table 2. Basic BDMP leaves for security modeling

Representation	Modeled behavior
	The "Attacker Action" (AA) leaf models an attacker's step towards the realization of his/her objective. In Idle mode, the action has not yet been tried. Active mode corresponds to attempts with a time to success exponentially distributed with a parameter λ. The Mean Time To Success (MTTS) for this action is equal to $1/\lambda$.
	"Instantaneous Security Event" (ISE) leaf models a security event that can happen instantaneously with a probability γ when the leaf switches from the Idle mode to the Active mode.

BDMP are used in the process of risk evaluation. Thanks to extensions described in [15], BDMP also allow detection and reaction modeling. We illustrate is Section 5 this ability and its utility to optimize the choice of countermeasures against attacks.

The details of the formal definition of BDMP are given in [15]. For reference, we show in Tab. 1 and Tab. 2 the main leaves used to build the BDMP models in the following and the behavior they model.

Besides the classical links used to connect a gate to its sons (represented as solid black lines), BDMP contain two special kinds of links described in Tab. 3.

BDMP have advantages both for building models and processing them. They are hierarchical, which means that in order to build a BDMP, the analyst starts from a high level of abstraction and progressively refines into detail levels. Abstraction is a fundamental mechanism used by the human mind for dealing with complexity. At each step in the reasoning (i.e. at each construction of a gate), the number of manipulated elements is small enough to reduce the possibility of errors. This process is also traceable, which implies that a model can easily be reviewed and checked, looking for potential incompleteness.

Table 3. Special links used in BDMP models

Representation	Modeled behavior
– – – – →	Defines the dynamic aspect of BDMP. The element pointed by the trigger link is not activated until the realization of the origin gate/leaf of the trigger. When this element becomes activated, it transmits the activation signal it receives from its parents to the sub-tree targeted by the trigger.
- - - - - - ▶	Creates a constraint in the order of realization of instantaneous events (on-demand failure leaves), in the case where they are required simultaneously.

The processing of BDMP is facilitated by the concept of "relevant events". The transition from false to true of a leaf (due to accidental failure or attack success) is said to be relevant if it changes the distribution of the instant where the top event will be realized. BDMP use a trimming mechanism of irrelevant events that considerably reduces the number of sequences explored by FigSeq and makes the explored sequences more interesting qualitatively (all the events listed in sequences are relevant). This concept and its advantages are described in details in the seminal paper on BDMP [2].

4 Illustration of Safety and Security Interdependencies

We propose in this section to show the importance of considering together security and safety aspects for an accurate risk evaluation and for decision-making in system design or exploitation.

4.1 Example of an Antagonism

We consider a person being at home and choosing whether to keep the house door locked or unlocked. When considering fire hazard and for safety reasons the door must be kept unlocked in order to facilitate evacuation. However, when considering potential attacks and for security reasons the door must be kept locked. This example is similar to the case of the exit door addressed by the literature in [19,4,5].

The undesirable event of our use case is some form of harm to the person, called later *person integrity affected*. We start our study by making a pure safety analysis considering only accidental events. The person can be harmed if a fire is accidentally initiated in the house and it is impossible for him to escape as the door is initially locked and the person cannot open it (lock blocked, keys not found). The BDMP given in Fig. 1 models this scenario. Here the *door locked* leaf corresponds to an instantaneous event which can happen with a probability of 0.5. The two triggers define the dependencies between the events associated to the leaves. When the *fire* leaf becomes true it creates, thanks to the first trigger, a mode change for the leaf *door locked*. Consequently, the latter can either stay false or switch to the true value (with probability of 0.5 for each alternative). If the *door locked* leaf becomes true it creates in turn a mode change for the leaf *door impossible to open*. According to the same mechanism, this leaf can instantly either remain false or take the value true. With this model, it is possible to see that the top event can never happen if the door is unlocked (i.e. when *door locked* takes the value false).

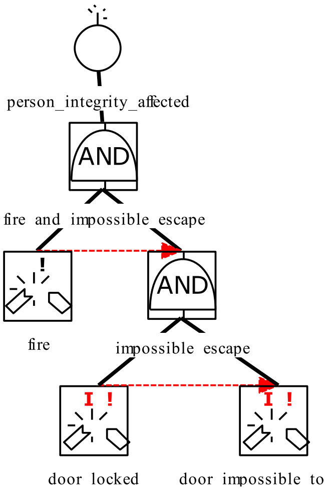


Fig. 1. BDMP modeling only safety hazards

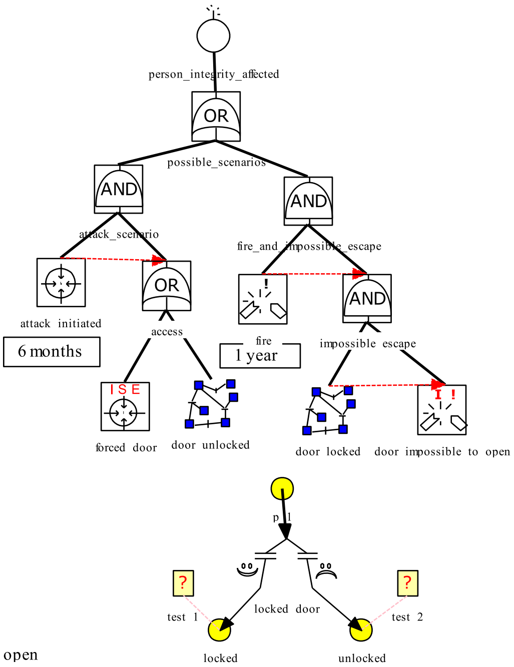


Fig. 2. BDMP modeling safety and security hazards

We consider in a second stage security-related events that may lead to the same undesirable event: a burglar can attack the person in the house to get the combination of a safe. The burglar can enter the house directly if the door is unlocked or he can force it if it is locked. We give in Fig. 2 the BDMP model covering both safety and security hazards. The Petri net models the fact that the door can be initially locked or unlocked with a probability of 0.5 for each alternative. Initially, a token is placed in p1. This token enables to activate at t=0 the transition *locked door* and at t > 0, the token is definitively either in place *locked* or in place *unlocked*. The Petri leaf *door locked* (resp. *door unlocked*) is true when there is a token in the *locked* (resp. *unlocked*) place (this is ensured through a non-graphical link between Petri leaves and the places).

Using the FigSeq tool we calculate for one month of mission time, the events realization probabilities (Pr) based on an estimation of the probabilistic param-

Table 4. Scenarios probabilities when the door is locked/unlocked

	Pr(attack scenario)	Pr(fire and impossible escape)	Pr(person integrity affected)
Locked	7.06e-02	7.85e-04	7.14e-02
Unlocked	7.06e-01	0	7.06e-01

eters of each BDMP leaf (fire estimated once a year, attack estimated once per 6 months, Pr(*forced door*)=0.1 and Pr(*door impossible to open*)=0.01). These parameters were chosen arbitrarily. The purpose of this example is not to give realistic estimates, but rather to show the reasoning. Results show that the probability of affecting the person integrity increases from 4.17e-4 when considering only safety hazards to 0.388 when considering additionally the attack scenario.

We give in Tab. 4 the probability of respectively the attack scenario, the accidental scenario (*fire and impossible escape*) and the top event (*person integrity affected*) in cases when the door is kept locked and when it is kept unlocked. The antagonism between safety and security is quantitatively verified: the probability of the attack scenario is lower when the door is locked while the accidental scenario is not possible when the door is unlocked. However, we can see that the top event probability is clearly higher when the door is unlocked. The optimal decision under the assumptions made here (this includes four parameters: the frequency of fire and attacks, and the probabilities of a burglar forcing the door and of the house occupant not being able to evacuate if needed) is to lock the door. If the parameters were radically different (house occupant is an old and blind heavy smoker, living in a very secure district, next to a police station), the quantification of the same model could lead to unlock the door.

Although elementary, this example shows the importance of considering safety and security together in the risk evaluation phase in order to identify possible conflicts between the two disciplines. Using BDMP we can not only identify the conflicts between safety and security measures, but also help choosing the most appropriate combination of security and safety measures for minimizing the global risk.

4.2 Example of Synergetic Interdependencies

We give in Section 5 a detailed case study inspired from the industrial domain. We do the same kind of analysis on this complex system in order to demonstrate possible synergies between safety and security measures.

5 Case Study

5.1 System Architecture Description

The system considered in the sequel is a hypothetical cyber-physical system used to transport a polluting substance. It is composed of a pipeline equipped with pumps used to force the stream and valves used to allow or block the stream. Throughout the pipeline sensors measure the pressure and flow inside each section of the pipeline. Each piece of equipment (pump or valve) is controlled by a Remote Terminal Unit (RTU) that communicates with a remote Control Center (CC). The tasks of the RTU are to:

- Collect data from sensors used to measure the pressure and the flow in the vicinity of each pump and valve;
- Control the operation/speed of pumps and the opening/closing of valves;
- Send data and alarm signals to the CC and receive instructions from it;
- Exchange with neighboring RTUs pressure measures and shutdown signals.

Safety requires RTUs to verify that the pressure in the pipeline does not exceed a maximum value P_{max}. Each RTU also calculates the pressure difference between the neighboring RTU and its own sensors: $\varDelta\mathrm{P} = |P_n - P_{n-1}|$. If $\varDelta\mathrm{P}$ exceeds a threshold $\varDelta P_{max}$, the RTU sends an alarm signal to the CC, which sends back an order to all RTUs to stop pumps and close valves. In addition the RTU sends a shutdown signal to its neighboring RTUs. The pressure difference threshold is generally reached when the pipeline is broken; this implies that the pressure measured before the break is too high compared to the pressure measured after the break, which makes the pressure difference large. A safety requirement enables each RTU to stop the pump or close the valve it controls when $\varDelta P_{max}$ is reached or when it receives a shutdown order from other RTU without waiting for CC instructions. This action is called later the "Reflex Action" and provides redundancy with CC instructions, with a higher priority. The architecture of the case study is given in Fig. 3. We assume RTUs are locally installed on pumps and valves and communicate with them via a wired link. Sensors which are relatively distant and scattered all through the pipeline use a wireless link to communicate with RTUs. Supposing that the pipeline is hundreds of kilometers long and that it is a hundred kilometers distant from the CC, we assume that communication is ensured by a GSM network. The industrial protocols used are Modbus/TCP for RTU-CC communication, Modbus/RTU for inter-RTUs communication and WirelessHART for sensor-RTU communication. These assumptions will be used later to estimate security events parameters.

5.2 System Modeling

The BDMP supporting a risk analysis of this system is given in Fig. 5. It models the different scenarios that lead to pollution of the environment (the top event). There are three types of possible scenarios: attack scenarios, accidental scenarios or hybrid scenarios. The first type of scenarios is a successful attack initiated by a malicious person, the second type is based on mere accidental events like failures of the system's components and the third type is a combination of attacks and components failures. This latter type best characterizes the possible interactions between safety and security events.

As explained in Section 3, BDMP use hierarchical reasoning in order to cover all the possible scenarios. The top event: pollution can be realized if and only

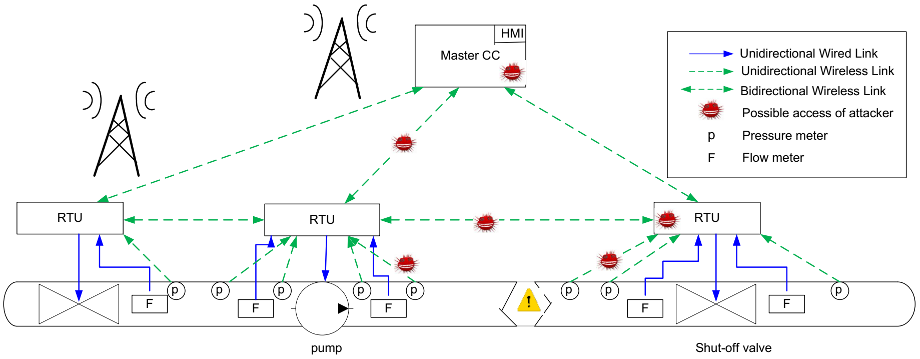

HMI
Master CC
Unidirectional Wired Link
Unidirectional Wireless Link
Bidirectional Wireless Link
Possible access of attacker
p Pressure meter
F Flow meter
RTU
RTU
RTU
F
p
p
F
p
p
F
p
p
p
F
F
p
pump
Shut-off valve

Fig. 3. Architecture of the case study

if the pipeline breaks and the protection system fails to react. The protection system refers to the detection of the pipeline break by RTUs and the system shutdown either thanks to the reflex action or by orders sent by the CC. The protection system can fail to react for two different reasons: either it was deactivated before the break by an attacker, or it accidentally does not work.

This reasoning corresponds to the top level of the BDMP. The gate named *attack protection syst then pipeline break* is a "PAND" gate, which becomes true only if its left input is true before the right input becomes true. If an attack is perpetrated after the pipeline break, this will not worsen the situation.

The Attack Scenario: We suppose that attacks for such an industrial infrastructure follow a Poisson process with an occurrence rate of once every 3 years. We assume that in the case of this pipeline, such a value can be defined based on the organization security historical data and on intelligence reports. The attack scenario starts by deactivating the protection system before provoking the pipeline breach by using the water-hammer phenomenon (closing suddenly a valve downstream when high velocity associated with a high pressure is propagating in the pipeline which causes a shock). In the attack preparation phase the attacker starts by getting access to the SCADA system: either by taking control over the CC (physically or remotely) or accessing physically to the RTU or creeping into the network via the communication link (between the RTU and the CC or between the sensors and the RTU). Secondly, the attacker must understand the system operation in order to be able to deactivate the protection system. Depending on what the attacker has gained access to, he will act differently in order to deactivate the protection. The attack steps in this phase will be quasi instantaneous (ISE security leaves) as the attacker has previously understood the system operation and is able to manipulate it. In order to deactivate the reflex action of RTUs the attacker can simply jam the communication between the RTUs so that the pipeline breach cannot be detected. The house event *No reflex action* models the existence or the non-existence of the reflex action as a safety measure implemented locally in the system; this leaf is set either to true or to false prior to any quantification. After preparing for his attack, the attacker is ready to break the pipeline with a water-hammer by provoking a high pumping pressure in the pipeline and closing suddenly the valve downstream which causes a pressure surge able to create a breach at the weakest point in the pipeline.

The Accidental Scenario: In this case pollution is caused if the pipeline breaks accidentally then the protection system fails to react. The protection failure is realized in two cases: no instructions given by the RTU or the on-demand failure of the equipments (valves and pumps) to react properly. The first case is realized if the RTU fails or if it doesn't react which implies that it receives no instruction from CC and it does not activate its reflex action. Safety leaves of the BDMP detail the accidental events leading to such scenarios.

The Hybrid Scenario: This scenario is built up from both accidental and malicious events. We can imagine that the attacker can remotely deactivate the protection system then give up the attack because he does not succeed in creating the water hammer. Then he can just wait until the pipeline breaks accidentally instead of trying another attack. This scenario has a very low probability and supposes that the protection system deactivation is not detected until the pipeline breaks.

5.3 Qualitative and Quantitative Analysis

To make the quantification, we associate the model leaves with parameters based on the estimation of the MTTS for security events, the MTTF for safety events and the probability for instantaneous events (see Tab. 1 and Tab. 2). These parameters are estimated by security and safety experts based on the assumptions we made on the protocols and the network (see Section 5.1). We also suppose that the attacker has a minimum knowledge of SCADA systems and protocols without necessarily being an insider. These parameters are marked on the model in Fig. 5 with comment boxes.

Results given below were obtained with FigSeq, as explained in Section 4.1. Based on the given parameters the pollution probability is estimated to about 2e-2 for a mission time of one year. We can see that attack scenarios are situated at the top of the list of scenarios. The most probable attack scenario given in Tab. 5 is the one in which the attacker gets access to the RTU, takes control over the equipments and sends false data to the CC and to the neighboring RTUs.

We give in Tab. 6 the probability of the most probable attack sequences according to the type of access. We infer from results that the RTU is the most critical and vulnerable component in our case study. Being left on the pipeline with little physical protection it is easy to attack. These results are of course based on the estimations we give to parameters, for instance we supposed that sensors communicate with RTUs using the WirelessHART protocol which is a secured protocol using authentication and encryption. The attacker must first find a vulnerability before gaining access to the communication link. On the other hand, the Modbus/TCP protocol used for RTUs and CC communication is not secured and data can be clearly read once the attacker accesses the GSM network.

Table 5. Most probable attack scenario from the BDMP model

Transitions		MT Proba	Contrib.
Name	Rate		
failF(attack occurence)	2.28e-5	1.31e-2	0.67
aa success(access to RTU)	0.0208		
aa success(understand syst operation)	0.0208		
ise nd real(falsify data sent to CC) ise nd real(falsify data sent to other RTUs) ise nd real(falsify instructions sent to equipments)	0.6 0.6 0.7		
ise nd real(high pumping pressure activation)	0.7		
ise nd real(closing valve)	0.7		

Table 6. Probability of attack sequences according to the type of access

Type of access	RTU	CC	CL(RTU & CC)	CL(sensors & RTU))
Pr(pollution)	1.31e-2	2.92e-3	7.85e-04	1.62e-4

The first hybrid scenario given in Tab. 7 has a probability of 4.03e-4, in which the attacker deactivates the protection system then gives up the attack before the pipeline breaks accidentally.

The first accidental scenario given in Tab. 8 appears with a probability of 1.98e-5 and consists of accidental break of the pipeline and failure of the sensors to communicate correct measures to RTUs. Redundancy among sensors and the elimination of single points of failure could be considered to prevent such accidental scenarios. Results demonstrate that the hybrid scenario is more probable than the accidental scenario. Security events accelerate very much the realization of the undesired event (pollution).

5.4 Safety and Security Interdependencies

We propose in this section to highlight the possible interdependencies between safety and security in the use case, and to illustrate how the model can be used to choose appropriate detection and reaction measures.

Mutual Reinforcement: The reflex action is a safety module implemented locally at each RTU in order to act in case of accidental pipeline break. In order to assess its influence on the system we calculate the pollution probability with and without reflex action (*No reflex action* leaf activated/deactivated). Results demonstrate that the pollution probability increases by 13 % if no reflex action is implemented at the RTUs (1.95e-2 with reflex action to 2.2e-2 without reflex action). The reflex action represents an additional barrier for the attacker to overcome. If the attacker causes the pipeline breach without deactivating the reflex action this latter would react to prevent pollution as the breach would be

Table 7. The most probable hybrid scenario

Transitions		MT Proba	Contrib.
Name	Rate		
failF(attack occurence)	2.28e-5	4.03e-4	0.026
aa success(access to RTU)	0.0208		
aa success(understand syst operation)	0.0208		
ise nd real(falsify data sent to CC) ise nd real(falsify data sent to other RTUs) ise nd real(falsify instructions sent to equipments)	0.6 0.6 0.7		
no realization(high pumping pressure activation)	0.3		
failF(pipe break accidentally) failF(pipe break accidentally)	1.14e-5 1.14e-5		

Table 8. Most probable accidental scenario

Transitions		MT Proba	Contrib.
Name	Rate		
failF(pipe break accidentally)	1.14e-5	1.98e-5	1.01e-3

good(CC RTU communication lost)
good(Control Center)
good(RTU)
good(faulty operator)
failI(faulty sensor measure)
good(inter RTU communication lost)
	0.99954
	0.999886
	0.999862
	0.99977
	0.00023
	0.9993		

detected by RTUs. We can infer consequently that this safety measure reinforces the system security.

Conditional Dependency: This kind of interdependency is the most common and implies that the safety level is dependent on the security level. This is more straightforward as, generally, the attackers' goal is to cause safety accidents through compromising the system security. This interaction is illustrated in the two following situations:

- As modeled in Fig. 5 the attacker can access the system via the wireless communication link between sensors and RTUs which is more difficult when the communication is secured. In this case the attacker can manipulate data sent by the sensors to RTUs in order to deactivate the reflex action. The attacker can even exploit the normal functioning of the reflex action to cause the pipeline breach; typically send low pressure measures to the RTU controlling the pump to activate high pumping speed and then when high pressure is reached the attacker can send false low pressure measures to the RTU controlling the valve downstream. This RTU will calculate a high ΔP (high P_{n-1} received from the previous RTU and low P_n given by the attacker)

and close the valve leading to a water-hammer. We remind that the reflex action is considered to have a higher priority as a safety module over CC instructions as this latter might detect inconsistencies in the RTUs measures.
- Strengthening the system security by adding detection and defense measures enhances the system safety as it contributes to the reduction of pollution probability. It is possible to include detection aspects in the BDMP model. The general idea is that each attack step can be detected at various moments: when it begins, during its progress, when it succeeds, or after completion. Whenever detection occurs, this changes all success rates or probabilities for attack steps which are still to be completed. The only thing the analyst has to do to take detection into account in the BDMP model is to change a global option in the model and add in each security leaf the detection rate and the realization rate after detection. This does not require any change in the BDMP structure. These detection parameters are taken into account in the quantitative processing. This increases considerably the number of sequences to explore, because each scenario of the model without detection can lead to many variants with detection occurring at various stages.

In order to evaluate the efficacy of detection we have done a sensitivity analysis; the results obtained are given in Fig. 4. We first assess the pollution probability evolution in two extreme cases: without any attack and with attacks but without any detection mechanism. Then we take into account detection and response measures and compare two detection strategies. We can model in the BDMP many detection strategies and various responses for each of them; we have chosen a simple scenario in order to be able to explain it concisely. We suppose that in the so-called "good detection" strategy, the RTU attack is detected at the instant where it succeeds with a probability γ ($\gamma \in [0.5 , 0.9]$). No other detection mechanism is implemented. The reaction is the fact that the subsequent attack step becomes impossible: the attack is completely blocked. To obtain the "bad detection" strategy, one simply has to replace "RTU" by "communication link between sensors and RTUs"' in the previous description. We have chosen here to place detection measures at the beginning of the attack on the components that are most and least likely to be attacked (cf. Tab. 6).

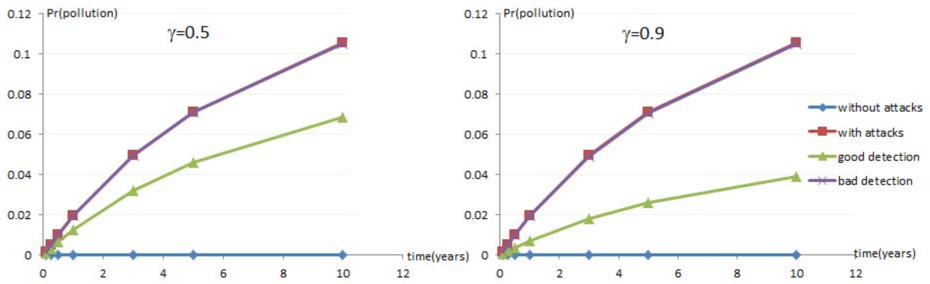
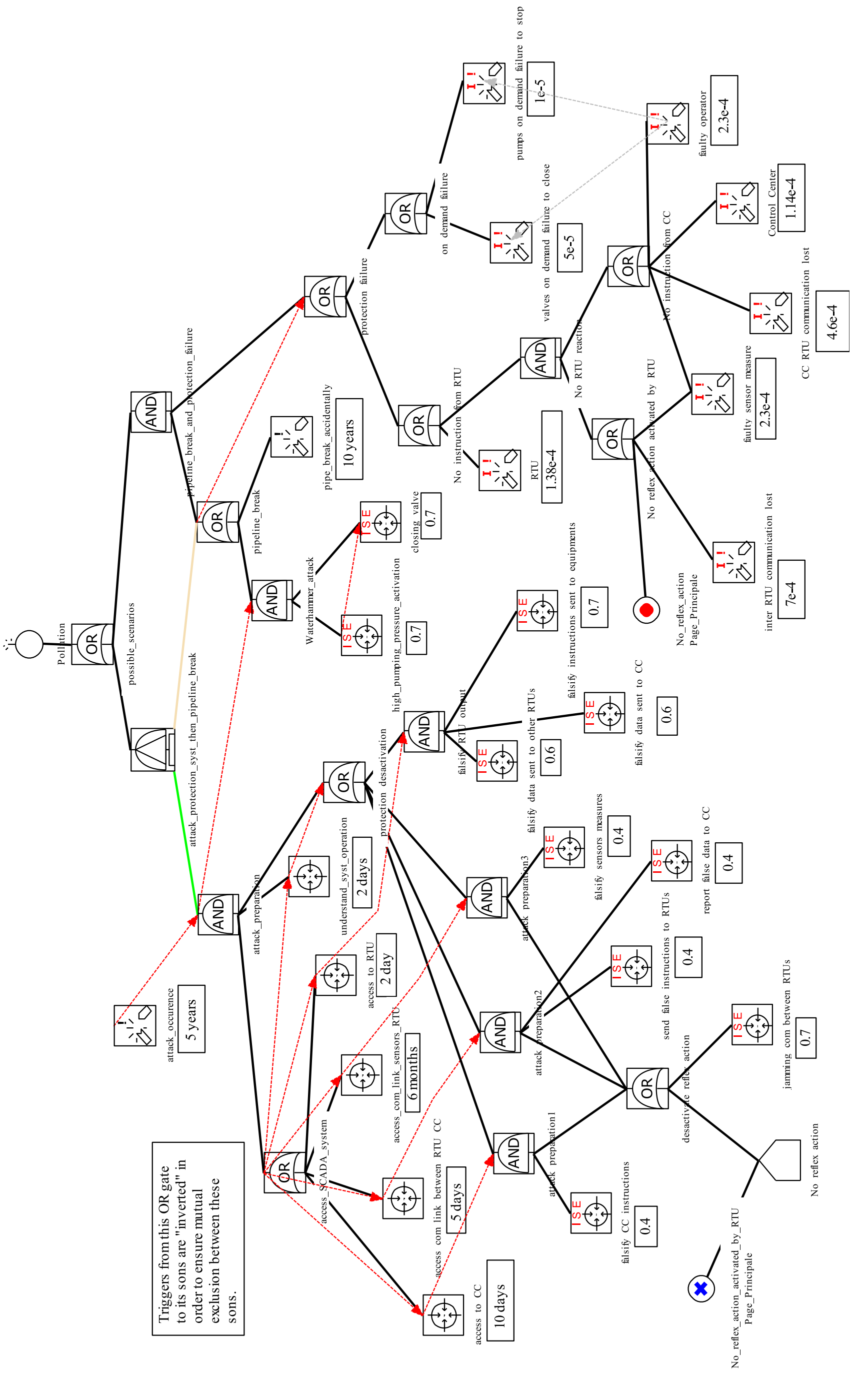


Fig. 4. Comparison of various detection strategies



Triggers from this OR gate to its sons are "inverted" in order to ensure mutual exclusion between these sons.

Fig. 5. BDMP model of the pipeline and its control system

We can infer from results that security related scenarios increase considerably the pollution probability (factor of 400 between the two extreme cases). We can also see that the influence of a bad detection strategy on the pollution probability is negligible whatever the detection probability (γ). However introducing a good detection strategy decreases significantly the pollution probability especially when the detection probability is high (almost 43% of pollution reduction when detection probability passes from 0.5 to 0.9). We infer from this sensitivity analysis the importance of the qualitative analysis given in Section 5.3 in the identification of the weakest point of the whole system and consequently the right detection strategy.

In this second example we have been able to put into evidence synergetic interactions between safety and security by modeling safety and security events in an industrial architecture. The qualitative and quantitative analyzes enable to rank the scenarios leading to the undesirable event and to identify the most probable scenarios. It is consequently possible to point out the most vulnerable items in the system and take preventive measures accordingly.

6 Conclusion and Future Work

We have illustrated in this paper the interest of considering safety and security aspects in a more integrated fashion in the risk evaluation process. Using the BDMP formalism we have modeled two examples: a simple common example and a more elaborated industrial case study. Thanks to the qualitative and quantitative capacities of the formalism one can characterize different interdependencies between safety and security: antagonism, conditional dependency and mutual reinforcement.

The main limitation of this work comes from the difficulty to evaluate the parameters associated to the security leaves of the model. Therefore we intend to work on the robustness of the decisions that can be taken, based on such analyzes. Our aim it to be able to determine decisions that remain valid for a wide range of values of the most uncertain parameters.

References

1. Bieber, P., Blanquart, J.P., Descargues, G., Dulucq, M., Fourastier, Y., Hazane, E., Julien, M., Leonardon, L., Sarouille, G.: Security and safety assurance for aerospace embedded systems. In: Proceedings of the 6th International Conference on Embedded Real Time Software and Systems, Toulouse, France, pp. 1–10 (2012)
2. Bouissou, M., Bon, J.-L.: A new formalism that combines advantages of fault-trees and markov models: Boolean logic driven markov processes. Reliability Engineering & System Safety 82(2), 149–163 (2003)
3. Chiaradonna, S., Di Giandomenico, F., Lollini, P.: Case study on critical infrastructures: Assessment of electric power systems. In: Wolter, K., Avritzer, A., Vieira, M., van Moorsel, A. (eds.) Resilience Assessment and Evaluation of Computing Systems, pp. 365–390. Springer, Heidelberg (2012)

4. Eames, D.P., Moffett, J.D.: The integration of safety and security requirements. In: Felici, M., Kanoun, K., Pasquini, A. (eds.) SAFECOMP 1999. LNCS, vol. 1698, pp. 468–480. Springer, Heidelberg (1999)
5. Hunter, B.: Integrating safety and security into the system lifecycle. In: Improving Systems and Software Engineering Conference (ISSEC), Canberr, Australia, p. 147 (August 2009)
6. Kornecki, A., Subramanian, N., Zalewski, J.: Studying interrelationships of safety and security for software assurance in cyber-physical systems: Approach based on bayesian belief networks. In: 2013 Federated Conference on Computer Science and Information Systems (FedCSIS), pp. 1393–1399 (2013)
7. Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S.: Experimental security analysis of a modern automobile. In: 2010 IEEE Symposium on Security and Privacy (SP), pp. 447–462 (2010)
8. Kriaa, S., Bouissou, M., Pietre-Cambacedes, L.: Modeling the stuxnet attack with BDMP: towards more formal risk assessments. In: 2012 7th International Conference on Risk and Security of Internet and Systems (CRiSIS), pp. 1–8 (2012)
9. Nai Fovino, I., Masera, M., De Cian, A.: Integrating cyber attacks within fault trees. Reliability Engineering & System Safety 94(9), 1394–1402 (2009)
10. Novak, T., Gerstinger, A.: Safety- and security-critical services in building automation and control systems. IEEE Transactions on Industrial Electronics 57(11), 3614–3621 (2010)
11. Pietre-Cambacedes, L., Bouissou, M.: Beyond attack trees: Dynamic security modeling with boolean logic driven markov processes (BDMP). In: Dependable Computing Conference (EDCC), 2010 European, pp. 199–208 (2010)
12. Pietre-Cambacedes, L., Bouissou, M.: Modeling safety and security interdependencies with BDMP (boolean logic driven markov processes). In: IEEE International Conference on Systems Man and Cybernetics (SMC), pp. 2852–2861 (2010)
13. Pietre-Cambacedes, L., Bouissou, M.: Cross-fertilization between safety and security engineering. Reliability Engineering & System Safety 110, 110–126 (2013)
14. Pietre-Cambacedes, L., Deflesselle, Y., Bouissou, M.: Security modeling with BDMP: from theory to implementation. In: 2011 Conference on Network and Information Systems Security (SAR-SSI), pp. 1–8 (2011)
15. Pietre-Cambacedes, L., Bouissou, M.: Attack and defense dynamic modeling with BDMP (extended version). Tech. rep., Technical Report, Telecom ParisTech (2010)
16. Pietre-Cambacedes, L., Chaudet, C.: The SEMA referential framework: Avoiding ambiguities in the terms “security” and “safety”. International Journal of Critical Infrastructure Protection 3(2), 55–66 (2010)
17. Smith, J., Russell, S., Looi, M.: Security as a safety issue in rail communications. In: Proceedings of the 8th Australian Workshop on Safety Critical Systems and Software, SCS 2003, vol. 33, pp. 79–88. Australian Computer Society, Inc., Australia (2003)
18. Steiner, M., Liggesmeyer, P.: Combination of safety and security analysis-finding security problems that threaten the safety of a system. In: Proceedings of Workshop DECS (ERCIM/EWICS Workshop on Dependable Embedded and Cyber-physical Systems) of the 32nd International Conference on Computer Safety, Reliability and Security (2013)
19. Sun, M., Mohan, S., Sha, L., Gunter, C.: Addressing safety and security contradictions in cyber-physical systems. In: 1st Workshop on Future Directions in Cyber-Physical Systems Security (CPSS 2009), Newark, United States (2009)