Reusing (Safety-oriented) Compliance Artifacts while Recertifying

Julieth Patricia Castellanos Ardila[a] and Barbara Gallina[b]
IDT, Mälardalen University, Västerås, Sweden
{*julieth.castellanos, barbara.gallina*}*@mdh.se*

Keywords: Process Recertification, Systematic Reuse, Automated Compliance Checking, ISO 14971.

Abstract: Revisions of safety-related standards lead to the release of new versions. Consequently, products and processes need to be recertified. To support that need, product line-oriented best practices have been adopted to systematize reuse at various levels, including the engineering process itself. As a result, Safety-oriented Process Line Engineering (SoPLE) is introduced to systematize reuse of safety-oriented process-related artifacts. To systematize reuse of artifacts during automated process compliance checking, SoPLE was conceptually combined with a logic-based framework. However, no integrated and tool-supported solution was provided. In this paper, we focus on process recertification (interpreted as the need to show process plan adherence with the new version of the standard) and propose a concrete technical and tool-supported methodological framework for reusing (safety-oriented) compliance artifacts while recertifying. We illustrate the benefits of our methodological framework by considering ISO 14971 versions, and measuring the enabled reuse.

1 INTRODUCTION

Revisions of safety-related standards lead to the release of new versions. Adjustments resulting from adding, deleting, or modifying requirements change the compliance status of organizations. Consequently, products and processes need to be recertified. To maintain processes compliance back in line, manufacturers perform a gap analysis between standards versions. A gap analysis permits manufacturers to understand what can be reused in terms of process information and process compliance demonstration (Gallina et al., 2014). In general, by reading the requirements of prescriptive standards, it is possible to identify similarities regarding tasks, work products, and other process-related artifacts, which are candidates for reuse. Based on product line-oriented best practices, reuse can be systematized at various levels, including the engineering process itself. As a result, Safety-oriented Process Line Engineering (SoPLE) (Gallina et al., 2012) is introduced to systematize reuse of safety-oriented process-related artifacts.

To increase confidence in process compliance via compliance proofs and efficiency via systematic reuse (Castellanos Ardila and Gallina, 2017), SoPLE was conceptually combined with a logic-based framework. The initial logic-based framework was adapted to be used with safety-related software processes (Castellanos Ardila et al., 2018a; Castellanos Ardila et al., 2018b). As such, it requires users to model process plans checkable for compliance in EPF-C (Eclipse-Foundation, 2018) (recently migrated from Eclipse Galileo 3.5.2 to Eclipse Neon 4.6.3 (Javed and Gallina, 2018a)), which provides the environment for modeling SPEM 2.0 (Systems & Software Process Engineering Metamodel) (OMG, 2008)-like artifacts. Process models of this type are composed of artifacts enriched with compliance information through annotations representing formalized standards requirements in FCL (Formal Contract Logic) (Governatori, 2005). FCL, a logic used to interpret and model normative knowledge, can be formally verified with Regorous (Governatori, 2015), a compliance checker created in the business and legal context. The addition of SoPLE was meant to extend systematic reuse to the automated compliance checking artifacts included in such models. However, no integrated and tool-supported solution was provided.

In this paper, we focus on showing process plan adherence with new versions of standards and propose a concrete technical and tool-supported methodological framework for reusing (safety-oriented) compliance artifacts while recertifying. In particular, we include the tool support for variability management offered by BVR-T (Base Variability Resolution Tool (SINTEF, 2016)), included in the tool-chain EPF-C ∘ BVR-T (Javed and Gallina, 2018b). EPF-

[a] https://orcid.org/0000-0001-9970-7580
[b] https://orcid.org/0000-0002-6952-1053

C ○ BVR-T was developed in the context of the AMASS project (de la Vara et al., 2019) and was used in the space domain (Gallina, 2019). Systematic reuse of compliance checking artifacts is done in four steps. 1) Initial compliance checking of single process plans is performed, via EPF-C and Regorous. 2) The resulting models are used as the base for evaluating commonalities and variabilities while adding standards of the same family, e.g., different versions of the same standard. The artifacts that vary are modeled in EPF-C. 3) The analysis of the compliance status of the standard-specific artifacts that are part of the variability is performed by taking into account the annotated compliance information. The compliance status can be analyzed by using Regorous. 4) The tool-chain EPF-C ○ BVR-T is used to model the families included in the compliance checking process, pre-check the choices at variation points and deliver the concrete standard-specific (safety-oriented) compliance checking artifacts, i.e., process models, rulesets denoting formalized requirements from standards, and compliance annotated process artifacts. We illustrate the benefits of our tool-supported methodological framework by considering the evolution (i.e., new versions of the standard resulting from revisions) of ISO 14971 (ISO, 2000)-process for risk management to medical devices. In particular, when published, ISO 14971:2007 (ISO, 2007) was internationally endorsed. In contrast, EN ISO 14971:2012 (ISO, 2012) is harmonized with EU directives for the European market. The latest version, ISO 14971:2019 (ISO, 2019), is internationally endorsed again. Thus, ISO 14971-related compliance is challenging for manufacturers of medical devices, who need to find approval from regulatory bodies within and outside the EU. By measuring the enabled reuse, we answer the question *To what extent process-related compliance artifacts can be reused?*

The paper is organized as follows. In Section 2, we provide essential background. In Section 3, we present our methodological framework for compliance checking artifacts reusability. In Section 4, we illustrate our methodological framework by considering ISO 14971 versions, and measure the enabled reuse. In Section 5, we discuss our findings. In Section 6, we present related work. Finally, in Section 7, we conclude our work and present future work.

2 BACKGROUND

In this section, we provide basic information on which we base our work.

2.1 ISO 14971 and Its Evolution

ISO 14971 (ISO, 2000) specifies the process required to identify hazards, estimate, evaluate, control, and monitor the risk of medical devices during its lifecycle. The content of ISO 14971 has been evolving over the years (Pulla and Bregu, 2020), incorporating consensus-based modifications and refinements. As a result, different versions have been published, i.e., ISO 14971:2007 (ISO, 2007), EN ISO 14971:2012 (ISO, 2012) and ISO 14971:2019 (ISO, 2019). Relevant concepts that are used in the following sections are presented in italics. In particular, the risk analysis phase in ISO 14971:2007 and EN ISO 14971:2012 corresponds to *clause 4* and requires the planning of three tasks, i.e., 1) *Define use/safety characteristics*, 2) *Estimate risks* and 3) *Identify hazards*. In contrast, the same phase corresponds to *clause 5* in ISO 14971:2019 and the task *Define use/safety characteristics* should be divided into two. For ISO 14971:2007, *the manufacturer shall discard the negligible risk*. Annexes of EN ISO 14971:2012 and ISO 14971:2019 provide a deviation, i.e., *the manufacturer shall consider all risks*. In all versions, *the manufacturer* is the role in charge, *the risk management plan* is the prerequisite of the clause, and the work products are *risk analysis document* and *risk management file*. The risk analysis document requires information regarding the *medical device description and identification, the identification of the person and organization, the scope, date, the intended use, and reasonably foreseeable misuse, the qualitative/quantitative safety characteristics of the medical device, known and foreseeable hazards associated with the medical device, fault conditions, reasonably foreseeable sequences of events,* and *the resulting hazardous situation*. Additional information is prescribed by ISO 14971:2019, i.e., *intended medical indication, patient population, part of the body/tissue, user profile,* and *operating principle*.

2.2 Automated Compliance Checking

Our logic-based framework for automated compliance checking (Castellanos Ardila et al., 2018a) requires process engineers to model process plans enriched with compliance annotations (see Fig. 1), which are extracted from formalized standards requirements. An expert in FCL (Formal Contract Logic) (Governatori, 2005) performs the required formalization. FCL is a logic that supports the modeling of norms representing obligations (**[O]**) and permissions (**[P]**) in a normative context that can be defeated by evolving knowledge. In FCL, norms are implications in which the antecedent represents the conditions for the requirements' applicability, and the conclusion represents compliance effects. Compliance effects express the concrete behavior of the process elements that adhere to standards requirements. Regorous receives the models automatically transformed from EPF-C (see (Castellanos Ardila et al., 2018b)) and perform the automated compliance analysis. The process engineer uses compliance results (which have the potential to be transformed back into EPF-C-like formats) to perform compliance analysis and improve the process compliance iteratively.

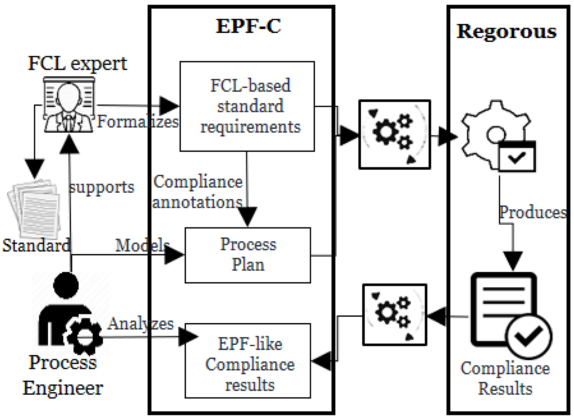


Figure 1: Process compliance checking framework.

More concretely, EPF-C is used to model the base process and its related library (see Fig. 2-(A_1)). A *role* represents who does a *task*. *Work products* identify a type of artifacts resulting from a task. *Guidance* represents free-form documentation that can be attached to process elements. A task is related to other elements as depicted in Fig. 2-(A_2). For performing automated compliance checking, the process engineer needs to model three plugins[1] in EPF-C (see Fig. 2-(A), -(B) and -(C)).

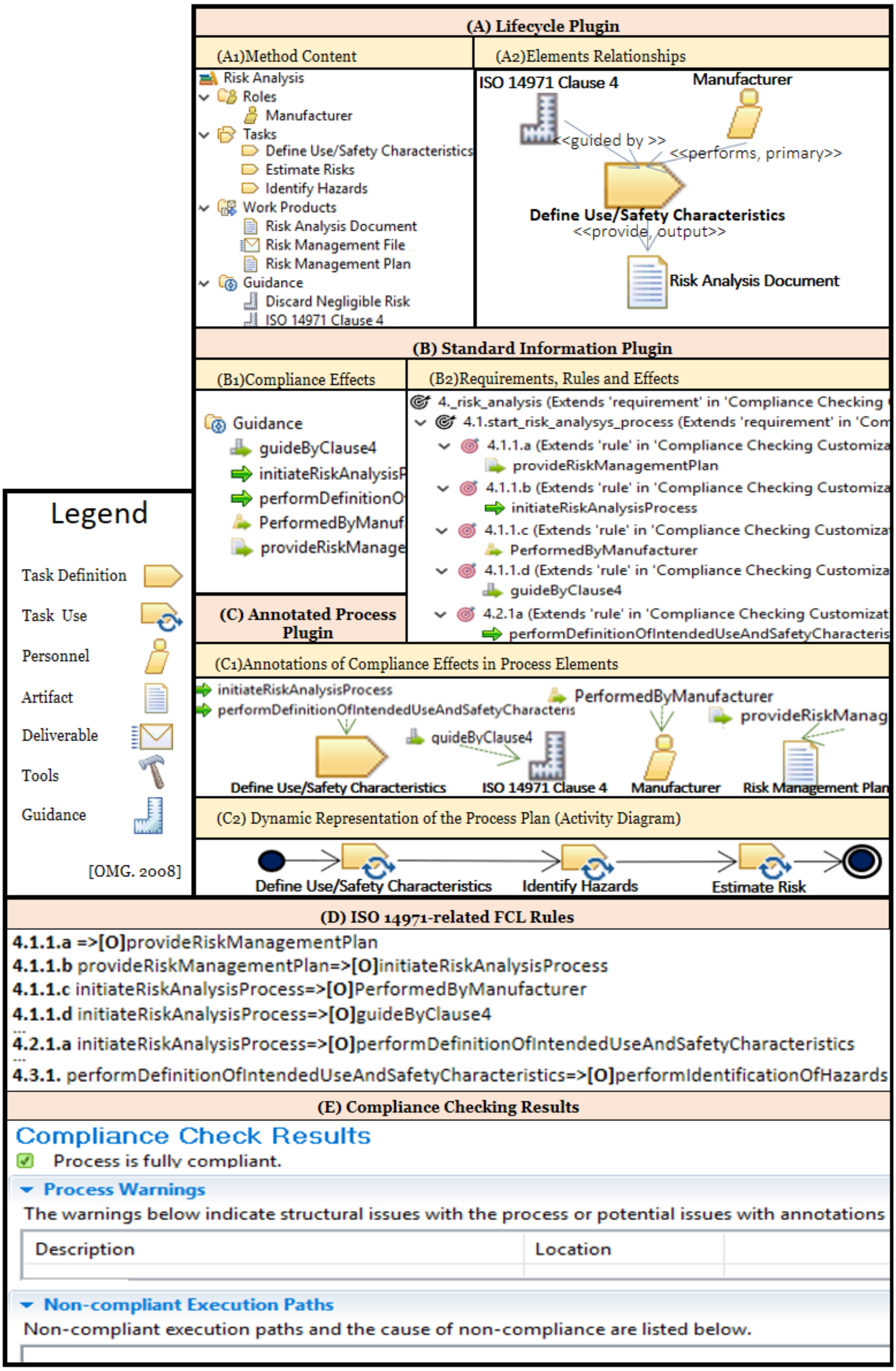
The **Lifecycle Plugin** (see Fig. 2-(A)) contains the method content necessary to create process plans. Fig. 2-(A_1) depicts method content required for manufacturing a medical device in compliance with ISO 14971:2007 (see (Pulla and Bregu, 2020)).

The **Standard Information Plugin** (see Fig. 2-(B)) contains the standard requirements and their formalization in FCL. To model FCL-related information, rule propositions are modeled by using SPEM 2.0 guidance elements customized in a specific way (Castellanos Ardila and Gallina, 2020). For this, we take into account the type of process elements that are targeted by the standard requirements. As a result, process elements definition are represented with specific icons (see Fig. 2-(B_1)) and the propositions are created based on templates, i.e., perform$\{$*TaskName*$\}$, provide$\{$*WorkProductName*$\}$, guidedBy$\{$*GuidanceName*$\}$, performedBy$\{$*RoleName*$\}$. Similarly the definition of process elements properties, i.e., $\{$*ElementName*$\}$with$\{$*Element Property*$\}$. Requirements and rules are also represented with specific customized icons (see Fig. 2-(B_2)). A set of FCL rules for ISO 14971-risk analysis is presented in Fig. 2-(D). For example, rule 4.1.1.a refers to the provision of the prerequisite, which as recalled in Section 2.1, is an obligation. Once provided, we have the obligation of initiate the risk analysis process (see 4.1.1.b).

The **Compliance Annotated Process Plugin** contains the process annotated with compliance effects (see Fig. 2-(C)). The annotation requires users to evaluate the effect that each element provide to the overall process compliance (see Fig. 2-(C_1)). For example, the task *DefineUse/SafetyCharacteristics* is used to initiate the risk analysis process and to perform the definition of intended use and safety characteristics. Thus, we annotate it with the corresponding compliance effects. Then, a dynamic representation of the process plans is created with the annotated process elements (see Fig. 2-(C_2)).

Regorous automatically generates a compliance state representation of the annotated process plan and analyses compliance against the FCL ruleset by using two functions. The function *State(t,i)* returns the state of a *task (t)*, in the *step (i)*. The function *Force(t,i)* = $\{O\}$ associates to each *task (t)*, in the *step (i)* a set of *obligations O*. See, for example, the rules 4.1.1.a, 4.1.1.b, 4.1.1.c, 4.1.1.d. and 4.2.1.a, presented in the ruleset excerpt (see Fig. 2-(D)). These rules represent the obligations in force at different steps. Thus, rule 4.1.1.a forces the first obligation, i.e., Force(1,1) = [O]provideRiskManagementPlan. In a similar manner, the subsequent rules are forced, because the antecedent is getting fulfilled. *Define use/Safety Characteristics* is the first task in the workflow (see Fig. 2-(C_2)), and all the elements are associated to this task (Fig. 2-(A_2)) have their corresponding annotated compliance effects (see Fig. 2-(C_1)). Thus, the state representation of this task, State (1,1), contains all the compliance effects required by the force functions and the task is compliant. Regorous apply this strategy to the whole workflow and provide the compliance status of the process as well as the counterexamples in case of rules violations. When no counterexamples exist, Regorous defines that the process is compliant (see Fig. 2-(E)).

[1] An EPF-C plugin is a mechanism for packaging content providing modularization and extensibility.


(A) Lifecycle Plugin
(A1)Method Content
Risk Analysis
Roles
Manufacturer
Tasks
Define Use/Safety Characteristics
Estimate Risks
Identify Hazards
Work Products
Risk Analysis Document
Risk Management File
Risk Management Plan
Guidance
Discard Negligible Risk
ISO 14971 Clause 4
(A2)Elements Relationships
ISO 14971 Clause 4
Manufacturer
<<guided by >>
<<performs, primary>>
Define Use/Safety Characteristics
<<provide, output>>
Risk Analysis Document
(B) Standard Information Plugin
(B1)Compliance Effects
Guidance
guideByClause4
initiateRiskAnalysisP
performDefinitionO
PerformedByManuf
provideRiskManage
(B2)Requirements, Rules and Effects
4._risk_analysis (Extends 'requirement' in 'Compliance Checking
4.1.start_risk_analysys_process (Extends 'requirement' in 'Com
4.1.1.a (Extends 'rule' in 'Compliance Checking Customiza
provideRiskManagementPlan
4.1.1.b (Extends 'rule' in 'Compliance Checking Customiza
initiateRiskAnalysisProcess
4.1.1.c (Extends 'rule' in 'Compliance Checking Customiza
PerformedByManufacturer
4.1.1.d (Extends 'rule' in 'Compliance Checking Customiza
guideByClause4
4.2.1a (Extends 'rule' in 'Compliance Checking Customizat
performDefinitionOfIntendedUseAndSafetyCharacteris
Legend
Task Definition
Task Use
Personnel
Artifact
Deliverable
Tools
Guidance
[OMG. 2008]
(C) Annotated Process Plugin
(C1)Annotations of Compliance Effects in Process Elements
initiateRiskAnalysisProcess
performDefinitionOfIntendedUseAndSafetyCharacteris
PerformedByManufacturer
provideRiskManag
guideByClause4
Define Use/Safety Characteristics
ISO 14971 Clause 4
Manufacturer
Risk Management Plan
(C2) Dynamic Representation of the Process Plan (Activity Diagram)
Define Use/Safety Characteristics
Identify Hazards
Estimate Risk
(D) ISO 14971-related FCL Rules
(E) Compliance Checking Results

4.1.1.a =>**[O]**provideRiskManagementPlan
4.1.1.b provideRiskManagementPlan=>**[O]**initiateRiskAnalysisProcess
4.1.1.c initiateRiskAnalysisProcess=>**[O]**PerformedByManufacturer
4.1.1.d initiateRiskAnalysisProcess=>**[O]**guideByClause4
...
4.2.1.a initiateRiskAnalysisProcess=>**[O]**performDefinitionOfIntendedUseAndSafetyCharacteristics
...
4.3.1. performDefinitionOfIntendedUseAndSafetyCharacteristics=>**[O]**performIdentificationOfHazards

Compliance Check Results

☑ Process is fully compliant.

Process Warnings

The warnings below indicate structural issues with the process or potential issues with annotations

Description	Location

Non-compliant Execution Paths

Non-compliant execution paths and the cause of non-compliance are listed below.

Figure 2: Modeling process plans checkable for compliance.

2.3 Compliance Proofs Reuse

A methodological framework (see Fig. 3) for enabling reuse of compliance proofs (Castellanos Ardila and Gallina, 2017) includes the combination of formal approaches with SoPLE (Safety-oriented Process Line Engineering) (Gallina et al., 2012). SoPLE manages families of processes and standards (i.e., families that exhibit several commonalities and differ via as set of managed variabilities, e.g., different versions of a standard). In SoPLE, commonalities, indeed, represent clearly reusable elements. These commonalities are defined beyond the syntactical comparison. We are interested in extracting full commonalities, i.e., whenever two elements of the same type expose only common aspects. With our methodological framework, we learned that proofs of compliance could be fully or partially reused, depending on the compliance effects produced by the variability. In Section 3.1, we extend the compliance analysis of such reuse.

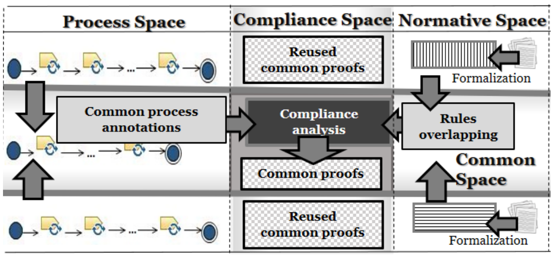


Figure 3: Framework for compliance proofs reuse.

The framework is composed by four spaces where the process engineer perform specific actions.

1. In the process space, he/she models a Safety-oriented Process Line (SoPL). A SoPL includes manually modeling the skeleton (with commonalities and variabilities) of the process sequence.
2. In the normative space, he/she formalizes rules and models a SoPL-like structure with such rules, i.e., selects the set of rules that overlap.
3. In the common space, he/she analyzes the compliance of commonalities between the process-related SoPL with the SoPL-like rules.
4. In the compliance space, he/she analyzes the compliance effects of the tasks that contribute to the variabilities in the standard-specific process.

2.4 EPF-C ∘ BVR-T

EPF-C ∘ BVR-T (Javed and Gallina, 2018b) is a tool-chain composed by EPF (recalled in Section 2.2) Composer and BVR-T (Base Variability Resolution Tool) (SINTEF, 2016) that enables SoPLE (recalled in Section 2.3). We focus on BVR-T. As summarized in (Gallina et al., 2020), BVR-T is used to manage the variability by providing an environment in which families of different kinds, e.g., processes or products, can be modeled. A BVR model consist of three parts. The first part is the variability model, called VSpec, which permits users to model the family via a feature diagram-like fashion supplemented with constraints. Feature diagrams permit to define the distinctive user-visible aspects of the family members that are common and that vary. Table 2 recalls some basic elements. A choice represents a yes/no decision. A constraint (given in Basic Constraint Language-BCL) specifies restrictions on permissible resolution models. A group dictates the number of choice resolutions. For example, 1..1 (represents an XOR) identifies that one of the child features must be selected. Solid lines permit to link the mandatory features to a parent feature, while dashed lines permit to link optional features. Fig. 5 depicts a VSpec diagram created with the mentioned elements.

Table 1: BVR essential modeling elements.

Choice	Constraint	Group
▭	▱	△

The second part, called the resolution, is used to allocate specific family members' values and validate such values. Thus, wrong choices violating the cross-variation points requirements designed in the VSpec can be detected. Finally, the realization permits users to bind conceptual resolutions with the concrete elements defined in EPF-C via the definition of fragment substitutions. The realization permits that specific processes are derived automatically. In this paper, we have not performed the realization part.

2.5 Reuse Measurement

A metric for reuse measurement is proposed by (Banker et al., 1993) (see below).

$$\%\,Reuse = (1 - \frac{Number\ of\ new\ objects\ built}{Total\ number\ of\ objects\ used}) * 100$$

The metric can be applied in hierarchical structures that permit the identification of the objects and the applications to which they were originally created. This metric is expressed in terms of percentage by considering the proportion of the number of new objects built (created from scratch) and the total number of objects used (in the absence of reuse). Besides, it focuses on the total benefit attributable to reuse. Thus, objects that are reused multiple times are considered to represent multiple instances of reuse.

3 COMPLIANCE ARTIFACTS REUSABILITY

In this section, we present our methodological framework for compliance artifacts reusability.

3.1 Compliance Analysis

The skeleton of a family in SoPLE (as recalled in Section 2.3) is represented as the sequence C1-V1-C2 (see Fig. 4). Such sequence is called the Safety-oriented Process Line or SoPL, where C1 and C2 represent the commonalities in the family and V1 represent the variability. For compliance checking (as recalled in Section 2.2), C1 and C2 are annotated with the compliance effects a and b, respectively. When deriving processes from the family, the variability, V1, is replaced either with R1 or R2, according to some aspect, e.g., the selection of a specific standard. Moreover, R1 is annotated with c, while R2 does not have any annotation.

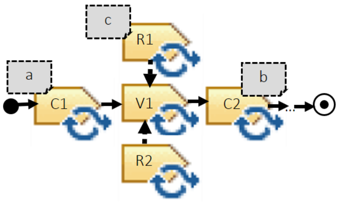


Figure 4: SoPL skeleton of a family of processes.

The VSpec model representing the skeleton of the family C1-V1-C2 is described in VSpec as features connected to the parent feature (Checking_Management) via solid lines (see Fig. 5). The variability R1 and R2 are connected via dashed lines. Additional information can be modeled. In particular, the standard versions (e.g., S1 and S2) are modeled with a group element. Moreover, BCL constraints are created to restrict the selection of the variations according to the selected standard, e.g., if S1 is selected, then R1 and its effect c become mandatory features.

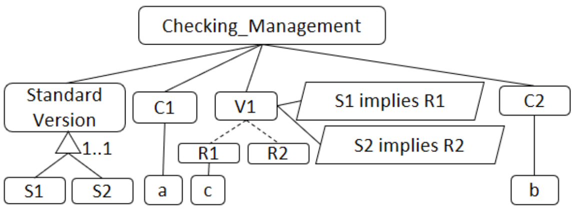
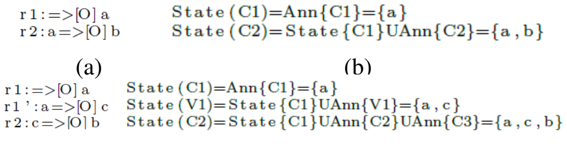


Figure 5: VSpec model of the checking management.

The compliance state representation of the baseline skeleton (see Fig. 6b) is different from the derived family member, in which the replacement R1, which is annotated with the compliance information c, is replaced in V1 (see Fig. 6d). Such representations have to comply with the respective ruleset (see Figs. 6a, 6c)



```
r1:=>[O] a
r2:a=>[O] b
```

(a)

```
State(C1)=Ann{C1}={a}
State(C2)=State{C1}UAnn{C2}={a,b}
```

(b)

```
r1:=>[O] a
r1':a=>[O] c
r2:c=>[O] b
```

(c)

```
State(C1)=Ann{C1}={a}
State(V1)=State{C1}UAnn{V1}={a,c}
State(C2)=State{C1}UAnn{C2}UAnn{C3}={a,c,b}
```

(d)

Figure 6: Effects/State representation of the variability.

Changes in the compliance status of the derived standard-specific processes depend on the normative effect of the variant. If $c = 0$, the composition of the process elements would not affect compliance since the ruleset in Fig 6a, would be the same that applies to the SoPLE-member. For $c \neq 0$, there are two cases. First, the effect is local to the task, i.e., the effect is triggered and fulfilled in the variant. Second, the variant effect is not triggered by a previous task and/or make a new influence in the subsequent task effect (see Fig. 6c). In both cases, the compliance status may be affected. For these cases, we consider the separations of concerns within the regulatory space and check the structural compliance (first case) separately from the compliance of the sequence of tasks (second case). The former permits the integration of the proof in the line without affecting the general compliance status. Such checking can be performed by BVR-T, which checks the presence/absence of process elements features. The latter makes the reuse of proof conditioned to additional compliance analysis of the tasks surrounding the variant (C1 and C2 in Fig. 4). This analysis can be performed by Regorous.

3.2 Systematic Reuse of Compliance Artifacts

The systematic reuse of compliance artifacts requires four steps (see Fig. 7).

1. **Manage Single Process Plan Compliance.** We seek for single process plan compliance by using the automated compliance checking method recalled in Section 2.2. Resulting artifacts are three EPF-C plugins and the compliance results issued by Regorous.

2. **Model the Variability.** We evaluate the commonalities and variabilities regarding the models obtained in step 1) while adding standards of the same family, e.g., different versions of the same standard. For this, we use the method recalled in Section 2.3. The artifacts that vary are modeled in EPF-C. Thus, the resulting models are a lifecycle plugin and standard

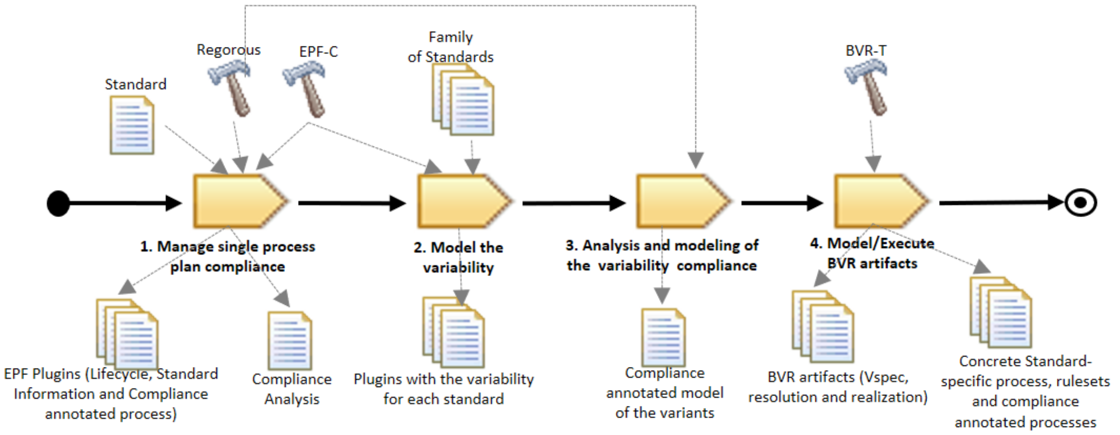

Standard
Regorous
EPF-C
Family of Standards
BVR-T
1. Manage single process plan compliance
2. Model the variability
3. Analysis and modeling of the variability compliance
4. Model/Execute BVR artifacts
EPF Plugins (Lifecycle, Standard Information and Compliance annotated process)
Compliance Analysis
Plugins with the variability for each standard
Compliance annotated model of the variants
BVR artifacts (Vspec, resolution and realization)
Concrete Standard-specific process, rulesets and compliance annotated processes

Figure 7: Family-oriented compliance checking process.

information plugin for each standard evolution, containing only artifacts related to the variability.

3. **Analysis and Modeling of the Variability Compliance.** An analysis of the changes in the compliance status of the standard-specific artifacts that are part of the variability, as presented in Section 3.1, is performed by taking into account the annotated compliance information. If needed, we use Regorous. However, if the variant is small, such analysis can be done manually. The result of this step is the compliance annotated process model of the variants.

4. **Model BVR Artifacts.** BVR-T is used to create the abstract representation of the families involved in compliance checking, i.e., lifecycle, standard information and compliance annotated processes. Resolution models are automatically generated from the VSpec models, and use to validate the membership of the elements according to the selected standard. In a final step, which is not part of the scope of this paper, realization models are created. Realization permits to define the replacements that should be part of the concrete standard-related artifacts that are exported back to EPF-C. Thus, in this step we use the tool-chain EPF-C ∘ BVR-T, recalled in Section 2.4.

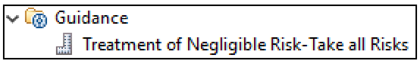
4 REUSE WITHIN ISO 14971 EVOLUTION

In this section, we use our solution (presented in Section 3.2) to systematize and measure compliance artifacts reuse within the evolution of the ISO 14971 standards (recalled in Section 2.1).

4.1 ISO 14971 Evolved Artifacts

As presented in Fig. 7, the first step consists of seeking the compliance of a process plan against an initial standard, in this case, ISO 14971:2007. The results of this step are three plugins that contain process elements, compliance rules, annotated process models (see Fig. 2-(A), -(B) and -(C)), and the compliance analysis delivered by Regorous (see Fig. 2-(E)), which shows that the process is compliant with the rules derived from the standard.

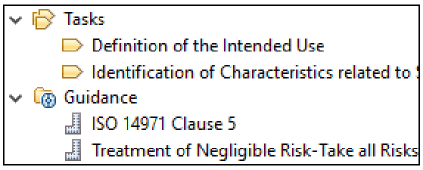
The second step consists of modeling the variability, i.e., we perform a gap analysis and model the additional artifacts imposed by the new standard versions. In particular, a new process element is additionally required for compliance with EN ISO 14971:2012, i.e., the guidance related to the inclusion of all risks for the treatment of negligible risk (see Fig. 8).



Guidance
Treatment of Negligible Risk-Take all Risks

Figure 8: EN ISO 14971:2012-Variable process elements.

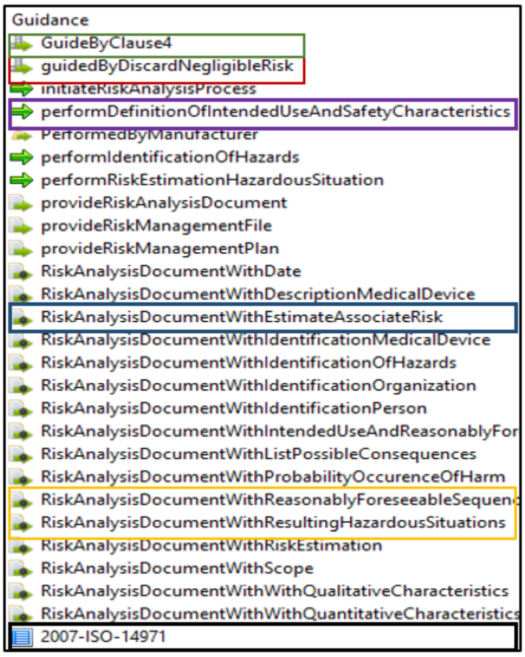
In contrast, four new elements are required for compliance with ISO 14971:2019, i.e., two guidance elements (ISO 14871 clause 5 and the treatments of negligible risk), and two additional tasks, which are the result of splitting the task *Define/use safety characteristics* (see Fig 9).



Tasks
Definition of the Intended Use
Identification of Characteristics related to
Guidance
ISO 14971 Clause 5
Treatment of Negligible Risk-Take all Risks

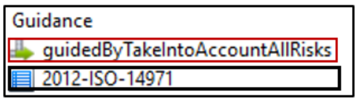
Figure 9: ISO 14971:2019-Variable process elements.

We also model the compliance effects. Fig. 10 represents compliance effects extracted from ISO 14971:2007. Fig. 11 shows 1 new compliance effect found in EN ISO14971:2012, while Fig. 12 shows 11 new compliance effects found in ISO 14971:2019.



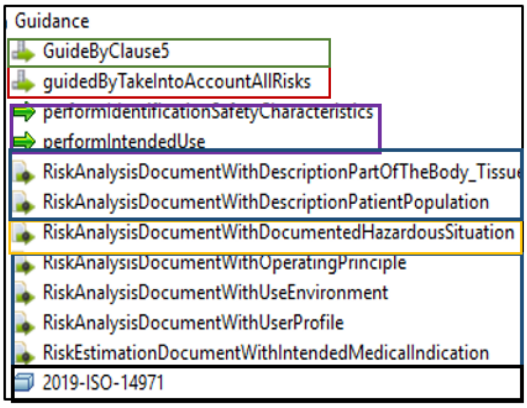
```
Guidance
GuideByClause4
guidedByDiscardNegligibleRisk
initiateRiskAnalysisProcess
performDefinitionOfIntendedUseAndSafetyCharacteristics
PerformedByManufacturer
performIdentificationOfHazards
performRiskEstimationHazardousSituation
provideRiskAnalysisDocument
provideRiskManagementFile
provideRiskManagementPlan
RiskAnalysisDocumentWithDate
RiskAnalysisDocumentWithDescriptionMedicalDevice
RiskAnalysisDocumentWithEstimateAssociateRisk
RiskAnalysisDocumentWithIdentificationMedicalDevice
RiskAnalysisDocumentWithIdentificationOfHazards
RiskAnalysisDocumentWithIdentificationOrganization
RiskAnalysisDocumentWithIdentificationPerson
RiskAnalysisDocumentWithIntendedUseAndReasonablyFor
RiskAnalysisDocumentWithListPossibleConsequences
RiskAnalysisDocumentWithProbabilityOccurenceOfHarm
RiskAnalysisDocumentWithReasonablyForeseeableSequen
RiskAnalysisDocumentWithResultingHazardousSituations
RiskAnalysisDocumentWithRiskEstimation
RiskAnalysisDocumentWithScope
RiskAnalysisDocumentWithWithQualitativeCharacteristics
RiskAnalysisDocumentWithWithQuantitativeCharacteristics
2007-ISO-14971
```

Figure 10: ISO 14971:2007-Compliance effects.



```
Guidance
guidedByTakeIntoAccountAllRisks
2012-ISO-14971
```

Figure 11: EN ISO 14971:2012-Effects variability.

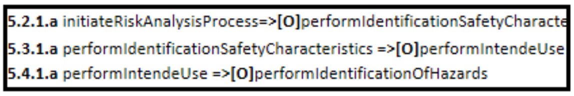


```
Guidance
GuideByClause5
guidedByTakeIntoAccountAllRisks
performIdentificationSafetyCharacteristics
performIntendedUse
RiskAnalysisDocumentWithDescriptionPartOfTheBody_Tissu
RiskAnalysisDocumentWithDescriptionPatientPopulation
RiskAnalysisDocumentWithDocumentedHazardousSituation
RiskAnalysisDocumentWithOperatingPrinciple
RiskAnalysisDocumentWithUseEnvironment
RiskAnalysisDocumentWithUserProfile
RiskEstimationDocumentWithIntendedMedicalIndication
2019-ISO-14971
```

Figure 12: ISO 14971:2019-Effects variability.

Figs. 10, 11, and 12 also depict artifacts highlighted with colors. Such colors represent replacements that are necessary to be done during the standard-specific derivation. For example, performIdentificationofSafetyCharacteristics and performIntendedUse, created for the ISO 14971:2019 ruleset, are meant to replace the effect performDefinitionOfIntendedUseAndSafetyCharacteristics, created for the ISO 14971:2007. In black, we highlight an artifact which contains the general information of the ruleset, which also varies with each standard. Compliance effects that are not highlighted represent artifacts that are common and can be reused.

In Step 3, the compliance analysis of the variability is performed, as presented in Section 3.1. In our case, we found that the compliance with EN ISO 14971:2012 requires that one new element, specifically a guidance called *Treatment of Negligible Risk-Take all Risks* (see Fig. 8) is annotated with a compliance effect called *guidedByTakeIntoAccountAllRisks* (see Fig. 11). A more complex analysis is performed in the case of ISO 14971:2019. In particular, there are requirements that mandate the replacement of the task Define/Use Safety Characteristics. This implies a variation in the ruleset as presented in Fig. 13, which is evidently different from the ruleset created for ISO 14971:2007 (see Fig. 2-(*D*)). With the introduction of these requirements, the compliance flow changes. Thus, we need to use Regorous for perform compliance checking in the first 3 tasks of the new workflow.



```
5.2.1.a initiateRiskAnalysisProcess=>[O]performIdentificationSafetyCharacte
5.3.1.a performIdentificationSafetyCharacteristics =>[O]performIntendeUse
5.4.1.a performIntendeUse =>[O]performIdentificationOfHazards
```

Figure 13: Ruleset variation respect ISO 14971:2019.

The remaining new elements (see Fig. 9) trigger and fulfil themselves the new compliance effects (see Fig 12). The result of this analysis corresponds to the compliance annotations presented in Table 2.

Table 2: ISO 14971: 2019-related Annotations.

Element	Compliance Effect
Task: Definition of the Intended Use	performIntendedUse, initiateRiskAnalysisProcess
Task: Identification of Characteristics related to Safety	performIdentificationSafetyCharacteristics
Work Product: Identification of Characteristics related to Safety	RiskAnalysisDocumentWithDescriptionPartOfTheTissue, RiskAnalysisDocumentWithDescriptionPatientPopulation, RiskAnalysisDocumentWithDocumentedHazardousSituation, RiskAnalysisDocumentWithIntendedMedicalIndication, RiskAnalysisDocumentWithIntendedUseAndReasonablyForeseeableMisuse, RiskAnalysisDocumentWithOperatingPrinciple, RiskAnalysisDocumentWithUseEnvironment, RiskAnalysisDocumentWithUserProfile
Guidance: ISO 14971 Clause 5	GuideByClause5
Guidance: Treatment of Negligible Risk-Take all Risks	guidedByTakeIntoAccountAllRisks

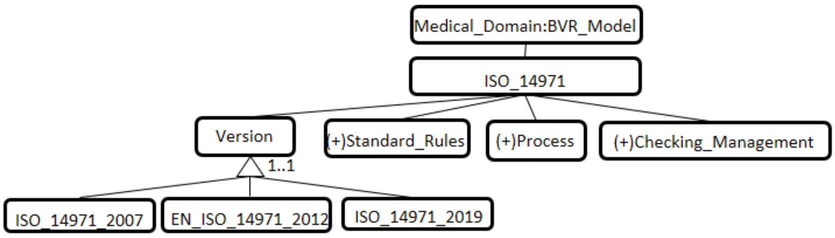


Figure 14: BVR VSpec.

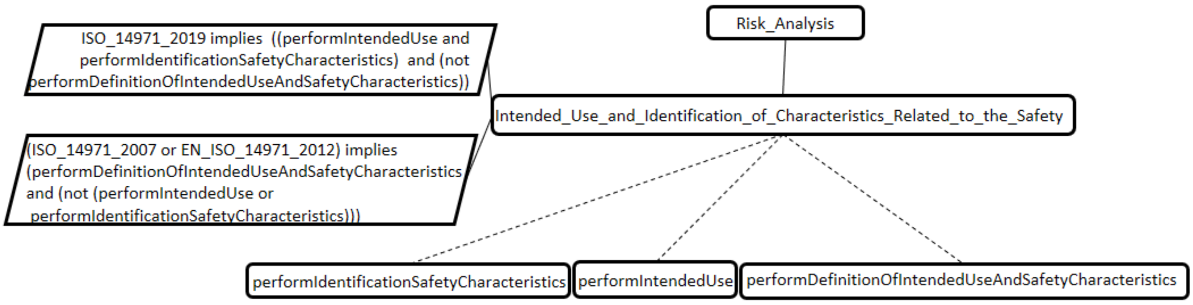

Risk_Analysis
ISO_14971_2019 implies ((performIntendedUse and performIdentificationSafetyCharacteristics) and (not performDefinitionOfIntendedUseAndSafetyCharacteristics))
Intended_Use_and_Identification_of_Characteristics_Related_to_the_Safety
(ISO_14971_2007 or EN_ISO_14971_2012) implies (performDefinitionOfIntendedUseAndSafetyCharacteristics and (not (performIntendedUse or performIdentificationSafetyCharacteristics)))
performIdentificationSafetyCharacteristics
performIntendedUse
performDefinitionOfIntendedUseAndSafetyCharacteristics

Figure 15: Variation related to compliance effects.

The fourth step is the modeling of BVR artifacts. In this step, we model the VSpecs of the families corresponding to the process, ruleset, and checking management. All the families are created under the same root, i.e., ISO_14971 (see Fig. 14). A branch of the feature model tree contains the version of the standards used to make the changes at variation points.

The interested reader may refer to (Pulla and Bregu, 2020) for detailed information regarding the VSpec of the process for risk management with ISO 14971. In this paper, we focus on the VSpec model for the ruleset and the checking management. For example, Fig. 15 depicts the representation of the compliance effects related to the requirements that impose the creation of the task Define use/safety characteristics. In particular, as presented in Section 2.1, such task is mandatory for ISO 14971:2007 and EN ISO 14971:2012, while in ISO 14971:2019 becomes two tasks, i.e., intended Use and Identification of Safety Characteristics. Thus, the three compliance effects (highlighted in purple in Figs. 10 and 11) are modeled and two BCL constraints are created to define the variations regarding the version of the standard selected. For example, if the standard ISO_14971_2019 is selected in the branch of the version, BVR resolution will check that we select performIdentificationSafetyCharacteristics and performIntendedUse during the selection of the family-member corresponding to the ruleset of such version. The VSpec for the branch compliance checking management, contains the compliant process elements grouped by their concern, i.e., tasks, role, work product, and guidance, and enriched with the compliance effects annotations. Fig. 16 presents the branch Compliant_Task that shows the set of tasks that should appear in the process plan as well as BCL constraint that restrict the correct representation according to the standard version selected. The resolution permits the selection of correct configuration that could be exported back to EPF-C via realization models. A realization model will permit to bind the selected configuration into the concrete EPF-C related models.

4.2 Reuse Measurement

In our approach, we opt to model the full commonalities between families of standards, the process they regulate, and the compliance annotations required for automated compliance checking. Full commonalities can be guaranteed by atomizing the elements in the compliance spaces as much as possible so that only common aspects are present. For this reason, we consider that the commonalities included in the modeling of such families have the potential to be fully reusable. In that light, the percentage of reuse of compliance artifacts can be performed by using the metric defined for reuse measurement which is recalled in Section 2.5.

4.2.1 Reuse-related to EN ISO 14971:2012

For compliance with EN ISO 14971:2012, the guidance called Treatment of Negligible Risk-Take all Risks (see Fig. 8) was additionally re-

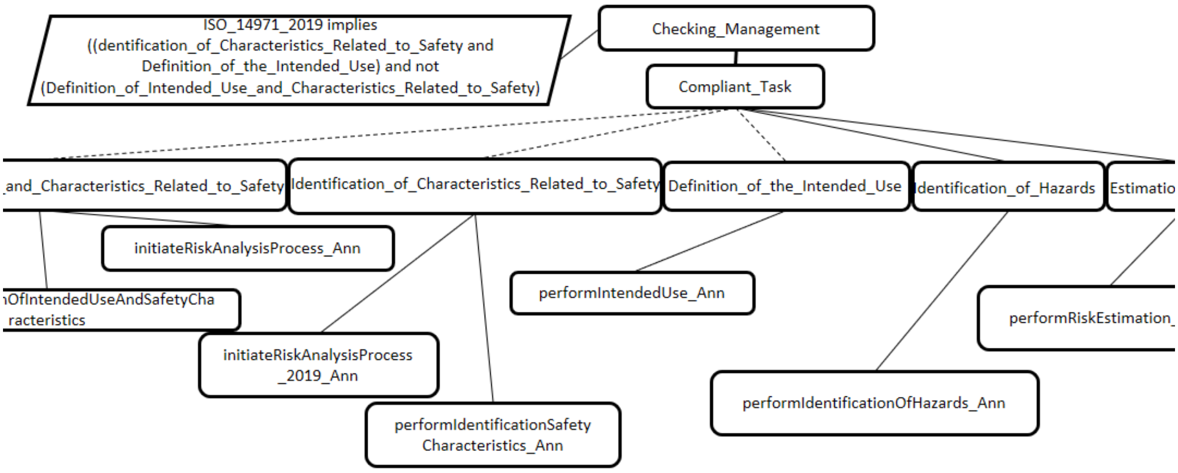

ISO_14971_2019 implies ((dentification_of_Characteristics_Related_to_Safety and Definition_of_the_Intended_Use) and not (Definition_of_Intended_Use_and_Characteristics_Related_to_Safety)
Checking_Management
Compliant_Task
_and_Characteristics_Related_to_Safety
Identification_of_Characteristics_Related_to_Safety
Definition_of_the_Intended_Use
Identification_of_Hazards
Estimatio
initiateRiskAnalysisProcess_Ann
ıOfIntendedUseAndSafetyCharacteristics
initiateRiskAnalysisProcess_2019_Ann
performIdentificationSafetyCharacteristics_Ann
performIntendedUse_Ann
performIdentificationOfHazards_Ann
performRiskEstimation_

Figure 16: Variation related to annotated compliant tasks.

quired with respect to compliance established with ISO 14971:2007. In total, we used 9 process elements. Thus, the percentage of reuse is 88,9%. We also need to create 1 compliance effect and 1 ruleset (see Fig. 11). As we used 27 artifacts, the reuse is 92,3%. The compliance effect is associated to the new guidance, which corresponds to a new compliance annotation of 26 used in total. Thus, the reuse of compliance annotations is 96,2%. (See Table 3).

Table 3: Reuse measurement related to EN ISO 14971:2012.

Type of artifacts	New	Total Used	Reuse Percentage
Process	1	9	88,9%
Compl. Effects	2	27	92,3%
Compl. Annotations	1	26	96,2%

4.2.2 Reuse-related to ISO 14971:2019

For compliance with ISO 14971:2019, we need to create 4 new process artifacts (see Fig. 9), 11 new compliance effects (see Fig. 12) and perform 13 compliance annotations (see Table 2). The number of total artifacts was 10 process elements, and 32 compliance effects and compliance annotations. Thus, reuse is 60%, 61,3% and 59,4% respectively (see Table 4).

Table 4: Reuse measurement related to ISO 14971:2019.

Type of artifacts	New	Total Used	Reuse Percentage
Process	4	10	60%
Compl. Effects	12	32	61,3%
Compl. Annotations	13	32	59,4%

5 DISCUSSION

For coping with the recertification demands enforced by the new versions of standards (new requirements, jurisdictional changes) in the medical domain, process plan reconfiguration is necessary. Compliant process plan reconfiguration supported by models automatically checked for compliance is a plausible solution. Such solution involves the creation of new modeling artifacts, as presented in Section 4.1. However, it also involves high degrees of artifacts reuse, as presented in Section 4.2. In particular, Tables 3 and 4 shows a positive gain in terms of compliance checking artifacts reusability. With these percentages, the answer to the question posed in the introductory part of this paper, *to what extent process-related compliance artifacts can be reused?*, could be the following: the reuse extent in the context of medical devices is significant (the minimum gain was 59,4%). In particular, given that the manual configuration of process models checkable for compliance in EPF-C could be labor-intensive and time-consuming, the context of medical devices complying with ISO 14971 can positively benefit from the systematic reuse of compliance checking artifacts. In general, processes and standards that evince low levels of variation could be part of a family that exhibits high reuse levels in terms of compliance checking artifacts and could benefit from using our methodological framework during the required modeling task.

It is widely recognized that standards requirements are challenging to understand due to their wordiness and how they relate to each other. Their evolution is also challenging, due to the need to handle the normative changes and the recertification effort, which, as for ISO 14971, may include crossjurisdictional spaces. When using our methodological framework, process engineers need to analyze new requirements systematically. This analysis is required to determine whether an existing compliance checking-related artifact can fulfill a specific requirement as-is or with modifications (new properties should be added/deleted), or if new artifacts have to be modeled from scratch. It also highlights problems between requirements, which may put compliance at risk, i.e., contradictory requirements, real/fake dependencies between requirements and new compliance information applicable to existing process plans. The most important is that the process engineer's analysis is recorded in graphical models, which not only provide automated checks but also automated process plan's reconfiguration. Thus, our methodological framework supports a confident reduction of the work required to be done when new instances of compliant process plans have to be modeled.

6 RELATED WORK

The change triggered by updated standards for software process is a topic tackled from different perspectives. In (Ocampo and Münch, 2009), the authors propose a method that permits to attach change information to process documents to facilitate change understandability. However, no systematic methods to reuse modeling artifacts facilitating the changes are proposed as we do in our work. Methods for modeling the change/variation and reuse of processes result from the application of software process lines methodologies, as recently surveyed in (Teixeira et al., 2019). In particular, SoPLE (Gallina et al., 2012) has been exploited to provide a representation of family members with safety information, e.g., reusable process arguments used in safety cases (Martin et al., 2016) and tailoring of process models according to safety integrity levels of products (Bressan et al., 2020). In our work, we also use SoPLE to provide mechanisms to support variation knowledge reuse regarding compliance checking artifacts, which has not being yet addresses in other approaches.

Advances regarding compliance artifacts reusability exist in the business community. Some researchers tackled reuse by defining building blocks that implement compliance requirements, e.g., compliance scopes (Schleicher et al., 2011), and compliance fragments (Görlach et al., 2011; Ma, 2012). Reuse is also approached with the use of process patterns (Kabir et al., 2017), and rule patterns (Elgammal et al., 2016). In contrast, we propose a holistic modeling framework for safety-related process compliance checking that permits to model artifacts, which can be automatically interleaved with evolutionary/changing artifacts originated from new versions of standards. In that way, not only building blocks that implement compliance requirements (i.e., called in our framework, process models checkable for compliance) are reusable but also process models and rulesets denoting formalized requirements from standards.

7 CONCLUSIONS AND FUTURE WORK

Recertification is the consequence of the release of new versions of standards. In this paper, we focused on process recertification needs (interpreted as the need to show process plan adherence with the new version of the standard). Taking this into account, we proposed a concrete technical and tool-supported methodological framework for reusing (safety-oriented) compliance artifacts while recertifying. This methodological framework encompasses process modeling, process compliance checking, and variability management capabilities to enable systematic reuse and automatic generation of process-related compliance checking artifacts (i.e., process models, rulesets denoting formalized requirements from standards, and compliance annotated process artifacts). We illustrate our methodological framework within the family composed of the versions of the standard ISO 14971. Finally, we answer our initial question regarding the extent of reuse of process-related compliance artifacts by measuring the reuse enabled by our methodological framework. In particular, in the context of medical devices complying with different versions of ISO 14971, the reuse is significant. We concluded that processes and standards that evince low levels of variation (such as ISO 14971) could benefit from using our methodological framework during the modeling task required for compliance checking.

In the future, we intend to perform evaluations that consider the entire ISO 14971 and related standards (e.g., process improvement and security). Moreover, we plan to conduct controlled experiments to evaluate the users' perceived usefulness. We also believe that when creating/updating standards, process models, and formal representations of the requirements should also be provided. Thus, we plan to contact standardization bodies to investigate this possibility, which could reduce our approach's modeling effort and at the same time reduce undesired room for interpretation of the standards. Finally, we intend to use more elaborated measurement frameworks to provide evidence concerning our solution's efficiency in terms of time and cost reduction, as well as scalability.

REFERENCES

Banker, R., Kauffman, R., and Zweig, D. (1993). Repository Evaluation of Software Reuse. *IEEE Transactions on Software Engineering*, 19(4):379–389.

Bressan, L., de Oliveira, A. L., Campos, F., Papadopoulos, Y., and Parker, D. (2020). An integrated approach to support the process-based certification of variant-intensive systems. In *International Symposium on Model-Based Safety and Assessment*, pages 179–193.

Castellanos Ardila, J. P. and Gallina, B. (2017). Towards increased efficiency and confidence in process compliance. In *Systems, Software and Services Process Improvement*, pages 162–174.

Castellanos Ardila, J. P. and Gallina, B. (2020). Separation of concerns in process compliance checking: Divide-and-conquer. In *Systems, Software and Services Process Improvement*, pages 135–147.

Castellanos Ardila, J. P., Gallina, B., and Ul Muram, F. (2018a). Enabling Compliance Checking against Safety Standards from SPEM 2.0 Process Models. In *Euromicro Conference on Software Engineering and Advanced Applications*, pages 45 – 49.

Castellanos Ardila, J. P., Gallina, B., and UL Muram, F. (2018b). Transforming SPEM 2.0-compatible Process Models into Models Checkable for Compliance. In *18th International SPICE Conference*.

de la Vara, J. L., Parra, E., Ruiz, A., and Gallina, B. (2019). AMASS: A Large-Scale European Project to Improve the Assurance and Certification of Cyber-Physical Systems. In *20th International Conference in Product-Focused Software Process Improvement*, pages 626–632.

Eclipse-Foundation (2018). *Eclipse Process Framework (EPF) Composer – EPF 1.5.2 Release*.

Elgammal, A., Turetken, O., van den Heuvel, W., and Papazoglou, M. (2016). Formalizing and applying compliance patterns for business process compliance. *Software and Systems Modeling.*, pages 119–146.

Gallina, B. (2019). Quantitative evaluation of tailoring within spice-compliant security-informed safety-oriented process lines. *Journal of Software: Evolution and Process*, e2212(e2212):1–13.

Gallina, B., Kashiyarandi, S., Martin, H., and Bramberger, R. (2014). Modeling a Safety- and Automotive-Oriented Process Line to Enable Reuse and Flexible Process Derivation. In *38th International Computer Software and Applications Conference*, pages 504–509.

Gallina, B., Pulla, A., Bregu, A., and Castellanos Ardila, J. (2020). Process Compliance Re-Certification Efficiency Enabled by EPF-C ∘ BVR-T : a Case Study. In *13th International Conference on the Quality of Information and Communications Technology*, pages 1–8.

Gallina, B., Sljivo, I., and Jaradat, O. (2012). Towards a Safety-oriented Process Line for Enabling Reuse in Safety Critical Systems Development and Certification. In *35th Annual IEEE Software Engineering Workshop*, pages 148–157.

Görlach, K., Kopp, O., Leymann, F., and Schumm, D. (2011). WS-BPEL extension for compliance fragments (BPEL4CFrags). Technical report, Institute of Architecture of Application Systems, University of Stuttgart.

Governatori, G. (2005). Representing Business Contracts in RuleML. *International Journal of Cooperative Information Systems.*, pages 181–216.

Governatori, G. (2015). The Regorous Approach to Process Compliance. In *19th International Enterprise Distributed Object Computing Workshop*, pages 33–40.

ISO (2000). *ISO 14971:2000 – Application of risk management to medical devices*.

ISO (2007). *ISO 14971:2007 – Application of risk management to medical devices*.

ISO (2012). *EN ISO 14971:2012 – Application of risk management to medical devices (ISO 14971:2007, Corrected version 2007-10-01)*.

ISO (2019). *ISO 14971:2019 – Application of risk management to medical devices*.

Javed, M. and Gallina, B. (2018a). Get EPF Composer back to the future: a trip from Galileo to Photon after 11 years. In *EclipseCon*.

Javed, M. and Gallina, B. (2018b). Safety-oriented Process Line Engineering via Seamless Integration between EPF Composer and BVR Tool. In *22nd International Systems and Software Product Line Conference*, pages 23–28.

Kabir, M., Xing, Z., Chandrasekaran, P., and Lin, S. (2017). Process Patterns: Reusable Design Artifacts for Business Process Models. *International Computer Software and Applications Conference*, 1:714–721.

Ma, Z. (2012). *Process fragments: enhancing reuse of process logic in BPEL process models*. Ph.d. dissertation, University of Stuttgart.

Martin, H., Krammer, M., Bramberger, R., and Armengaud, E. (2016). Process-and product-based lines of argument for automotive safety cases. In *7th International Conference on Cyber-Physical Systems*.

Ocampo, A. and Münch, J. (2009). Rationale Modeling for Software Process Evolution Alexis. *Software Process: Improvement and Practice*, 14(2):85–105.

OMG (2008). Software & Systems Process Engineering Meta-Model Specification. Version 2.0.

Pulla, A. and Bregu, A. (2020). Master Thesis: Evaluating the Compliance Re-Certification Efficiency Enabled by the AMASS Platform for Medical Devices, Mälardalen University, School of Innovation, Design and Engineering, Västerås, Sweden.

Schleicher, D., Grohe, S., Leymann, F., Schneider, P., Schumm, D., and Wolf, T. (2011). An approach to combine data-related and control-flow-related compliance rules. In *International Conference on Service-Oriented Computing and Applications*, pages 1–8.

SINTEF (2016). BVR Tool, https://github.com/SINTEF-9012/bvr.

Teixeira, E. N., Aleixo, F. A., de Sousa Amâncio, F. D., OliveiraJr, E., Kulesza, U., and Werner, C. (2019). Software process line as an approach to support software process reuse: A systematic literature review. *Information and Software Technology*, 116:106175.