Automatic Verification and Diagnosis of Security Risk Assessments in Business Process Models

ÁNGEL J. VARELA-VACA [1], LUISA PARODY[2], RAFAEL M. GASCA[1], AND MARÍA T. GÓMEZ-LÓPEZ[1]

[1]Department of Languages and Computer Systems, Universidad de Sevilla, 41004 Seville, Spain
[2]Department of Quantitative Methods, Universidad Loyola Andalucía, 41014 Seville, Spain

This work has been partially funded by the Ministry of Science and Technology of Spain by ECLIPSE and SEQUOIA (TIN2015-63502-C3-2-R) projects, the European Regional Development Fund (ERDF/FEDER), and the Cátedra of Telefónica.

ABSTRACT Organizations execute daily activities to meet their objectives. The performance of these activities can be fundamental for achieving a business objective, but they also imply the assumption of certain security risks that might go against a company's security policies. A risk may be defined as the effects of uncertainty on the achievement of the goals of a company, some of which can be associated with security aspects (e.g., data corruption or data leakage). The execution of the activities can be choreographed using business processes models, in which the risk of the entire business process model derives from a combination of the single activity risks (executed in an isolated manner). In this paper, a risk assessment method is proposed to enable the analysis and evaluation of a set of activities combined in a business process model to ascertain whether the model conforms to the security-risk objectives. To achieve this objective, we use a business process extension with security-risk information to: 1) define an algorithm to verify the level of risk of process models; 2) design an algorithm to diagnose the risk of the activities that fail to conform to the level of risk established in security-risk objectives; and 3) the implementation of a tool that supports the described proposal. In addition, a real case study is presented, and a set of scalability benchmarks of performance analysis is carried out in order to check the usefulness and suitability of automation of the algorithms.

INDEX TERMS Business process management business process model security-risk assessment model-based diagnosis constraint programming.

I. INTRODUCTION

Organizations carry out several activities to meet their objectives. The execution of each of these activities can imply tackling certain security risks. For example, when a web service is published to provide the products of an organization, data leakage or loss of confidentiality can occur, although these updates are essential for the modernization of the organization. Moreover, the activities are not executed solely in an isolated manner; they can be choreographed by using business processes models formed of a set of activities [1] whose execution can imply tackling more complex security risks. Therefore, the analysis of the business processes [2] is crucial to understanding the impact of the possible risks. In this work, risks refer to IT security risks. A risk is defined as the effects of uncertainty on the achievement of the goals (e.g.; data corruption or unauthorized access). The decision to execute a business process in a company to achieve its objective [3] implies the acceptance of the derived risk (or even operational risks [4]). This derived risk is a combination of single risks associated with the activities that conform to the process. The risk assessment of business process models is crucial to detecting potential security risks. For instance, business process compromise attacks [5] are used in an attempt to understand a business process behavior with the aim of manipulating it and generating specific profits for attackers. After understanding a process behavior, an attacker might deploy malware within certain tasks that are executed unintentionally by an employee. This malware can allow the attacker the unauthorized access to the systems, such as access to confidential information. Therefore, the organization must measure and assess the isolated risks and combined activity risks that can cause this type of threat in their business process models (e.g.; data leakage caused by staff). The main

objective should be determine which tasks might potentially be affected by these threats.

Organizations are becoming increasingly complex but security-aware, because their services tend to be automated and published on software platforms. However, only a few organizations assess their security risks [6]. A vast number of risk methodologies are available, such as *MAGERIT*© [7], *CRAMM*© [8], COSO [9], CORAS [10], and the use of standards such as ISO/IEC 27000 series, NIST SP 800-30, AS/NZS 4360:2004, and BS 7799-3:2006. The main objectives of these methodologies include the identification of risks that could compromise the normal work of the organization, the identification of the assets that could be affected, and the remedial action(s) that must be adopted. Each method and standard provides its own metrics and catalogs to carry out risk management. Although these methods address risks from a general point of view, open problems persist. In this paper, we focus on how the partial risk of the activities combined in the business processes of the companies can affect the global risk of the organization. Another important point to analyze is the automation of this risk analysis for combined activities because the implementation of the majority of these methods [11] implies a manual, informal, textual, detailed and complex process. This process requires a large investment in resources by the organization [11].

The standards ISO/IEC 27005:20018 [12] and UNE 71504:2008 [13] identify business processes and information as relevant assets to be measured in organizations. Unfortunately, the proposals found in the literature are oriented towards the definition of risk for each single activity. To the best of our knowledge, there is no solution that infers the security-risk level of the entire process and takes into account the work-flow that combines the tasks and the partial risk.

This paper focuses on combining together business process management (BPM) and security-risk description. More concretely, determining how to obtain the level of risk for the entire process and how to identify the risk responsible for a nonconformity are paramount to this relationship. To achieve it, the proposals of the paper include (1) a framework for a risk-aware design and the development of business process models; (2) a verification algorithm that checks whether every trace of the annotated process model satisfies the risk objectives determined by the organization; (3) an algorithm to diagnose the risk responsible in the case of a nonconformity; and (4) the integration of the previous proposals into an implemented tool that supports graphical design, verification and diagnosis.

This paper is structured as follows: Section II introduces a motivating case study. Afterwards, the set of elements involved in risk-aware business processes is formalized in Section III, and the extension of the business process models is detailed in Section IV. In Section V, the verification and diagnosis of a risk-aware business process model is formulated. Section VI describes the associated models and algorithms to verify and diagnose the problem in an automatic manner. In Section VII, our proposed framework and the implemented tools are explained. Section VIII describes the application of the tools to the motivating case study and Section IX discusses the results pertaining to the scalability and the performance of our tool. Section X provides an overview and comparison of related work found in the literature. Finally, conclusions are drawn and future work is proposed in Section XI.

II. MOTIVATING CASE STUDY OF RISK ASSESSMENT

To illustrate the scope of the proposal, the case study depicted in Figure 1 is used. The example shows a business process model that describes the hiring process steps in an organization. This process is an adaptation of a real business process from the Bonita Open Solution suite of examples [14] and is very similar to the processes that might be audited in an ISO/IEC 27001:2018 certification. The process tends to be automated for the organization because different departments are involved and various tasks can programmed. Figure 1 describes three business processes, divided into different pools that represent the three departments of the organization, *human resources*, *hiring nanager* and *IT*. In this paper, we use BPMN 2.0 [15] as the business process standard which permits us to describe the relational order between the activities in an imperative manner. Following BPMN 2.0, every business process starts with a start event and ends with an end event (both represented by a circle). The execution order of the activities (rounded rectangles) is determined by the control flow (arrows) and gateways ($+$ or $\times$) for parallel and exclusive execution of their branches. The *human resource* process includes activities related to managing the register with the social security administration and payroll of employees. The *hiring manager* organizes the place to work and the accreditation to company access. The *IT* business process configures the software profile and hardware requirements.

The business process models must be assessed. To this end, as shown in Table 1, security experts have identified a set of threats that could affect those processes.

III. FOUNDATIONS: RISK-AWARE BUSINESS PROCESS MODELS, VERIFICATION AND DIAGNOSIS

Risk is defined by ISO/IEC 27005:2018 [12] as the estimation of the degree of the value of exposure to a threat that materializes over a number of assets causing damage or loss to the organization. It is particularly important to analyze when organizations use business process and software solutions as a service (BPaaS or SaaS). In these cases, security risk analysis is essential due to the outsourced services. The risk estimation is based on a risk formula that involves certain metrics, which refers to business process model elements and threats. Formally, the estimation of risk can be defined as follows:

Definition 1: A **risk**, R_i, is defined by a *formula*, f_{R_i}, used to estimate the value of risk with regard to the combination of a set of metrics ($m_1 \times m_2 \times m_3 \cdots \times m_p$) related to assets and threats.

$$f_{R_i} : m_1 \times m_2 \times m_3 \cdots \times m_p \rightarrow R_i \tag{1}$$

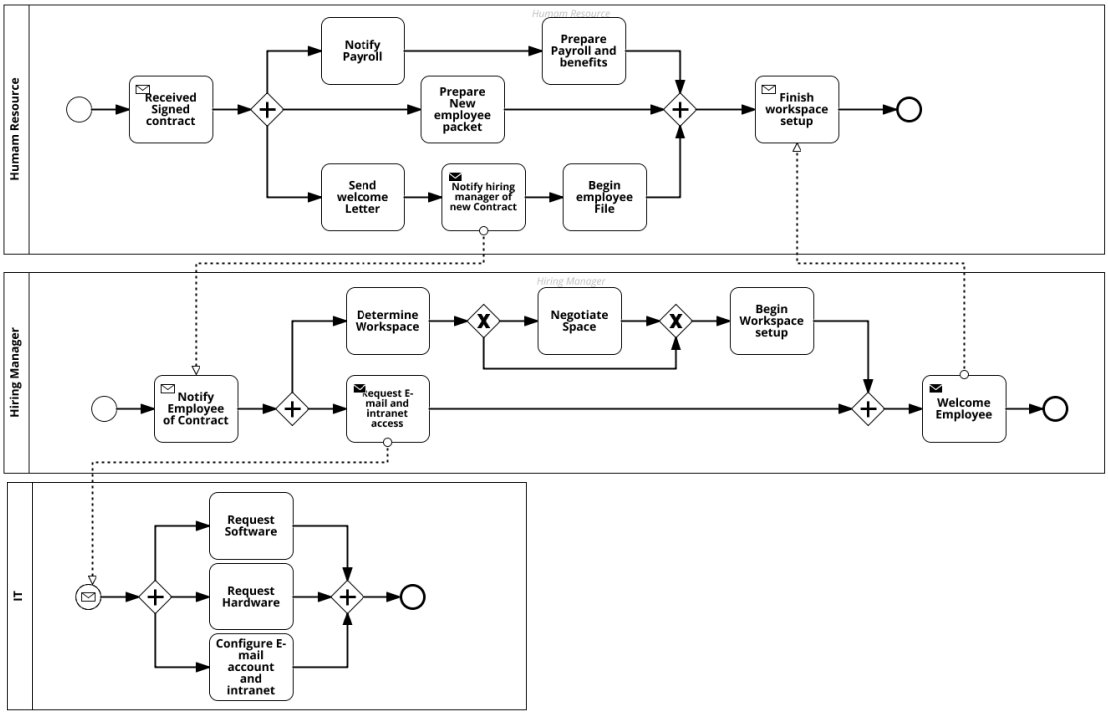


FIGURE 1. **Business process model of the arrival of a new employee to an organization.**

TABLE 1. **Description of threats.**

Abbr.	Name	Description
R11	Incidents caused by staff	Refers to incidents produced by misuse of resources such as misuse of email access, web access, and unauthorized access to systems and/or data.
R12	System failure or data corruption	Refers to failures produced by flaws in software or hardware components such as software bugs or a computer crash. A technical failure can be catastrophic if, for example, crucial data are lost on a failed hard drive and no backup copy is available.
R13	Infrastructure failures	Refers to failures produced in the infrastructure of the organization that interrupts the business process such as the loss of an Internet connection can interrupt business.
R21	Infection by viruses or malicious software	Refers to infections produced by viruses or malicious software that interrupts the correct functioning of the resources (e.g., computers, software).

Frequently, a risk formula combines the value of an asset, the frequency of appearance, and the consequence of the execution of a certain threat. Therefore, a risk formula can be represented by the following formula:

$$Risk = value * consequence * frequency \tag{2}$$

As previously mentioned, ISO/IEC 27005:2011 [12] and UNE 71504:2008 [13] establish processes as relevant assets to be considered in risk assessment. In our approach, we assume as assets both a business process model and an activity within it. Therefore, a risk can be associated with an execution of the entire business process and the combination of the execution of its activities. In any case, the definition of the business process model is essential to identify the possible risks. The example introduced in Figure 1, BPMN 2.0 is used to describe the business processes.

Definition 2: A **business process model**, BP_k, is composed of a set of m activities $\{A_1, A_2, \cdots, A_m\}$ and events (i.e., start, intermediate and end) that are performed in coordinated manner using a set of control-flow gateways (i.e., AND, OR, XOR) that describe the relationship between them.

Despite the existence of a wide range of business process modeling languages such as BPMN 2.0, Petri Nets [16], Event-driven Process Chain (EPC) [17], and UML Activity Diagram [18], none define specific issues concerning risk management.

A risk must be estimated by combining of the risk obtained for each individual activity and regarding the control-flow perspective of the business process model.

Definition 3: The risk of a BP_k is a combination of the risk of each activity $\{R_{A_1}, R_{A_2}, \cdots, R_{A_m}\}$ of the model, according to the order relation between the activities defined by the control-flow.

$$R_{BP_k} = f_{ControlFlow}(R_{A_1}, R_{A_2}, \cdots, R_{A_m}) \tag{3}$$

The estimation of these risk values is part of the risk assessment procedure. Thus, the estimation of a risk only produces a value that must be compared with the acceptable level of risk included in the company goals. This acceptable level of

risk can be used as a risk threshold to verify whether a specific value associated with a risk is acceptable. Organizations must establish a set of business goals related to the appraised value, e.g., a risk of a business process BP_i is acceptable if $R_{BP_i} \leq n$, where n may be the acceptable risk threshold.

Definition 4: A **risk-aware business process** model (**RBP**) is described by the tuple $\langle R_{BP_k}, BP_k, BG_j \rangle$, where R_{BP_k} represents the risk related to the business process model BP_k, and BG_j represents a business goal which establishes, for instance, a threshold of acceptable risk for a R_{BP_k}:

$$RBP \equiv \langle R_{BP_k}, BP_k, BG_j \rangle \tag{4}$$

In general, this risk threshold is fixed globally for the risk assessment. This threshold allows for the comparison of the acceptable level of risk with the risk of business processes.

Definition 5: **Verification of RBP conformance** (**VRC**) is defined of the tuple $\langle RBP, con_{p_i} \rangle$, where con_{p_i} is a set of elements $\{p_1, p_2, p_3, \cdots, p_n\}$, where each p_i is a tuple $\langle Risk_{A_k}, \text{bool}_k \rangle$, where bool_k is a Boolean value that represents whether the $Risk_{A_k}$, which belongs to a process, BP_k in RBP, satisfies the risk criterion according to the business goals, BG_j in RBP.

$$\bigcup_{i=1}^{n} p_i \cup BG_j \nvdash \top \tag{5}$$

The system con_{p_i} is unsatisfiable with regard to the BG_j constraints established, i.e. if any $bool_k$ is *false*. Therefore, the risk of each activity has a truth value that describes the conformance to the goals.

The execution flow of activities in a business process model is specified by arrows (i.e., sequence flows in BPMN) and control flow elements (i.e., gateways in BPMN) between the activities. A business process model is composed of various potential sequences of execution flows, which are possible paths of executions.

Definition 6: A **potential execution flow (PEF)**, PEF_i consists of a possible sequence of activities $\{A_1, A_2, \cdots, A_m\}$ that can be executed according to the work-flow [19]. PEF_i, is a set of activities that corresponds to a possible instance in a business process model from a start event to an end event of a BP_k.

To determine what happens when the risks exceed the expected goals, the identification of which element produces the fault responsible for the nonconformity is necessary. However, it is also important to note the problems to define a treatment plan and thereby diagnose which is the risk responsible. We propose the use of a model-based diagnosis [20] to detect the parts of a system that fail in accordance with the expected model [20], [21]. This model-based diagnosis must be adapted to risk-aware business process models, which implies the analysis of the conformance of the business process model and each PEF.

The diagnosis aims to identify the activities whose associated risk produces an inconsistency. This identification might be achieved by fault diagnosis theory. The fault diagnosis of a *VRC* identifies the set of activities of the business process model BP_i in RBP that are responsible for the inconsistency. The diagnosis therefore strives to determine why a risk-aware business process model is unexpectedly nonconforming to the acceptable risk level.

Definition 7: The **fault diagnosis of a VRC** is the minimal subset of activities, $\triangle$, that belong to the PEFs, such that $\triangle$ contains at least one activity for each PEF_k where the $bool_k$ element of p_i is *false* (cf. Def. 5). The subset $\triangle$ of PEF_k is minimal iff no proper subset of $\triangle$ is a fault diagnosis of PEF_k. In this work, only the minimal diagnosis is considered.

$$(\bigcup_{i=1}^{n} p_i - \triangle) \cup BG_j \vdash \top, \quad \triangle \subseteq \bigcup_{a \in PEF_k} \tag{6}$$

IV. RISK EXTENSION FOR BUSINESS PROCESS MODELS IN A NUTSHELL

In previous works, we defined a lightweight extension of the BPMN 2.0 meta-model [22], [23]. This extension derives from two main models UML Profile for Modeling Quality of Service and Fault Tolerance (hereinafter *QFTP*) [24] and Business Motivation Model (*BMM*) [25]. *QFTP* provides a set of generic concepts to develop risk assessment capabilities within IT systems. In contrast, *BMM* provides a model for defining and developing business plans. Business plans are carried out in a final stage by business processes [3]. Thus, *BMM* enables both the identification of factors and relations to define business plans and determine how to achieve and assess these plans.

As an example of the extension the *IT* process from the proposed case study is illustrated in Figure 2. The pools are extended with information related to the objectives and threat scenarios. These threat scenarios enable the definition of the threats and countermeasures to be considered for the risk assessment. Each activity is enriched the corresponding metrics along three security dimensions and linked to the threats from the scenario. More information about the elements of the extension is provided in [22] and [23].

V. RISK ASSESSMENT OF BUSINESS PROCESS MODELS

The risk assessment of the business processes of an organization is crucial to detecting and avoiding undesirable situations. The extension of the BPMN metamodel described in the previous section to a business process management system provides a mechanism for automating the risk assessment and the detection of nonconformance elements, minimizing human intervention. To this end, this section introduces how the partial risk of the activities can be combined in a formulation to carry out the estimation of risk of an entire business process model. This formulation is based on a set of patterns according to the control-flows included in the process, which are used afterwards to verify the conformance of the process. In our approach, independence on the activities risk is assumed.

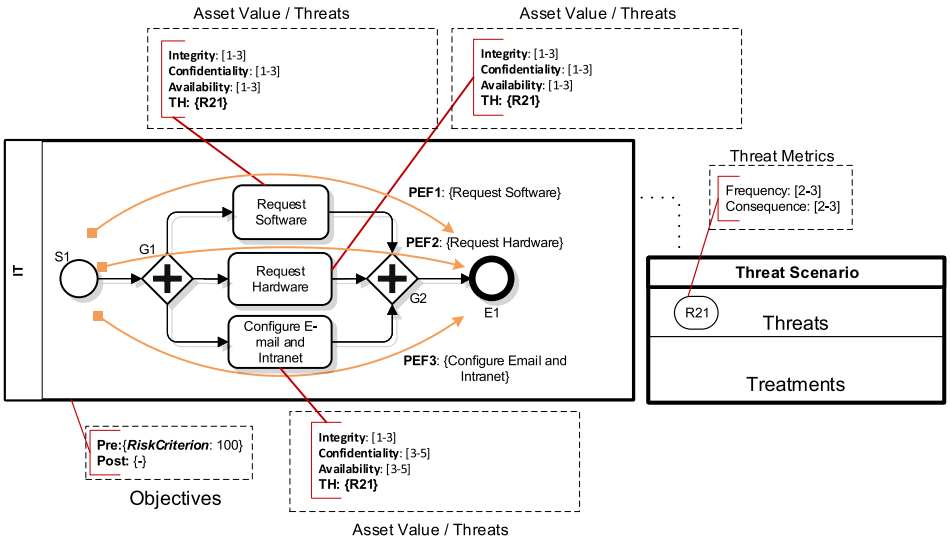


FIGURE 2. **Example of business process model extended for risk assessment.**

A. CONTROL-FLOW PATTERN-BASED RISK ESTIMATION

Following Def. 1, the risk of an asset must calculated by means of a formula. This formula is defined based on metrics related to the activities and the threats. Numerous risk assessment methods are widely used in the estimation of risks, such as FMEA [26] and MAGERIT [7]. In our approach, the following risk formula is adopted. Nevertheless, we must highlight that any other risk formula can be easily adopted for our approach.

$$Risk^{D}_{A_i} = Value^{D}_{A_i} * Consequence^{D}_{th_j} * Frequency^{D}_{th_j} \quad (7)$$

In this formula, D refers to security dimensions (e.g., *Integrity, Confidentiality and Availability* of the asset, and *Consequence* and *Frequency* refer to properties of a particular threat.

The risk formula could consider countermeasures. This consideration requires to adjusting the risk formula by subtracting the *risk reduction* (RR) of *consequence* and/or *frequency* of threats. Therefore, the *consequence* and the *frequency* can be reformulated as follows:

$$f^{RR}_{C} = Consequence^{D}_{th_j} - \frac{Consequence^{D}_{th_j} * RR^{D}}{100} \quad (8)$$

$$f^{RR}_{F} = Frequency^{D}_{th_j} - \frac{Frequency^{D}_{th_j} * RR^{D}}{100} \quad (9)$$

These reductions can be included in the risk formula as follows:

$$Risk^{D}_{A_i} = Value^{D}_{A_i} * f^{RR}_{C} * f^{RR}_{F} \quad (10)$$

In our approach, risks and threats are associated with activities. Therefore, the main problem is determining how to address the risk of the entire business process model. Our approach considers that the risk of a business process model should be estimated through the combination of the risks of each individual activity regarding the control-flow of the business process model.

The standard ISO/IEC 27005:2011 [12] in its Appendix E applies an average to determine the global risk for a set of assets. Subsequently, this standard suggests the suitability of this average for the risk determination of business processes. As proposed in the mentioned standard, a set of patterns for risk estimation as the average of the activities of a business process model is provided in [23].

A generic formulation based on those patterns and the average is proposed and specified in the *Formula* column of Table 2. These risk formulas take into account the structure of the business process and the average as a similar adaptation to the estimation of the time-efficiency proposed in [27] and the estimation of security proposed in [28]. The defined formulas are examples that illustrate each pattern because they can be customized. Business processes with a complex structure can be calculated using a combination of these patterns. This combination results in an approach for determining the average of the risk of the activities for an entire business process.

As an illustration, a small example of one risk estimation of the business process *BP1* is established in Figure 3. The risks of the activities of *BP1* are assumed as already calculated for the dimension of integrity: $Risk^{I}_{A_1}$, $Risk^{I}_{A_2}$, $Risk^{I}_{A_3}$, $Risk^{I}_{A_4}$, $Risk^{I}_{A_5}$, $Risk^{I}_{A_6}$, $Risk^{I}_{A_7}$, $Risk^{I}_{A_8}$, $Risk^{I}_{A_9}$, and $Risk^{I}_{A_{10}}$. Similarly, risk can be calculated for the remaining security dimensions.

$Risk^{I}_{BP_1}$ is dynamically built in accordance with the control-flow and the patterns defined in Table 2. First, the business process begins with a start event S_1, which is followed by a sequence of activities that starts with A_1. The sequential pattern introduced therefore indicates that the risk is the sum of the activities that compose this sequence, divided by the total number of activities. In this case, the sequence is composed of A_1, A_2, a *Parallel* pattern (hereinafter P_1), A_5, A_6, an *Exclusive* pattern (hereafter E_1),

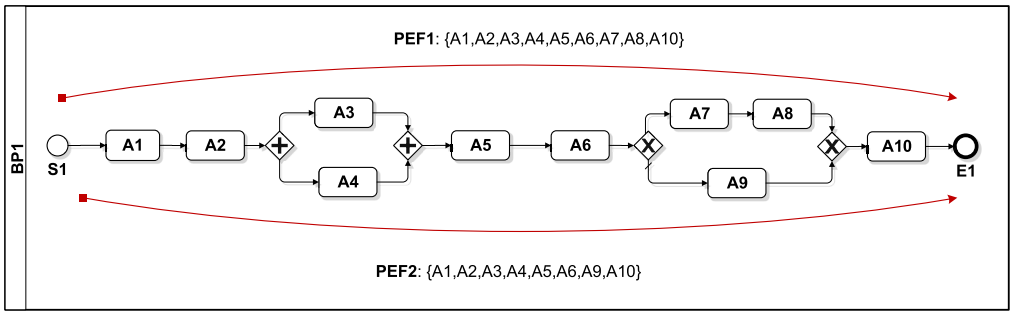
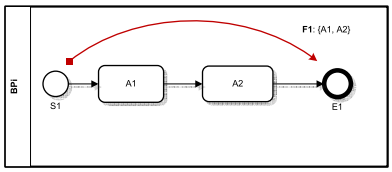
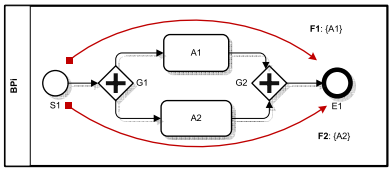
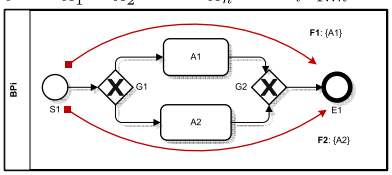
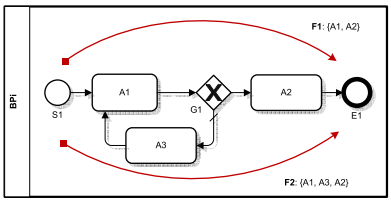


FIGURE 3. Example of a business process model to be assessed.

TABLE 2. Basic patterns for risk determination in business process models.

Pattern	Formula	Business Process
Sequential	$Risk^D_{BP_i} = Risk^D_{F_i} = f_{seq}(R^D_{A_1}, R^D_{A_2}, \cdots, R^D_{A_n})$	 $f_{seq}(R^D_{A_1}, R^D_{A_2}, \cdots, R^D_{A_n}) = \sum_{i=1..n}(Risk^D_{A_i})/n \implies \frac{Risk^D_{A_1}+Risk^D_{A_2}}{2}$
Parallel	$Risk^D_{BP_i} = f_{par}(R^D_{A_1}, R^D_{A_2}, \cdots, R^D_{A_n})$	 $f_{par}(R^D_{A_1}, R^D_{A_2}, \cdots, R^D_{A_n}) = \sum_{i=1..n}(Risk^D_{F_i})/n \implies \frac{Risk^D_{A_1}+Risk^D_{A_2}}{2}$
Exclusive	$Risk^D_{BP_i} = f_{exclusive}(R^D_{A_1}, R^D_{A_2}, \cdots, R^D_{A_n})$	 $f_{exclusive}(R^D_{A_1}, R^D_{A_2}, \cdots, R^D_{A_n}) = MAX(Risk^D_{F_1}, Risk^D_{F_2}) \implies MAX(Risk^D_{A_1}, Risk^D_{A_2})$
Loop	$Risk^D_{BP_i} = f_{loops}(R^D_{A_1}, R^D_{A_2}, \cdots, R^D_{A_n})$	 $f_{loops}(R^D_{A_1}, R^D_{A_2}, \cdots, R^D_{A_n}) = MAX(Risk^D_{F_1}, Risk^D_{F_2}) \implies MAX\left(\frac{Risk^D_{A_1}+Risk^D_{A_2}}{2}, \frac{Risk^D_{A_1}+Risk^D_{A_2}+Risk^D_{A_3}}{2}\right)$

and finally A_{10}. Hence, $Risk^I_{BP_1}$ is given as follows:

$$\begin{aligned} Risk^I_{BP_1} &= f_{seq}(Risk^I_{A_1}, Risk^I_{A_2}, Risk^I_{P_1}, Risk^I_{A_5}, \\ &\quad Risk^I_{A_6}, Risk^I_{E_1}, Risk^I_{A_{10}}) \\ &= (Risk^I_{A_1} + Risk^I_{A_2} + Risk^I_{P_1} + Risk^I_{A_5} + Risk^I_{A_6} \\ &\quad + Risk^I_{E_1} + Risk^I_{A_{10}})/7 \end{aligned} \tag{11}$$

As previously mentioned, the standard ISO/IEC 27005:2018 [12] in Appendix E applies an average to determine the global risk. Therefore, the inclusion of the average by means of the total risk of activities gives rise to an approach of risk as $1 \leq Risk^I_{BP_1} \leq 100$.

The next step is to determine the risk of $Risk^I_{P_1}$ and $Risk^I_{E_1}$. It has been assumed that the business process is well-designed

$$Risk^I_{BP_1} = \frac{Risk^I_{A_1} + Risk^I_{A_2} + \left(\frac{Risk^I_{A_3} + Risk^I_{A_4}}{2}\right) + Risk^I_{A_5} + Risk^I_{A_6} + MAX\left(\frac{Risk^I_{A_7} + Risk^I_{A_8}}{2}, Risk^I_{A_9}\right) + Risk^I_{A_{10}}}{7} \quad (14)$$

without structural faults, and gateways are presumed to be opened and closed correctly. Based on the concept of an average, the risk of a *Parallel pattern* is estimated as the sum of the risk activities of which each branch of the pattern is composed, divided by the total of activities of the parallel pattern. In the example there are two branches: the first branch composed of activity A_3, and the second activity composed of activity A_4. Therefore, $Risk^I_{P_1}$ is estimated by the following formula:

$$Risk^I_{P_1} = f_{par}(Risk^I_{A_3}, Risk^I_{A_4}) = \left(\frac{Risk^I_{A_3} + Risk^I_{A_4}}{2}\right) \quad (12)$$

In contrast, the risk of an *exclusive pattern* is estimated by the maximum risk between the involved branches. The exclusive pattern is based on the idea that only one path is executed. Although all the paths must be considered, we only select the one with the maximum risk value.

In this case, there are two branches: the first composed of activities A_7 and A_8, and the second branch composed of activity A_9. Therefore, $Risk^I_{E_1}$ is determined as follows:

$$\begin{aligned} Risk^I_{E_1} &= f_{excl}(Risk^I_{A_7}, Risk^I_{A_8}, Risk^I_{A_9}) \\ &= MAX\left(\frac{Risk^I_{A_7} + Risk^I_{A_8}}{2}, Risk^I_{A_9}\right) \end{aligned} \quad (13)$$

Finally, by combining the three formulas previously described, f_{seq}, f_{par}, and f_{excl}, the risk $Risk^I_{BP_1}$ becomes as indicated in the listing (14), as shown at the top of this page. These formulas are described to provide a way of estimating the risk of business process models.

B. PEF-BASED RISK ESTIMATION

The estimation of risk of the business process model described in the previous section is necessary for the verification of conformance with regard to the acceptable risk. Nevertheless, PEFs are necessary for the diagnosis of which activities are responsible for the nonconformance (if any).

A business process model is composed of a set of PEFs (cf. Def. 6), where these PEFs define different sequences of execution. Therefore, the risk of each PEF is determined by the risk of the activities that compose it.

We propose to use the addition of the activities risk of each PEF as the risk estimation of each PEF:

$$Risk_{PEF_i} = \sum_{\forall A_i \in PEF_i} Risk^D_{A_i} \quad (15)$$

This risk estimation could be adjusted depending on the necessity of the organization because another approach might be required, such as, the average of risks instead of the average. In our approach, these adjustments can be established at the beginning and before the risk assessment is carried out.

This separation between PEFs is suitable for the diagnosis. In general, the diagnosis enables the identification of the parts that fail, and determines why a correctly designed system fails to work as expected. Adapted to our problem, the diagnosis is utilized to identify which elements in the model are in nonconformance with respect to the acceptable risk level.

One of the most important advantages of the proposal is the use of these elements to diagnose the fault responsible for the nonconformity. To automate both the verification of conformance and the diagnosis, constraint programming (CP) technique is proposed. CP is an artificial intelligence technique widely used to solve diagnosis problems in various fields [29]–[31]. In the following section, the verification and diagnosis using CP are described in detail.

VI. AUTOMATIC VERIFICATION OF CONFORMANCE AND DIAGNOSIS BY USING CONSTRAINT PROGRAMMING

To automate both the verification of conformance and the diagnosis, we propose a two-step subprocess called *Automate Security Risk Assessment* (see Figure 4). More details about the entire process are provided in Section VII, where the tool is described.

First, the *Verify Conformance* activity runs the risk estimation of the business process model and verifies its conformance with regard to the *acceptable risks* that are included as a part of the *CSP*. This verification task is responsible for the calculation of the truth values of the verification (cf. Def. 5). The truth values of *VRC* are obtained by means of a constraint satisfaction problem (CSP) (cf. *CSP* in the figure) created automatically by the transformation of the risk-aware business process model into a *CSP* model. The resolution of the *CSP* obtains those truth values. If any risk formula is nonconforming, the fault diagnosis (cf. Def. 7) is executed (cf. *Diagnose* in the figure) by creating and solving a *Max-CSP* to identify the activities whose risks are directed toward the VRC. Both *CSP* and *Max-CSP* are explained follows.

Constraint programming [32], [33] is based on the algorithmic resolution of CSPs which are defined as follows.

Constraint Satisfaction Problem. A constraint satisfaction problem *(CSP)* consists of the triple *(V,D,C)*, where V is a set of n variables $\{v_1, v_2, \cdots, v_n\}$ whose values are taken from finite, discrete domains $D_{v_1}, D_{v_2}, \cdots, D_{v_n}$ respectively, and C is a set of constraints on their values. The constraint $c_k(x_{k_1}, \cdots, x_{k_n})$ is a predicate that is defined on the Cartesian product $D_{k_1} \times \cdots \times D_{k_n}$. This predicate is true iff the value assignment of these variables satisfies the constraint c_k.

Constraint solvers strives to propagate a value for each variable to satisfy the constraints within CSP, where each constraint is defined over some subset of the original set of variables and limits the combinations of values that the

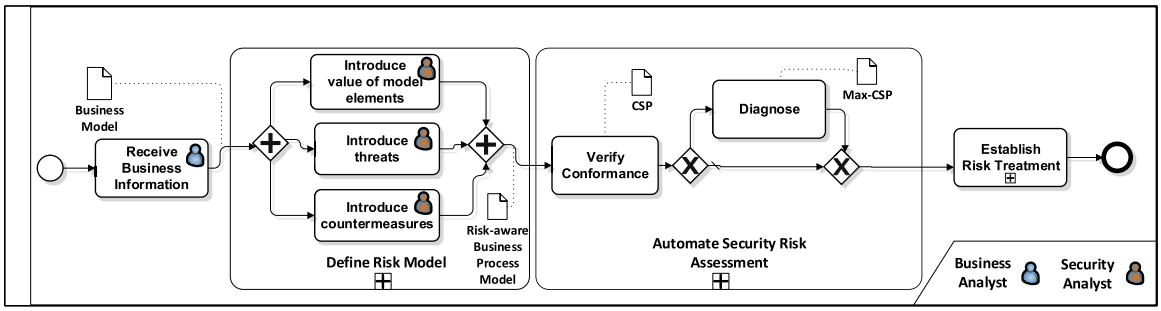


FIGURE 4. Description of the process for verification nonconformance and diagnosis of security-risks.

```
Variables and Domains: {Integrity_A1: [1,3], Integrity_A2: [1,5], Confidentiality_A2: [1,5],
Availability_A2: [1,5], Frequency_TH2: [2,4], Consequence_TH1: [4,5], Frequency_TH2: [1,3],
Consequence_TH2: [4,5], Frequency_TH3: [3,4], Consequence_TH3: [3,5], RiskReduction_T1: 10,
Acceptable risk_BP1: 120, RiskI_A1: [1, 1000], RiskC_A1: [1,1000], RiskA_A1: [1,1000], RiskI_A2:
[1, 1000], RiskC_A2: [1,1000], RiskA_A2: [1,1000],Risk_Process_Integrity: [1,1000],
Risk_Process_Confidentiality: [1,1000], Risk_Process_Availability: [1,1000]}
Constraints: {
% Risk estimation of activities
% Risk Activity A1 - Defined by Integrity dimension
RiskI_A1 = (Integrity_A1) * ((Consequence_TH1 - Consequence_TH1*RiskReduction_T1) * (Frequency_TH1
- Frequency_TH1*RiskReduction_T1) + (Integrity_A1) * (Consequence_TH3 - Consequence_TH3 *
RiskReduction_T1) * (Frequency_TH3 - Frequency_TH3* RiskReduction_T1) + (Consequence_TH2 -
Consequence_TH2*RiskReduction_T2) * (Frequency_R2 - Frequency_R2*RiskReduction_T1);

% Risk Activity A2 - Defined by Integrity, Confidentiality, Availability dimensions
RiskC_A2 = (Confidentiality_A2) * ((Consequence_TH1 - Consequence_TH1 * RiskReduction_T1) *
(Frequency_TH1 - Frequency_TH1 * RiskReduction_T1) + (Confidentiality_A2) * (Consequence_TH3 -
Consequence_TH3 * RiskReduction_T1) * (Frequency_TH3 - Frequency_TH3 * RiskReduction_T1);
. . . % the same for integrity and availability

% Risk estimation based on the control-flow
% Or-Pattern A1-A2 - Maximum of the activities of each branch for each dimension
Risk_Process_Integrity = Maximum (RiskI_A1)
Risk_Process_Confidentiality = Maximum (RiskC_A1, RiskC_A2)
Risk_Process_Availability = Maximum (RiskA_A1, RiskA_A2)

%Conformance
(Acceptable risk_BPi ≥ Risk_Process_Integrity);
(Acceptable risk_BPi ≥ Risk_Process_Confidentiality);
(Acceptable risk_BPi ≥ Risk_Process_Availability);
```

FIGURE 5. Code of the CSP for the verification of conformance.

variables in this subset can take. The goal is to find one assignment to the variables such that the assignment satisfies all the constraints. In certain types of problems, the goal is to find all such assignments [34].

In our approach, a CSP is created combining the formula obtained from the control-flow analysis and the risks deemed acceptable by the company. The parts of the CSP are: (1) the variables and domains of the problem corresponding to the metrics provided by the activities (e.g., integrity, confidentiality, and availability), threats (e.g., frequency and consequence), and countermeasures (e.g., risk reduction); (2) the risk estimation of the activities represented using constraints; (3) constraints obtained from the control-flow pattern-based risk estimation, using the pattern formulas provided in Table 2; and (4) the acceptable risks corresponding to the objectives of the organization. An example of a *CSP* is given in Figure 5. This code might represent a piece of the *CSP* generated for a business process model similar to that shown in Figure 2, where two activities, A_1 and A_2, are in an exclusive pattern. We can assume, for example, that activity A_1 is defined only for the integrity dimension and is affected by threats TH_1 and TH_2 and that activity A_2 is defined for integrity, confidentiality, and availability dimensions and is affected by the same threat as A_1. The acceptable risk level (cf. $Acceptable_{risk_{BP_i}}$) is limited to one hundred twenty.

The variables in the example are defined with an open domain, because, prior to solving the *CSP*, it is impossible to determine their specific values until an attempt is made to satisfy the constraints. Thus, there are three types of constraints:

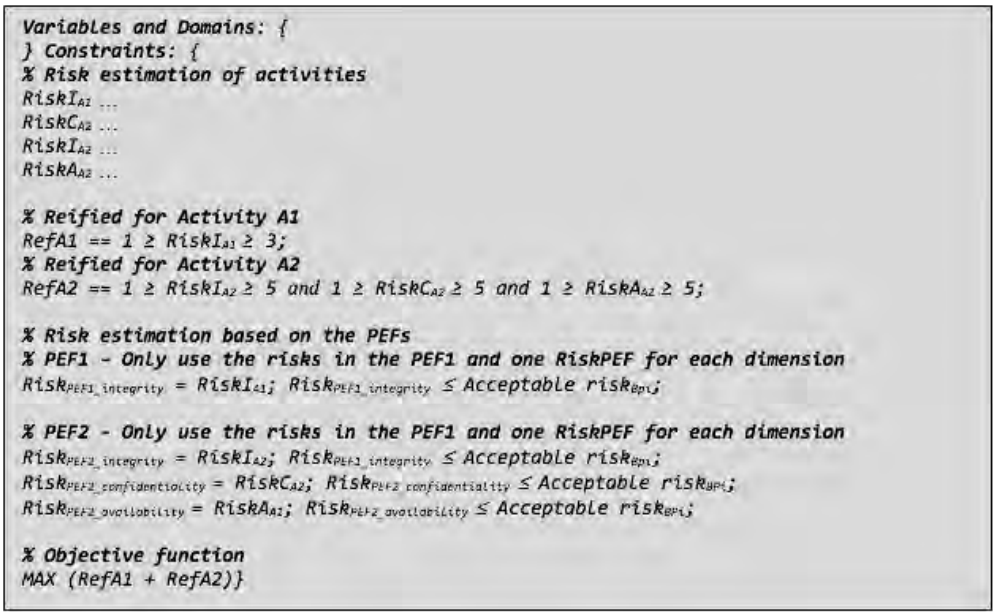


FIGURE 6. **Code of the Max-CSP for the diagnosis.**

1) *Risk estimation of activities*, which defines how the risk determination is calculated based on the risk method previously selected, such as the ones defined in (10).
2) *Risk estimation based on the control-flow*, which represents the combination of risks of activities following the patterns defined in Table 2.
3) *Conformance*, which represents the achievement of the acceptable risks. For example, the risk of the business process for each dimension is less than the acceptable risk level.

This *CSP* is solved to determine if there is a solution (i.e., conformance) or not (i.e. non-conformance). A case of non-conformance, means that the model is not conformant to the acceptable risk. To ascertain which activity is responsible of the nonconformance, a new model is computed to determine the diagnosis. This new model consists of the risk formulas related to all the PEFs of the business process model as a *Max-CSP* to discover the minimum explanation of the malfunction.

Max-CSP. The *maximal constraint satisfaction* problem (*Max-CSP*) is an optimization problem over CSPs with a function f to optimize (minimize or maximize). The goal is to assign values to the variables to optimize the function.

Following the same example, the *Max-CSP* includes the same structure as the previous CSP but includes the PEFs instead of the control-flow pattern-based risk formula (PEF_1 and PEF_2 for the example), and assigns the possible responsibility of the nonconformance to a Boolean variable (Reified Constraints). The possible ranges of the metrics were defined as a part of the variable domain in the previous *CSP*, however, if a nonconformance is found these domains can fail. For this reason, in the *Max-CSP* code in Figure 6, these domains are associated with a Boolean value (reified constraints) that allow these domains to be nonsatisfiable. Due to the exclusive pattern, the business process is composed of two PEFs: (1) PEF_1, which is composed of activity A_1; and (2) PEF_2, which is composed of activity A_2. In any case, the objective function is to maximize the satisfaction of every domain, the constraints $RefA_1$ and $RefA_2$ in this example. These variables take a value of 1 (i.e., true) if the formula is satisfiable, and 0 (i.e., false) otherwise. These reified constraints indicate whether the constraint can be satisfied. That is, $RefA_1$ is evaluated as *true* iff $Risk_{PEF_{1_{integrity}}}$ can achieve a value less than $Acceptable_{risk_{BP_i}}$; otherwise, $RefA_1$ is *false* (cf. Def. 5). When $RefA_1$ cannot be satisfied, a nonconformance in this PEF is indicated by the activity A_1 in this dimension. In this particular case, the diagnosis explains this problem as the impossibility of satisfying the constraint associated with an activity by attaining a set of assignments of values that achieve less than the acceptable risk value. Constraints can be defined similarly for other PEFs and dimensions.

When all PEFs are modeled in the same manner, the objective is to determine an assignment that enables the satisfaction of the maximum number of constraints related to the all activities that composing the PEFs of the model. As shown in Figure 6, the function of *Max-CSP* indicates the necessity to satisfy both $RefA_1$ and $RefA_1$ if possible.

In a manual process, all the activities involved in the PEFs must be reviewed. Nevertheless, diagnosis provides the minimal number of activities (parsimony principle) that must be treated to reduce the risks of the business process model. This problem is too complex to solve manually; therefore, we establish a mapping to an optimization problem by means of constraints (cf. *Max-CSP*).

VII. TOOLING

Figure 4 describes our proposal to ensure a risk-aware business process model development described by using a business process model. To easily support the diagnosis using

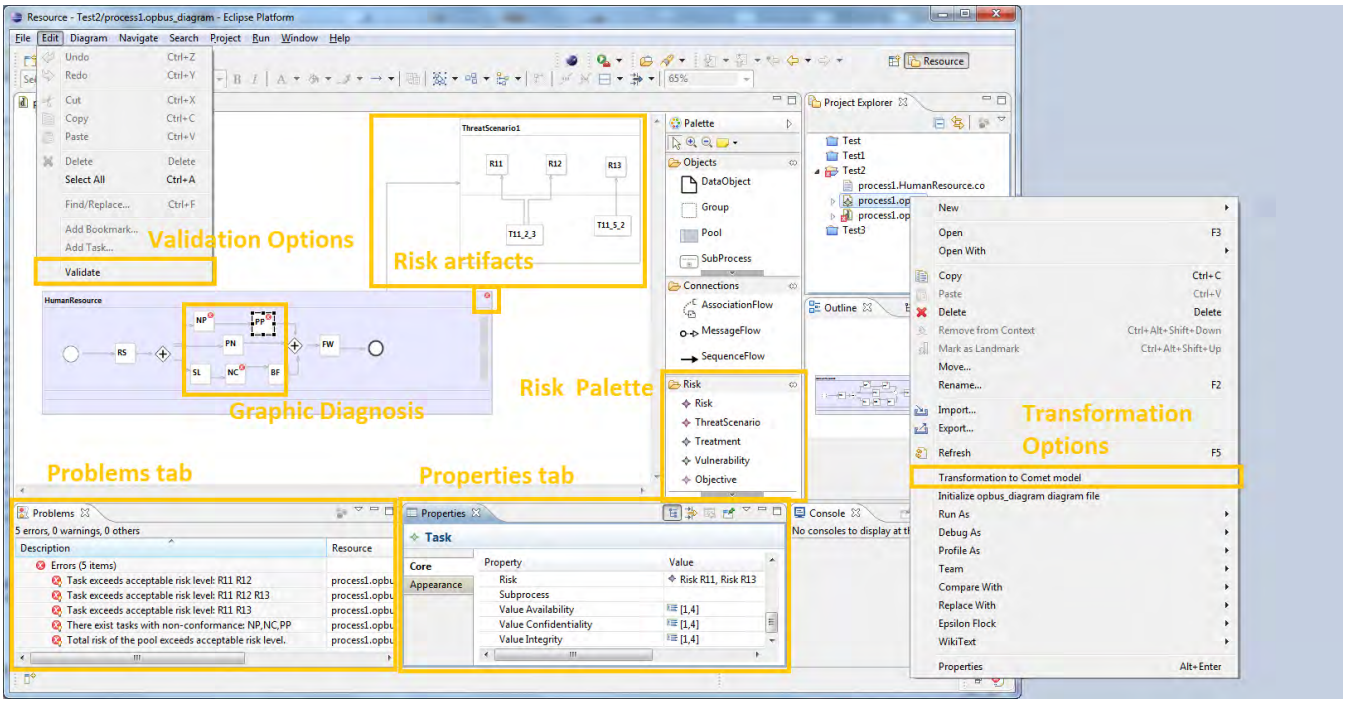


FIGURE 7. OPBUS-Risk integrated development editor.

CSPs, we implement a tool following the steps described using the business process model in Figure 4.

The implemented tool (called OPBUS-Risk) is an extension of OPBUS [35], an Eclipse plug-in based on model-driven architecture technologies that integrates (1) a business process modeler that supports the specification of the extension presented in Section IV; (2) a transformation engine that enables business process models extended with risk information to be translated into CSP and COP models; (3) a mechanism to support various constraint solvers; and (4) the automation of the verification and diagnosis processes through a set of algorithms that create the CSPs and Max-CSP and solve them.

To render our proposal flexible, agile, and general, we define a solver-independent approach through transformations. A model-driven approach is based on a set of transformations (model-to-model) that enables the automatic translation of business process models, extended with a risk model, into platform-specific *Max-CSP* programs for IBM CPLEX [36], ChocoSolver [37], and *COMET*© Solver [38]. This transformation uses a set of auxiliary functions to determine PEFs, reified constraints, risk expressions, and other structures that compose the *CSP* and *Max-CSP* scripts. Whenever any other platforms require support, we must only to provide a transformation to those platforms.

Figure 7 shows the OPBUS-Risk tool workspace. The modeler enables the users to define a business process model and set up the risk information by means of the *Properties* tab (cf. Figure 7). The *Properties* tab is where the users can edit properties of the model, such as the acceptable risk value for a business process within objectives and the value of assets, and can include threats to activities. The modeler is provided with a set of validation scripts that enables the detection of possible structural faults (e.g., live-locks, starvations) and verification of the correctness of time events, conditions, etc. Moreover, the OPBUS-Risk environment is equipped with specific features to obtain a direct transformation of business process models into *COMET*© models, as shown in the contextual menu of Figure 7. The transformation can be configured through property windows of the tool.

Furthermore, the OPBUS-Risk plug-in is equipped with a validation option, as indicated in the *Edit* menu in Figure 7. In this case, the validation option performs the following steps in an automatically: (1) business process models in the current workspace are transformed into *CSP* and *Max-CSP* models; (2) *CSP* and *Max-CSP* models are solved by a specific solver; and (3) results are returned to the graphical model.

In validation, risk estimation is carried out and nonconformance of risks is identified. The results are retrieved over the graphical elements of the business process, whereby those elements that are in nonconformance are highlighted in red. The identification of these elements in the model constitutes the completion of the diagnosis. A video of the key features of the OPBUS-Risk plug-in, including the complete set of resources (plug-in, models, CSPs, etc.) used for this paper can be consulted at http://www.idea.us.es/portfolio-item/opbus-tool/.

In the following section, a case study is presented as an illustrative example. This example describes the complete process of applying our framework to develop a risk-aware

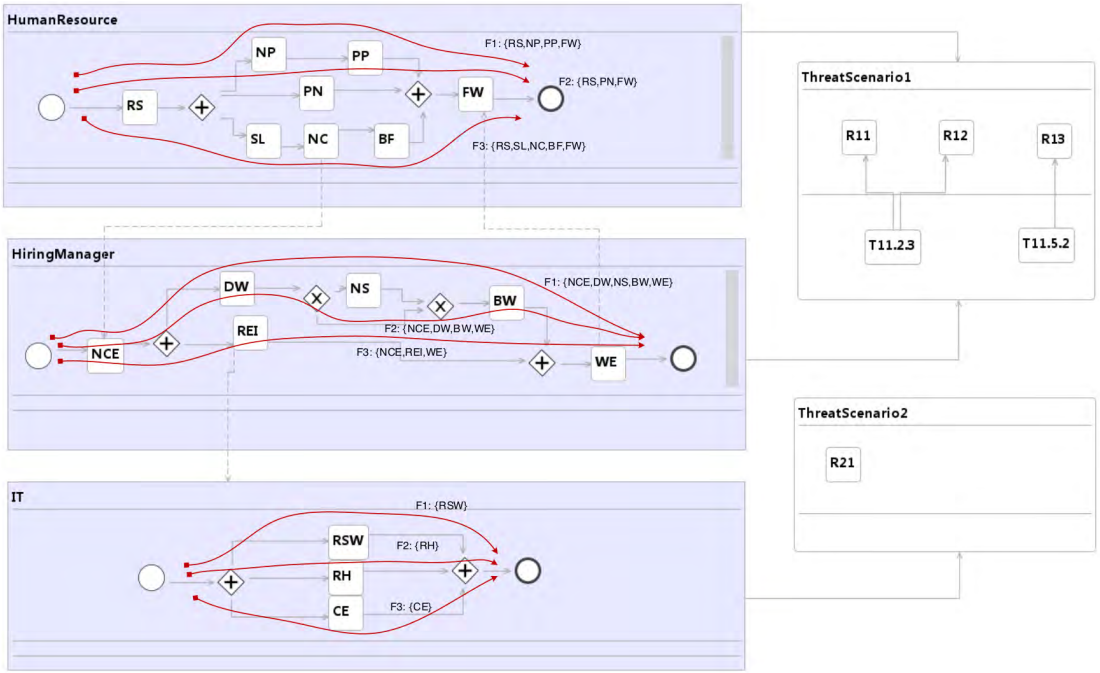


FIGURE 8. **Business process model of the example with PEFs.**

business process model and our tool for the automatic risk assessment.

VIII. APPLYING TO THE MOTIVATING CASE STUDY

The case study described Section II was developed using the OPBUS-Risk modeler as shown in Figure 8. In the figure, the activity labels are abbreviations of the real name of activities whose names are listed in Table 3.

The threats presented in Table 4 must be assessed. To this end, security experts attach threat scenarios to the model, as shown in Figure 8. *Human resources* and *hiring manager* departments have an associated threat scenario (*Threat Scenario 1*) composed of three threats and two countermeasures. *IT*, however, has an associated threat scenario (*Threat Scenario 2*) composed of a single threat, as shown in Figure 2. To simplify the example, the labels of threats and countermeasures are only identifiers. Tables 4 and 3 provide descriptions of countermeasures and threats respectively.

Security analysts include these features to carry out automatic risk assessment and identify of any nonconformance. Because the problem is focused on the diagnosis of the nonconformance to an acceptable risk level of a business process, the acceptable level of risk for each business process must be defined first.

One of the main challenges associated with security is its measurement [39]. Most risk management proposals provide their own metrics. These metrics are defined by qualitative and quantitative approaches. Nevertheless, stakeholders are held responsible for the choice of either the acceptable range of values (in the case of a qualitative approach) or the acceptable qualitative value (with regard to the global qualitative scale). A good practice using a quantitative approach is to define a mapping of the range of values to a qualitative scale, as given in [40]. This mapping provides an overview of values that may be considered of low, medium or high risk.

TABLE 3. **Activity abbreviations for the example.**

Abbreviation	Activity
RS	Received signed contract
NP	Notify payroll
SL	Send welcome letter
PN	Prepare new employee packet
NC	Notify hiring manager of new contract
BF	Begin employee file
PP	Prepare payroll and benefits
FW	Finish workspace setup
RSW	Request software
RH	Request hardware
CE	Configure e-mail account and intranet
NCE	Notify employee of contract
DW	Determine workspace
REI	Request e-mail and intranet access
NS	Negotiate space
BW	Begin workspace setup
WE	Welcome employee

TABLE 4. **Description of countermeasures.**

Abbr.	Name	Description
T11.2.2	Privilege management	Restricts and controls the allocation and use of privileges.
T11.5.2	User identification and authentication	All users should have a unique identifier for their own exclusive use.

TABLE 5. Risk criteria for business processes.

Pool	Objective
Human Resources (HR)	$\{RiskCriterion : 150\} \wedge Risk_{HR} \leq RiskCriterion$
Hiring Manager (HM)	$\{RiskCriterion : 150\} \wedge Risk_{HM} \leq RiskCriterion$
IT	$\{RiskCriterion : 100\} \wedge Risk_{IT} \leq RiskCriterion$

Subsequently, business and security stakeholders must agree on the acceptable risk level and introduce it into the business process. One of the main advantages of our proposal is that stakeholders must adjust the acceptable risk values in the business processes, and then our tool can automatically diagnose whether business processes can achieve or exceed this level.

The main objective is the identification of any nonconformance. Therefore, security experts should indicate these objectives for each business process separately, as shown in Table 5. In the same table, business objectives establish what states of the business process risk cannot exceed the risk criterion.

TABLE 6. List of threats and values associated with the activities of the business process.

Activity	Threats	Asset Value (I)	Asset Value (C)	Asset Value (A)
RS	{R11}	[1-2]	[1-2]	[1-2]
NP	{R11, R12, R13}	[1-3]	[4-5]	[4-5]
SL	{R11}	[1-1]	[1-1]	[1-1]
PN	{R11, R12, R13}	[1-4]	[1-1]	[1-1]
NC	{R11, R12, R13}	[1-3]	[4-5]	[4-5]
BF	{R11, R12, R13}	[1-1]	[1-1]	[1-1]
PP	{R11, R13}	[1-4]	[1-4]	[1-4]
FW	{R13}	[1-4]	[1-4]	[1-4]
NCE	{R11}	[1-1]	[5-5]	[5-5]
DW	{R11, R12}	[1-1]	[2-2]	[2-2]
REI	{R11, R12}	[3-3]	[4-4]	[4-4]
NS	{R11}	[1-1]	[2-2]	[2-2]
BW	{R11, R12}	[1-1]	[2-2]	[2-2]
WE	{R11}	[3-3]	[4-4]	[4-4]
RSW	{R21}	[1-3]	[1-3]	[1-3]
RH	{R21}	[1-3]	[1-3]	[1-3]
CE	{R21}	[1-3]	[3-5]	[3-5]

In a second step, business and security experts have to collaborate to evaluate business process activities. The business process activities are configured by linking threats and evaluation to each activity. The relationships between threats and value are presented in Table 6. The activity values are specified by intervals of values that indicate the minimum and maximum allowed values. Similarly, properties for threats and countermeasures are described in Tables 7 and 8, respectively.

At this point, the security analyst is ready to apply the automatic diagnosis. To this end, the security analyst has to utilize the "Validate" options provided by the OPBUS-Risk tool. This option automatically transforms the business process models into CSP models, and a constraint solver obtains the solutions for these constraint models. As explained in the previous section, the diagnosis addresses the identification of

TABLE 7. Frequencies and consequences related to threats.

Threat	Frequency	Consequence
R11	[1-3]	[2-5]
R12	[3-4]	[4-5]
R13	[1-4]	[1-4]
R21	[2-3]	[2-3]

TABLE 8. Risk reduction values related to countermeasures.

Countermeasure	Risk reduction
T11.2.2	[10-30]
T11.5.2	[20-50]

which potential execution flows in the business process are in nonconformance to the objectives. In Figure 8, the PEFs for the example are highlighted, but these PEFs are only taken into consideration in the definition of the CSP model.

Because, the OPBUS-Risk tool supports the transformation into *COMET*© CSP models, a CSP model is generated for each business process. As explained in the previous sections, a Max-CSP model is also generated for each business process.

TABLE 9. Nonconformance by activity.

Activity	Risk value	Non-conformance	PEF
RS	45	C	{F1,F2, F3}
NP	243	NC	{F2}
SL	84	C	{F3}
NC	473	NC	{F3}
BF	129	C	{F3}
PP	248	NC	{F1}
PN	129	C	{F2}
FW	160	NC	{F1,F2, F3}
NCE	150	C	{F3}
REI	132	C	{F3}
RSW	132	C	{F1}
WE	165	NC	{F3}
RH	27	C	{F2}
CE	108	NC	{F3}

Table 9 presents the risk value obtained in the solution of CSPs for all the activities belonging to certain PEFs previously identified. Similarly, nonconformance of these activities is indicated with regard to the acceptable risk of the business process.

These results are obtained automatically in background mode. The nonconformances are reflected in the graphical model, as shown in Figure 9. Activities highlighted in red are nonconform.

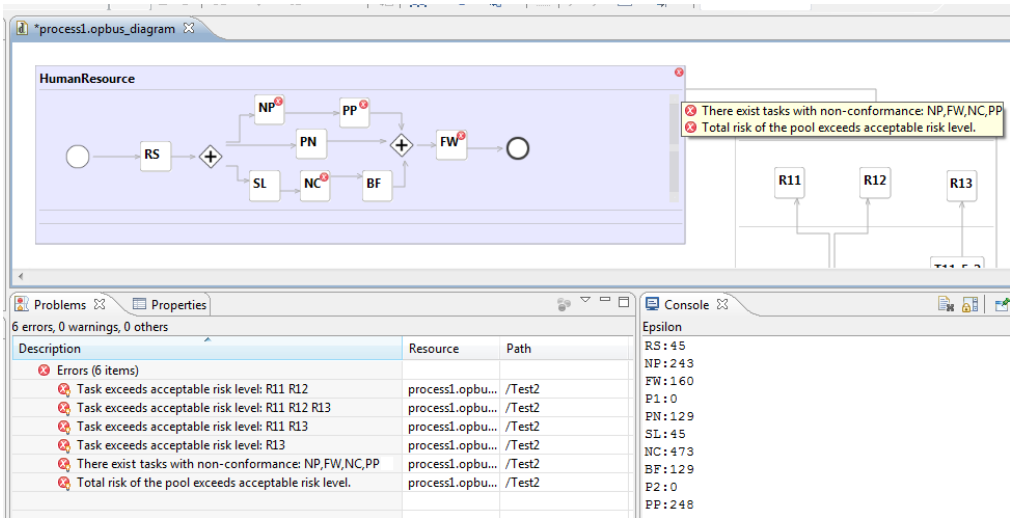


FIGURE 9. **Results of the diagnosis of nonconformance in the business process model.**

IX. IMPLEMENTATION PERFORMANCE AND DISCUSSION OF RESULTS

The benchmarks consist in performing the verification of nonconformance and diagnosis using three different constraint programming engines: IBM CPLEX, *COMET*©, and ChocoSolver 2.0 for various examples of business processes. The examples have been categorized with regard to the size, understanding size as the addition of activities, threats, and treatments within the business process model: (1) tiny business processes with no more than 10 elements; (2) medium-large business processes with more than 10 and fewer than 20 elements; and (3) large business processes with more than 20 elements. We have used the examples in Table 2 (sequential, parallel, exclusive, and loop) for the first category. Business processes of the case study (human resource, hiring manager, and IT) have been used for the second category. Regarding the third category, two synthetic examples have been employed. The first synthetic example (Sy1) is composed of 18 activities, 10 gateways, 3 threats, and 2 treatments. The second synthetic example (Sy2) is composed of 18 activities, 10 gateways, 10 threats, and 5 treatments.

Three features have been measured to analyze the scalability and performance: (1) number of variables and constraints required to create the CSP models; (2) memory consumption required by the engine to find a solution; and (3) time in milliseconds required by the engine to find a solution. The hardware used in the execution of the benchmarks is an Intel Core i7 2675-Q 2.20 GHz, with 8GB RAM (DDR3) and a Windows (64-bits) operating system.

Regarding variables and constraints, it is important to note that each constraint programming engine has a particular syntax and semantics with which to define constraint satisfaction programs. The number of variables and constraints varies depending on the problem, because, for each activity, threat, and treatment, at least one variable in the *CPS* must be created. The results are similar among the three constraint programming engines. Nevertheless, specific variables need to be computed with regard to various other variables and certain engines; for example, ChocoSolver and IBM CPLEX use expressions to represent this type of variable. That is, the terms are considered variables by the *CSP*. This is the reason why ChocoSolver and IBM CPLEX show the same trend in all examples. Nevertheless, *COMET*© uses constraints to represent this type of variable. Hence, *COMET*© shows a peak in the majority of examples, such as shown in Figure 10a.

Figure 10b shows the results obtained with regard to memory consumption. The results illustrate how the memory consumption levels off and remains unchanged in terms of the size of the problem for every constraint engine. Native implementation of the engine has been used. Nevertheless, we must note that memory consumption is a particular feature of each constraint programming engine. *COMET*© uses an engine implemented in C++ although it provides libraries for using the engine in JAVA. In contrast, ChocoSolver and IBM CPLEX use an engine implemented in JAVA, although it provides connectors to be used in C, C++, JAVA, FORTRAN, and others languages.

Regarding the performance, it should be noted that a logarithmic scale has been used to represent the results for a better comparison as shown in Figure 10c. In general, the performance results are feasible for the automation of our proposal with regard to all engines less than one second in the worst cases. The results fluctuate depending on the problem and the execution engine as shown in Figure 10c. IBM Cplex levels off in all cases although the size of the problem is increased as shown for *Sy1* and *Sy2*. Nevertheless, IBM Cplex yields better results than Choco and COMET do in the worst cases. ChocoSolver and *COMET*© yield similar results in the small and large cases, although in the medium cases, *COMET*© is

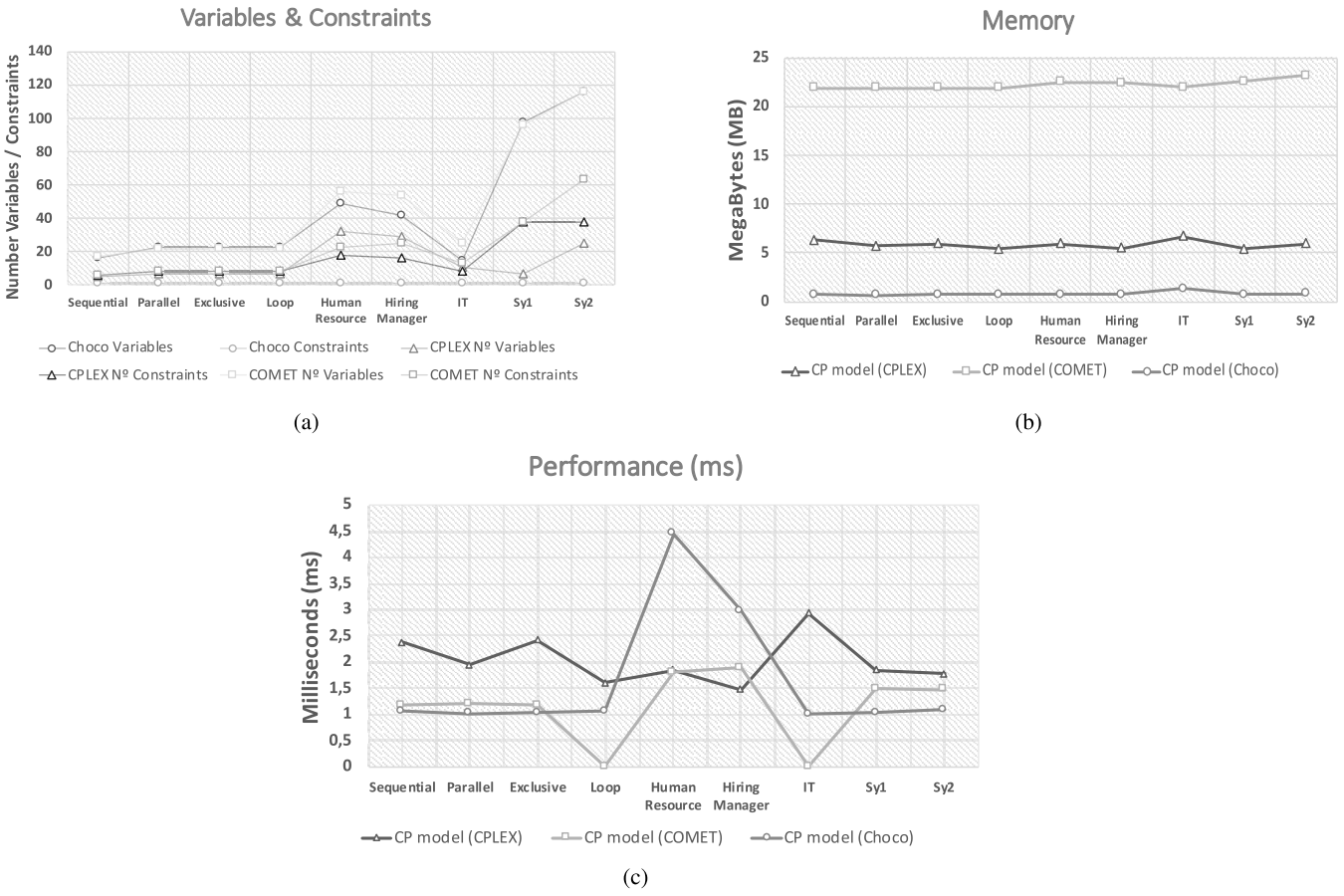


FIGURE 10. **Results of the benchmarks. (a) Number of variables and constraints. (b) Memory consumption. (c) Performance.**

better than ChocoSolver. ChocoSolver show improvements in the medium cases; however, Choco's results level off as the proble size increases.

X. RELATED WORK

Business process management (BPM) and risk description are typically considered disjoint concerns as stated in [41]. This study is one of the few approaches in academia that provides risk-aware business process management. Nevertheless, Suriadi *et al.* [41] indicate the following as the main gaps to address BPM and risk management (1) the degree of formalization of various manifestations of risk within a process model is minimal because most approaches formalize their risk-related constructs only at the syntactic level (without execution semantics), thus limiting an automation; (2) there is a lack of research to support risk-aware business process design; and (3) the adoption of existing risk management techniques and standards into BPM systems should be strengthened.

Another initiative in the context of BPM that bridges the gap between security and business domains is [42]. Ahmed and Matulevičius [42] propose a set of security patterns based on BPMN to ensure a secure-aware development of a business process model, but the authors lack mechanisms for measuring risks and diagnosing the risk responsible for a nonconformity. Their proposition can be considered a set of controls to treat possible security risks from a catalog of possibilities.

There exists a set of proposals focused on providing enhancements in business process languages through new domain specific languages (DSLs) for the incorporation of assets, requirements, goals, and threats into business process models. Certain relevant studies provide approaches for the integration of risks into the business process. Cope *et al.* [43] propose new notation for business process modeling notation (BPMN) to aid documentation in the risk assessment of business processes. The two major limitations of this approach are as follows: (1) the proposal extension is very complex because it presents three separate models related to the same problem; and (2) the extension is only valid for BPMN models. zur Muehlen and Ho [44] propose taxonomy to enable the integration of risk into business processes focusing on EPC-based process models. The taxonomy is applied with the aim of enabling the analysis and documentation of business processes. Lambert *et al.* [45] propose an extension of the integrated definition for function (IDEF) modeling that

supports the description of sources of programmatic risk in business processes. Churilov *et al.* [46] present a framework for the evaluation of risks in business process management based on value-focused process engineering. Rodríguez *et al.* [47] propose an extension to UML 2.0 activity diagrams such that graphical annotations can be provided for the specification of security requirements in the diagrams. This extension is defined by means of a UML profile called BPSec. Their approach is very similar to that presented in [48], although Wolter *et al*. provide a set of security annotations to specify requirements in BPMN models. Xue *et al.* [49] propose an extension of BPMN models with risk management properties. These authors use the control flow of business processes to determine the risk in terms of economic consequences of a data error. Fenz *et al.* [50] define an approach for the automatic determination of the importance of resources that takes into consideration the control flow of business processes. The authors use a transformation of BPMN models to Petri nets and define a formalization to determine the importance of resources used in business processes. Our approach considers a set of patterns influenced by ISO standards that enable the determination of the risk based on the control-flow perspective. However, our approach is more adaptable and flexible because no risk formula for activities is fixed in the formulation. Any other risk formula can be configured as explain in the tool section. However, the adjustment of the patterns to another formulation involve a minimal effort because the use of a model-to-model transformations requires only a change in the transformation.

Many more general approaches exist. Governance, risk management, and compliance (hereinafter GRC) [51] has emerged in the organization arena as a frame of reference for integrating these three areas. GRC aims to align and integrate governance, enterprise risk management and compliance concerns to avoid and overlap gaps between them. Racz *et al.* [52] present a survey that shows the lack, in the literature, of approaches pertaining to integrated GRC. The authors highlight a lack of consensus regarding the concept of GRC, and underline a fuzzy separation between GRC and enterprise risk management (ERM) in the organizations. The authors propose a frame of reference for integrated GRC. There exists a need for integrated GRC with business process and management, as stated in [53], in which a survey of state-of-the-art GRC software is provided. Jürjens [54] presents a UML extension called UMLsec. This extension provides certain UML profiles to aid the security-aware development of systems based on UML. Nevertheless, UMLsec is only defined for UML-based developments because it is not a business-oriented approach. Jakoubi and Tjoa [55] propose a notation-independent model as a reference model. Likewise, Sackman [56] extends current risk management methods by bridging the gap between the business process view and the more technical view of IT risks. These approaches propose theoretical reference models to fill the void between business and risk domains. In other respects, Neubauer *et al.* [57] propose a framework for the analysis of the security of business processes from the point of view of cost-benefit. Their framework proposal is defined for integration into any business process management approach. Neubauer and Heurix [58] and Neubauer *et al.* [59] provide other contributions focused on the determination of security controls. Neubauer and Heurix [58] propose an approach for the risk analysis and the selection of adequate security controls for business processes. However, only an overview of the approach is provided because no details on how to calculate business process risk or on the selection of security controls are given. Neubauer *et al.* [59] focus on the selection of ISO/IEC 27001 controls countermeasures based on multiple objectives (such as cost and benefit). The CORAS method [10] conducts context-independent security risk analysis, which is abbreviated to ‘‘security analysis’’, and provides a domain-specific language inspired by UML for threat and risk modeling. The CORAS language includes various types of diagrams using varied notation, thereby providing a computerized tool designed to support the documentation, maintenance and reporting of analysis results through risk modeling. Sienou *et al.* [60] focus on presenting a framework that unifies risk management and business process management. Their approach is limited to the presentation of various stages of the framework and how it operates from a theoretical point of view. Other approaches that consider processes but also data perspectives are presented in [61]. The authors provide a DSL that extends data flow diagrams (DFD) with risk descriptions to easily assess the risks of the data from a personal data protection point of view.

The main drawback in all these studies lies in the manual nature of their approaches. These approaches are focused on extending models to enrich their expressibility such that the documentation of risk assessment in business processes can be supported and improved. However, there is a serious lack of tools and mechanisms for the automation of the process of risk assessment in business processes. Other approaches strive towards the automation of the generation of security countermeasures and/or controls in business process models. Menzel *et al.* [62] propose an approach to automate the generation of security controls for business processes in accordance with specific risk thresholds. The authors provide a risk scale aligned to a set of security controls that can be applied in different parts of the model. Nevertheless, the authors make no previous assessment of the model and hence fail to properly identify which risks exist in the model. Related to this work, Wolter *et al.* [48] provide security annotations for graphical business processes that enable security configurations to be directly set up in the business process model. However, the approach pays no attention to risk or to the previous risk assessment of the model because these authors focus only on presenting the mechanisms to set up and generate specific security configurations in the model. Other approaches, such as that described [63], try to determine the level of risk based on a business process state. Feng *et al.* [63] apply fuzzy mechanisms to study the level of risk of a business process state.

TABLE 10. Comparison of approaches.

Name	Modeling	Security Dimensions	Objectives	Threats Vuln.	Counterm.	Automatic Analysis	Risk Estimation	Control Flow
[42]	BPMN	✓	∼	✓	✓	×	×	×
[46]	EPC	×	✓	×	×	×	×	×
[43]	BPMN	×	×	✓	✓	×	×	×
[63]	Undefined	×	×	×	×	∼	∼	×
[50]	Petri-Nets	×	×	×	×	×	∼	
[55]	*	✓	∼	✓	∼	×	×	×
[54]	UML	∼	✓	✓	✓	×	×	×
[45]	IDEF	×	×	×	×	×	✓	✓
[62]	BPMN	✓	✓	×	✓	×	×	×
[57]	*		∼	∼	✓	×	×	×
[58]	*	×	×	×	×	×	∼	×
[47]	UML	✓	✓	×	×	×	×	×
[64]	EPC	×	×	∼	∼	×	✓	✓
[56]	*	✓	∼	∼	∼	×	×	×
[48]	BPMN	✓	∼	×	∼	×	×	×
[49]	BPMN	×	✓	×	✓	∼	✓	✓

To provide a clear picture of all aforementioned research, a comparative study of the most relevant approaches related to the topic of this paper is given. The comparative study follows the survey presented in [22], as shown in Table 10. The symbol ✓is used to indicate that the approach supports this category, the symbol ∼ is used to indicate that the approach partially supports this category, and the symbol * is used as a wildcard to indicate that the approach supports all possible values in this category. This comparison is carried out according to the following categories. (1) Modeling: indicates which modeling languages are supported. (2) Security dimensions: indicates whether the evaluation of assets is carried out with regard to different security dimensions. (3) Objectives: indicates whether the approach supports the specification of requirements. (4) Threats and vulnerabilities: indicates whether the approach supports the specification of threats and vulnerabilities. (5) Countermeasures: indicates whether the approach supports the specification of Countermeasures. (6) Automatic analysis: indicates whether the approach supports the automatic assessment of models to detect nonconformances. It should be noted that the majority of approaches support several characteristics. Furthermore, no approach supports or fosters a process for the analysis of the conformance of the requirements specified with regard to risk or security issues as identified in the proposed model. (7) Risk estimation: indicates whether the approach supports the determination of the risk value of business processes or specific elements within the model. (8) Control flow: indicates whether the approach takes into consideration the control flow for the risk estimation.

XI. CONCLUSIONS AND FUTURE RESEARCH WORK

In this paper, the problem of automatic security risk management in the current BPMS is addresses. First, a formalization of the risk elements according to process models is included. These elements are supported as a BPMN 2.0 extension of risk information that is analyzed to determine nonconformance regarding risk goals. In addition, a diagnosis of the risk associated with the activity responsible for the nonconformance is also carried out. To this end, the proposal applies mechanisms based on the model-based diagnosis in which activities are in nonconformance with regard to the acceptable level of risk. The automation of diagnosis is carried out using artificial intelligence techniques based on constraint programming. The proposal is supported by the implementation of a plug-in that enables the graphical specification of the extension and the automation of the verification and diagnosis process. To the best of our knowledge, this is the first published work that addresses the risk-aware design of business processes with automatic techniques.

Our approach has been used to support the ISO/IEC 27001 certification process of the security in the business processes of R+D projects developed by a foundation [65]. The OPBUS-Risk tool has played a crucial role in the risk assessment of potential security-risk nonconformance in business processes, and the foundation has been successfully certified for more than three years in ISO/IEC 27001.

The present work can be extended in several ways. We propose to study the inclusion of new metrics to provide wider assessments with regard to other objectives (e.g., data quality). Moreover, a risk treatment stage can be included in cases in which security controls are selected to act against nonconformances diagnosed in risk assessment. The framework could be extended with specific algorithms to automatically select the best countermeasures to act against specific threats. These countermeasures should be transformed into specific real configurations. Likewise, M2T transformation can be equipped to generate tailored code, configurations and/or procedures for a specific platform where business processes can be performed, such as in transformations to a specific BPM engine.

DISCLOSURE

All the authors are responsible for the concept of the paper, the results presented and the writing. All the authors have approved the final content of the manuscript. No potential conflict of interest was reported by the authors.

ACKNOWLEDGMENT

The authors would like to thank the Foundation for Investigation and Development of Information Technologies (FIDETIA) for their support and the application of our approach.

REFERENCES

[1] M. Weske, *Business Process Management: Concepts, Languages, Architectures*. Berlin, Germany: Springer-Vergla, 2007.

[2] S. Sakr, Z. Maamar, A. Awad, B. Benatallah, and W. M. P. van der Aalst, "Business process analytics and big data systems: A roadmap to bridge the gap," *IEEE Access*, vol. 6, pp. 77308–77320, 2018.

[3] J. M. Pérez-Álvarez, A. Maté, M. T. Gómez-López, and J. Trujillo, "Tactical business-process-decision support based on KPIs monitoring and validation," *Comput. Ind.*, vol. 102, pp. 23–39, Nov. 2018.

[4] D. Fernández-Cerero, A. Jakóbik, D. Grzonka, J. Kołodziej, and A. Fernández-Montes, "Security supportive energy-aware scheduling and energy policies for cloud environments," *J. Parallel Distrib. Comput.*, vol. 119, pp. 191–202, Sep. 2018.

[5] T. Micro, "Business process compromise (BPC)," Trend Micro, Vienna, Austria, Tech. Rep., 2017.

[6] D. R. Klahr *et al.*, "Cyber security breaches survey," Inst. Criminal Justice Stud., Univ. Bortsmouth Ipsos MORI Social Res. Inst., Bortsmouth, U.K., Tech. Rep. 16-046473-01, 2017.

[7] S. Goverment, "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información," Ministerio Hacienda Admin. Públicas, Gobierno España, Madrid, Spain, Tech. Rep. 630-12-171-8, 2006.

[8] *CCTA Risk Analysis and Management Method*, Central Comput. Telecommun. Agency (CCTA), London, U.K., 2002.

[9] COSO. (2004). *Enterprise Risk Management—Integrated Framework*. [Online]. Available: https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf and https://www.coso.org/

[10] M. S. Lund, B. Solhaug, and K. Stølen, *Model-Driven Risk Analysis: The CORAS Approach*. Springer, 2011.

[11] R. Levine, "Risk management systems: Understanding the need," *Inf. Syst. Manage.*, vol. 21, no. 2, pp. 31–37, 2004.

[12] *Information Technology—Security Techniques—Information Security Risk Management*, Standard ISO/IEC 27005:2018, 2018. [Online]. Available: https://www.iso.org/standard/75281.html

[13] *Risk Analysis Methodology and Management for Information Systems*, AENOR UNE, Madrid, Spain, 2008. [Online]. Available: https://www.aenor.es

[14] B. Soft, "Bonita Open Solution," BonitaSoft, Grenoble, France, Tech Rep., 2017.

[15] *Business Process Model and Notation*, OMG, Needham, MA, USA, 2017.

[16] K. Salimifard and M. Wright, "Petri net-based modelling of workflow systems: An overview," *Eur. J. Oper. Res.*, vol. 134, no. 3, pp. 664–676, 2001.

[17] W. M. P. van der Aalst, "Formalization and verification of event-driven process chains," *Inf. Softw. Technol.*, vol. 41, no. 10, pp. 639–650, 1999.

[18] M. Dumas and A. H. M. T. Hofstede, "UML activity diagrams as a workflow specification language," in *Proc. 4th Int. Conf. Unified Modeling Lang. (UML)*, London, U.K., Berlin, Germany: Springer-Verlag, 2001, pp. 76–90.

[19] D. Borrego, R. Eshuis, M. T. Gómez-López, and R. M. Gasca, "Diagnosing correctness of semantic workflow models," *Data Knowl. Eng.*, vol. 87, pp. 167–184, Sep. 2013.

[20] J. de Kleer, A. K. Mackworth, and R. Reiter, "Characterizing diagnoses and systems," *Artif. Intell.*, vol. 56, nos. 2–3, pp. 197–222, 1992.

[21] M.-O. Cordier, P. Dague, F. Levy, J. Montmain, M. Staroswiecki, and L. Trave-Massuyes, "Conflicts versus analytical redundancy relations: A comparative analysis of the model based diagnosis approach from the artificial intelligence and automatic control perspectives," *IEEE Trans. Syst., Man, Cybern. B. Cybern.*, vol. 34, no. 5, pp. 2163–2177, Oct. 2004.

[22] A. J. Varela-Vaca, R. M. Gasca, and A. Jimenez-Ramirez, "A model-driven engineering approach with diagnosis of non-conformance of security objectives in business process models," in *Proc. 5th Int. Conf. Res. Challenges Inf. Sci.*, May 2011, pp. 1–6.

[23] A. J. Varela-Vaca, R. M. Gasca, and S. Pozo, "Opbus: Risk-aware framework for the conformance of security-quality requirements in business processes," in *Proc. SECRYPT*, 2011, pp. 370–374.

[24] *UML Profile for Modeling Quality of Service and Fault Tolerance Characteristics and Mechanisms*, Object Management Group (OMG), Needham, MA, USA, 2009.

[25] *Business Motivation Model (BMM) 1.1*, OMG, Needham, MA, USA, 2007.

[26] Y. Papadopoulos, J. McDermid, R. Sasse, and G. Heiner, "Analysis and synthesis of the behaviour of complex programmable electronic systems in conditions of failure," *Rel. Eng. Syst. Safety*, vol. 71, no. 3, pp. 229–247, 2001.

[27] S.-M. Huang, Y.-T. Chu, S.-H. Li, and D. C. Yen, "Enhancing conflict detecting mechanism for Web services composition: A business process flow model transformation approach," *Inf. Softw. Technol.*, vol. 50, no. 11, pp. 1069–1087, 2008.

[28] H. Zo, D. L. Nazareth, and H. K. Jain, "Security and performance in service-oriented applications: Trading off competing objectives," *Decis. Support Syst.*, vol. 50, pp. 336–346, Dec. 2010.

[29] R. Ceballos, M. T. Gómez-López, R. M. Gasca, and C. D. Valle, "A compiled model for faults diagnosis based on different techniques," *AI Commun.*, vol. 20, no. 1, pp. 7–16, 2007.

[30] R. Ceballos, R. M. Gasca, C. Del Valle, and D. Borrego, "Diagnosing errors in DbC programs using constraint programming," in *Current Topics in Artificial Intelligence* (Lecture Notes in Computer Science), vol. 4177, R. Marín, E. Onaindía, A. Bugarín, and J. Santos, Eds., Berlin, Germany: Springer, 2006, pp. 200–210.

[31] D. Borrego, "Diagnostic reasoning with structural analysis and constraint programming for quality improvement of business process management systems," Ph.D. thesis, Dept. Lang. Comput. Syst., Univ. Seville, Seville, Spain, 2012.

[32] P. van Hentenryck, V. Lifschitz, and B. Porter, "Constraint programming," in *Proc. 5th Int. Conf. Evol. Multi-Criterion Optim. (EMO)*, Berlin, Germany: Springer-Verlag, 2009, p. 3.

[33] F. Rossi, P. Van Beek, and T. Walsh, Eds., *Handbook Constraint Programming*. New York, NY, USA: Elsevier, 2006.

[34] V. Kumar, "Algorithms for constraint-satisfaction problems: A survey," *AI Mag.*, vol. 13, no. 1, pp. 32–44, 1992.

[35] A. J. Varela-Vaca, "OPBUS tools," Univ. Sevilla, Seville, Spain, Tech. Rep., 2018.

[36] *IBM ILog CPlex Optimizer*. (2017). [Online]. Available: http://www-01.ibm.com/software/integration/optimization/cplex-optimizer/

[37] C. Prud'homme, J.-G. Fages, and X. Lorca, *Choco Documentation*, document TASC-LS2N CNRS UMR 6241, COSLING S.A.S., 2017.

[38] Dynadec Decision Technologies. (2012). *COMET*. [Online]. Available: http://dynadec.com/

[39] R. Barabanov, S. Kowalski, and L. Yngström, "Information security metrics: State of the art: State of the art," Stockholm Univ., Stockholm, Sweden, Tech. Rep. DSV Report series No 11-007, 2011.

[40] C. Fang and F. Marle, "A simulation-based risk network model for decision support in project risk management," *Decis. Support Syst.*, vol. 52, no. 3, pp. 635–644, 2012.

[41] S. Suriadi *et al.*, "Current research in risk-aware business process management: Overview, comparison, and gap analysis," *Commun. Assoc. Inf. Syst.*, vol. 34, no. 1, pp. 933–984, 2014.

[42] N. Ahmed and R. Matulevičius, "Securing business processes using security risk-oriented patterns," *Comput. Standards Interfaces*, vol. 36, no. 4, pp. 723–733, 2014.

[43] E. W. Cope, J. M. Kuster, D. Etzweiler, L. A. Deleris, and B. Ray, "Incorporating risk into business process models," *IBM J. Res. Develop.*, vol. 54, no. 3, pp. 1–13, 2010.

[44] M. Z. Muehlen and D. T.-Y. Ho, "Risk management in the BPM lifecycle," in *Proc. Business Process Manage. Workshops*, 2005, pp. 454–466.

[45] J. H. Lambert, R. K. Jennings, and N. N. Joshi, "Integration of risk identification with business process models," *Syst. Eng.*, vol. 9, no. 3, pp. 187–198, 2006.

[46] L. Churilov, D. Neiger, M. Rosemann, and M. Z. Muehlen, "Integrating risks in business process models with value focused process engineering," in *Proc. 14th Eur. Conf. Inf. Syst.*, 2006, pp. 1–11.

[47] A. Rodríguez, E. Fernández-Medina, and M. Piattini, "Towards a UML 2.0 extension for the modeling of security requirements in business processes," in *Trust and Privacy in Digital Business* (Lecture Notes in Computer Science), vol. 4083. Berlin, Germany: Springer, 2006, pp. 51–61.

[48] C. Wolter, M. Menzel, A. Schaad, P. Miseldine, and C. Meinel, "Model-driven business process security requirement specification," *J. Syst. Archit.*, vol. 55, no. 4, pp. 211–223, 2009.

[49] X. Bai, R. Krishnan, R. Padman, and H. J. Wang, "On risk management with information flows in business processes," *Inf. Syst. Res.*, vol. 24, no. 3, pp. 731–749, 2012.
[50] S. Fenz, A. Ekelhart, and T. Neubauer, "Business process-based resource importance determination," in *Proc. 7th Int. Conf. Bus. Process Manage. (BPM)*, Berlin, Germany: Springer-Verlag, 2009, pp. 113–127.
[51] *Integrity-Driven Performance. A New Strategy for Success Through Integrated Governance, Risk and Compliance Management*, Pricewaterhouse-Coopers, London, U.K., 2004.
[52] N. Racz, E. Weippl, and A. Seufert, "A frame of reference for research of integrated governance, risk and compliance (GRC)," in *Communications and Multimedia Security* (Lecture Notes in Computer Science), vol. 6109, B. De Decker and I. Schaumüller-Bichl, Eds. Berlin, Germany: Springer, 2010, pp. 106–117.
[53] N. Racz, E. Weippl, and A. Seufert, "Governance, risk & compliance (GRC) software - An exploratory study of software vendor and market research perspectives," in *Proc. 44th Hawaii Int. Conf. Syst. Sci.*, Jan. 2011, pp. 1–10.
[54] J. Jürjens, "UMLsec: Extending UML for secure systems development," in *The Unified Modeling Language*, J.-M. Jézéquel, H. Hussmann, and S. Cook, Eds. Berlin, Germany: Springer, 2002, pp. 412–425.
[55] S. Jakoubi and S. Tjoa, "A reference model for risk-aware business process management," in *Proc. 4th Int. Conf. Risks Secur. Internet Syst.*, 2009, pp. 82–89.
[56] S. Sackmann, "A reference model for process-oriented it risk management," in *Proc. ECIS*, vol. 246, pp. 1–13, 2008.
[57] T. Neubauer, M. Klemen, and S. Biffl, "Business process-based valuation of it-security," *ACM SIGSOFT Softw. Eng. Notes*, vol. 30, no. 4, pp. 1–5, 2005.
[58] T. Neubauer and J. Heurix, "Defining secure business processes with respect to multiple objectives," in *Proc. 3rd Int. Conf. Availability, Rel. Secur. (ARES)*, Washington, DC, USA: IEEE Computer Society, 2008, pp. 187–194.
[59] T. Neubauer, A. Ekelhart, and S. Fenz, "Interactive selection of ISO 27001 controls under multiple objectives," in *Proc. SEC*, 2008, pp. 477–492.
[60] A. Sienou, E. Lamine, A. Karduck, and H. Pingaud, "Conceptual model of risk: Towards a risk modelling language," in *Proc. Web Inf. Syst. Eng.-WISE Workshops* (Lecture Notes in Computer Science), vol. 4832, M. Weske, M.-S. Hacid, and C. Godart, Eds. Berlin, Germany: Springer, 2007, pp. 118–129.
[61] S.-C. Cha and K.-H. Yeh, "A data-driven security risk assessment scheme for personal data protection," *IEEE Access*, vol. 6, pp. 50510–50517, 2018.
[62] M. Menzel, I. Thomas, and C. Meinel, "Security requirements specification in service-oriented business process management," in *Proc. Int. Conf. Availability, Rel. Secur. (ARES)*, Washington, DC, USA: IEEE Computer Society, 2009, pp. 41–48.
[63] N. Feng, X. Yu, R. Dou, and B. Pan, "Managing risk for business processes: A fuzzy based multi-agent system," *J. Intell. Fuzzy Syst.*, vol. 29, no. 6, pp. 2717–2726, 2015.
[64] M. Rosemann and M. Z. Muehlen, "Integrating risks in business process models," in *16th Australasian Conference on Information Systems (ACIS)*, 2005, pp. 1–11, Paper 50.
[65] *Foundation for Investigation and Development of Information Technologies (FIDETIA)*, Standard ISO/IEC 27001, AENOR, 2013.