Assurance Case Exchange Standard (ACES): Supplementary Material

Tássio Fernandes Costa[*], Álvaro Sobrinho[†], Lenardo Chaves e Silva[‡], Leandro Dias da Silva[§] and Angelo Perkusich[¶]

September 2020

1 Introduction

1.1 Overview

Assurance Case Exchange Standard (ACES) is a marking document standard used to represent assurance cases defined with the Goal Structuring Notation (GSN) [1]. Concepts related to requirements traceability are also taken into account when defining the standard. An ACES warranty case must have the following main characteristics:

- an ACES assurance case is maintained by a manufacturer of a product under development;
- an ACES assurance case shall be authenticated by a manufacturer;
- the authentication of an ACES assurance case applies to isolated parts of the document (modules);
- an ACES assurance case shall be coded using the Extensible Markup Language (XML); and
- versions of requirements defined in ACES assurance cases shall be controlled.

[*]Federal University of Alagoas
[†]Federal University of the Agreste of Pernambuco
[‡]Federal Rural University of the Semiarid
[§]Federal University of Alagoas
[¶]Federal University of Campina Grande

1.2 Scope

The scope of ACES regards to the representation of assurance cases defined using modular GSN. ACES also aims to assist manufacturers and regulatory agencies to exchange assurance cases for certification. The standard also considers concepts related to the traceability of requirements of the product under development and the possibility of verifying compliance with regulatory requirements.

2 Description of Elements

The start and end of an ACES document is the `<assuranceCase>` tag. To enable the version control, each ACES document has a general identification named `generalId`, along with the version identification (`versionId`) and local identification (`localId`). The `generalId` attribute of the `<assuranceCase>` tag is a unique identifier for all the versions of the ACES document, while the `versionId` and `localId` have different identifiers for each new version to represent the modifications in the document. The beginning of the document also contains specific data about the product under development by means of the `<device>` tag. It includes the manufacturer's social name (`<manufacturerLegalName>`), manufacturer's fantasy name (`<manufacturerFantasyName>`), manufacturer's address (`<manufactuerAddress>`), manufacturer's phone number (`<manufacturerPhone>`), manufacturer's email (`<manufacturerEmail>`), manufacturer's unique identifier (`<manufacturerUniqueIdentifier>`), device name (`<deviceName>`), and device description (`<deviceDescription>`). Fig. 1 presents a sample of ACES document considering the `<assuranceCase>` and `<device>` tags.

```
<?xml version="1.0" encoding="UTF-8"?>
<assuranceCase generalId="0001" versionId="A01" localId="1000">
        <device>
                <manufacturerLegalName> Insulin Infusion Pump Manufacturer </manufacturerLegalName>
                <manufacturerFantasyName> IIP Manufacturer </manufacturerFantasyName>
                <manufactuerAddress> Av. Lourival Melo Mota, s/n - Tabuleiro do Martins, Maceió - PE,  57072-900 </manufactuerAddress>
                <manufacturerPhone> +55-82-3214-1100 </manufacturerPhone>
                <manufacturerEmail> tfc@ic.ufal.br </manufacturerEmail>
                <manufacturerUniqueIdentifier> IIP01 </manufacturerUniqueIdentifier>
                <deviceName> Insulin Infusion Pump System </deviceName>
                <deviceDescription>  Device used to treat patients with diabetes. </deviceDescription>
        </device>

```

Figure 1: Sample of ACES document considering the `<assuranceCase>` and `<device>` tags.

Considering that assurance cases contain a set of related arguments about quality attributes of a system, ACES represents them using the `<parentArgument>` and `<childArgument>` tags. The `<parentArgument>` tag composes the body of the `<assuranceCase>` tag, placed after the `<device>` tag. The `<parentArgument>` represents the main structure of the assurance case in modular GSN, while the `<childArgument>` tag represents structures that are parts of the body of the `<parentArgument>` tag. In this case, an ACES document only contains one

<parentArgument> that may consist of multiple assurance case modules: child arguments relates to specific GSN modules. Each ACES argument contains the <legalAuthenticator> tag, aiming to record the author of modifications in the ACES document. The <legalAuthenticator> tag is also composed of the <time>, <organization>, and <author> tags (Fig. 2).

```
51 <legalAuthenticator>
52         <time value="25200000" />
53         <author>Mr. Sobrinho</author>
54         <organization> UFAPE </organization>
55 </legalAuthenticator>
```

Figure 2: Sample of ACES document considering the <legalAuthenticator> tag.

The ACES includes the main GSN elements: Goal, Solution, Strategy, Context, Assumption, Justification, SupportedBy, and InContextOf. In addition, it includes the modular GSN elements: Away Goal, Module, Contract, Away Solution, Away Context, and Public Indicator. ACES structures these elements in its body using the <group> tag. This element has the attribute named type, that constrains it to group GSN elements of the same type. For instance, to represent a Goal, it is necessary to define an ACES tag to represent a specific goal in the body of the <group> tag. Each <group> tag related to a type of ACES tag is only defined once in the body of each <parentArgument> and <childArgument> tags.

The <goal> tag represents a GSN Goal element (Fig. 3). All the GSN elements (except relationships) contain, at least, an attribute named id and a child tag named <description>. The <goal> tag can also contain the optional attributes named public, undeveloped, and toBeSupportedByContract. Therefore, goals represent assurance case claims, supported by a set of sub-claims. In ACES, goals can also represent requirements, when the attribute named requirement is set to true (the default value of this attribute is false). Fig. 4 illustrates a sample of ACES document considering the <childArgument>, <group>, and <goal> tags. It enables manufacturers to document quality requirements using ACES. Manufacturers can document product artifacts related to these requirements using GSN solutions. For each goal of a GSN module, a CPN module (XML specification) or a temporal logic formula can be embedded in the ACES document (<formalDefinition> tag) to maintain the formal description of the requirements. The <formalDefinition> tag (Fig. 5) may contain the required and provided tags (interfaces) to enable the specification of module composition. In addition, the <formalDefinition> tag can contain the <shared> tag to allow specification of resource sharing between modules.

The <solution> tag (Fig. 7) defines an ACES solution (Fig. 6), containing the additional attribute named public. Manufacturers use solutions to represent evidence that supports claims. The attribute named artifact, when set as true, associates the solution with a product artifact. A tag named externalArtifactUrl connects a solution to a specific evidence. Defining solutions as product artifacts

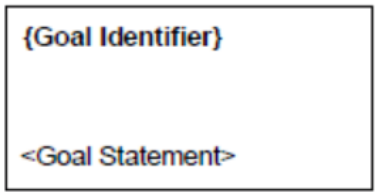

Figure 3: Example of goal GSN element.

```
68          <childArgument moduleId="SYSTEM-M1">
69                  <group type="goal">
70                          <goal id="ISO14971-G1">
71                                  <description> Risk Management in conformance with ISO </description>
72                                  <relationships>
73                                          <relationIncontextOf id="r8" type="context" relId="ISO14971-C1" />
74                                          <relationIncontextOf id="r9" type="context" relId="ISO14971-C2" />
75                                          <relationSupportedBy id="r10" type="strategy" relId="ISO14971-S2" />
76                                  </relationships>
77                          </goal>
78                          <goal id="ISO14971-M5">
79                                  <description> Production and Post-Production in Conformance with Section 8 of ISO </description>
80                          </goal>
81                  </group>
```

Figure 4: Sample of ACES document considering the `<childArgument>`, `<group>`, and `<goal>` tags.

are relevant to enable the requirements traceability.

For reasoning about connections among claims (possibly requirements), manufacturers use `Strategies` (Fig. 8). The `<strategy>` tag represents a strategy that contains an additional optional attribute named `undeveloped`. Fig. 9 illustrates a sample of ACES document considering the `<strategy>` tag. The `<relationship>` is discussed later in this document.

Another important characteristic of the requirements engineering considered using ACES is the source of requirements. For assurance cases, the GSN `Context` element (Fig. 10) provides information about specific claims, represented in ACES using the `<context>` tag (with the additional attribute named `public`). Fig. 11 illustrates a sample of ACES document considering the `<group>` and `<context>` tags. In ACES, GSN `Context` elements define the source of requirements, setting the attribute named `source` to `true`. When this attribute is `true`, a new tag named `<externalSourceUrl>` associates the source with the location of the declared source. Defining contexts as requirements source is also relevant to perform the requirements traceability using ACES.

It may also be necessary to improve confidence in the validity of claims and strategies using the GSN `Assumption` element (Fig. 12), defined by the ACES `<assumption>` tag. Additionally, manufacturers may provide justifications about the definition of claims and strategies. Therefore, the ACES `<justification>` tag represents a GSN `Justification` element (Fig. 13). In the ACES-based requirements engineering, the `<justification>` tag enables manufacturers to justify changes in requirements. The justifications add information in the obso-

```
496 <goal id="PRODUCT-G12" requirements="true">
497         <description> Administration standard mode </description>
498         <informalDefinition> Correct Output Administration Standard Mode </informalDefinition>
499         <formalDefinition>
500                 <cpnet>
501                         <globbox>
502                                 <block id="ID1412310166">
503                                         <id>Standard priorities</id>
504                                         <ml id="ID1412310255">
505                                                 val P_HIGH = 100;
506                                                 <layout>val P_HIGH = 100;</layout>
507                                         </ml>
```

Figure 5: Sample of ACES document considering the `<formalDefinition>` tags.

Figure 6: Example of solution GSN element.

```
354 <group type="solution">
355         <solution id="ISO14971-E13">
356                 <description> Literature and Data Analyses </description>
357         </solution>
358 </group>
```

Figure 7: Sample of ACES document considering the `<group>` and `<solution>` tags.

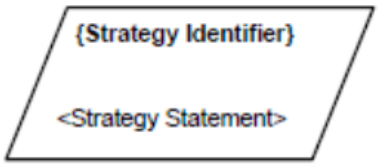

Figure 8: Example of strategy GSN element.

lete version of the requirement defined in the ACES document (version control), i.e., a justification is attached to the `<goal>` tag used to represent the obsolete requirement. The usage of the `<assumption>` and `<justification>` tags is similar

```
14869 <strategy id="PRODUCT-S4">
14870         <description> Verification of General Properties </description>
14871         <relationship>
14872                 <relationSupportedBy id="r91" type="goal" relId="PRODUCT-G8" />
14873         </relationship>
14874 </strategy>
```

Figure 9: Sample of ACES document considering the `<strategy>` tag.

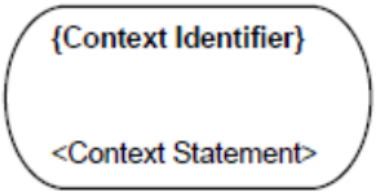

Figure 10: Example of context GSN element.

```
26 <group type="context">
27         <context id="SYSTEM-C1">
28                 <description> Software Components </description>
29         </context>
30         <context id="SYSTEM-C2">
31                 <description> Hardware Components </description>
32         </context>
33 </group>
```

Figure 11: Sample of ACES document considering the `<group>` and `<context>` tags.

to the context element (Fig. 11).

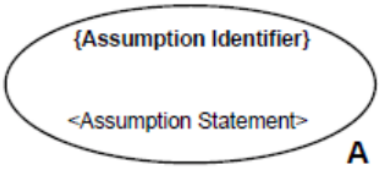

Figure 12: Example of assumption GSN element.

The ACES represents connections between elements using the `<relationships>` tag. The declaration is optional, but when it occurs, it should contain at least one child tag. The `<relationSupportedBy>` tag is a binding notation used to indicate relationships between requirements and project artifacts (evidence),

Figure 13: Example of justification GSN element.

requiring the attributes `id`, `type`, and `relID`. The `relID` attribute is the identifier that relates GSN elements, respecting the rules defined in the GSN standard. There is also a binding notation used to indicate contextual relationships using the `<relationInContextOf>` element, and also contains attributes named `id`, `type`, and `relID`. The `<relationSupportedBy>` and `<relationInContextOf>` elements (Fig. 14) are part of the body of the `<relationships>` tag. Fig. 15 illustrates the graphic representation of these relationship elements.

```
<goal id="SYSTEM-G1">
        <description> System is Safe and Effective </description>
        <relationships>
                <relationIncontextOf id="r1" type="context" relId="SYSTEM-C1" />
                <relationIncontextOf id="r2" type="context" relId="SYSTEM-C2" />
                <relationSupportedBy id="r3" type="strategy" relId="SYSTEM-S1" />
                <relationSupportedBy id="r4" type="strategy" relId="SYSTEM-S2" />
        </relationships>
</goal>
```

Figure 14: Sample of ACES document considering the `<relationship>` tag.

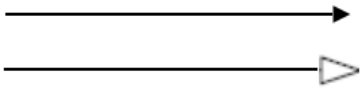

Figure 15: SupportedBy and InContextOf GSN elements.

For modular GSN, the `<awayGoal>` tag defines an `Away Goal` element (Fig. 16), containing the additional attribute named `goalId`. An away goal enables manufacturers to reuse a claim presented in another assurance case module. In the definition of the `<awayGoal>` tag (Fig. 17), we use the `id` of a goal of a specific module to identify a claim. To represent the reference to a module (set of claims), ACES provides the `<module>` tag.

The standard also enables one to display a reference to a contract module containing the relationships previously defined between two modules (GSN `Contract`). The `<contract>` tag defines the contract, and contains the additional attribute named `idContractModule`. Manufacturers define a contract module

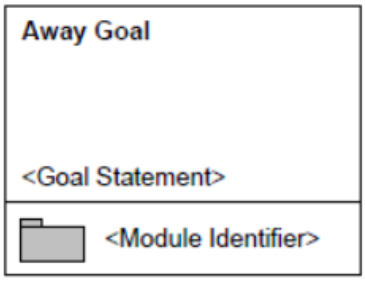

Figure 16: Example of Away Goal GSN element.

```
<awayGoal id="Away Goal" goalId="G2">
  <description> Goal Statemente </description>
</awayGoal>
```

Figure 17: Sample of ACES document considering the `<awayGoal>` tag.

using the `<module>` tag (Fig. 18), related to the contract module through the attribute `idContractModule`. Fig. 19 illustrates an example of module GSN element. It is also possible to relate a contract with a goal defined in a module, setting the attribute `toBeSupportedByContract` as `true`, to indicate that the contract will be defined later.

```
<module id="module">
   <description> Module Description </description>
</module>
```

Figure 18: Sample of ACES document considering the `<module>` tag.

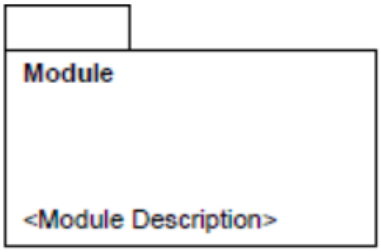

Figure 19: Example of the module GSN element.

In addition, a contract module reference (Contract) is defined using the `<contract>` element (Fig. 20). This element shall contain the attributes named

`id` and `idContractModule`. A description shall be written in the body of this element. A contract module reference is used to present a reference to a contract module that contains the relationships between two modules. A contract module shall be defined using the `<module>` element which must be related to a contract module reference by the `idContractModule` attribute. According to the GSN standard, a contract module reference is represented by the graphical notification shown in Fig. 21.

```
5  <contract id="Contract" idContractModule="Module">
6    <description> Contract Description </description>
7  </contract>
```

Figure 20: Sample of ACES document considering the `<contract>` tag.

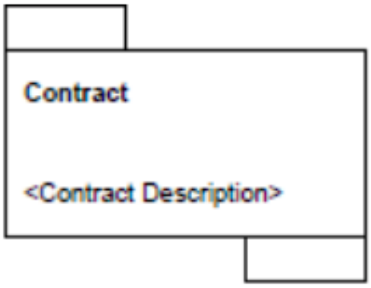

Figure 21: Example of the contract GSN element.

A contract can be related to a goal defined in a module using an element that indicates that the contract will be defined later (i.e. `To be supported by contract`). In this case, the `toBeSupportedByContract` attribute shall be defined in a `<goal>` element as true. According to the GSN standard, an element that indicates that a contract will be defined later shall be placed below the element using it to represent a goal, and is represented by the graphical notation shown in Fig. 22.

An away solution enables manufacturers to reuse a reference to evidence of another module. The `<awaySolution>` represents a GSN `Away Solution` element (Fig. 23), containing the additional attribute named `solutionId`. The identifier of a solution of a specific module is used to reference a piece of evidence. Fig. 24 presents a sample of the ACES document considering the `<awaySolution>` tag. The same approach is available for contexts, enabling the reuse of a reference to the context of another module.

The `<awayContext>` defines a GSN `Away Context` element (Fig. 25), containing an additional attribute named `contextId`. The identifier of a context of a specific module is also used to reference a contextualization. Fig. 26 presents a sample of the ACES document considering the `<awayContext>` tag.

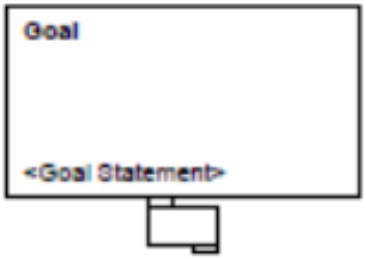

Figure 22: Example of the to be supported by contract GSN element.

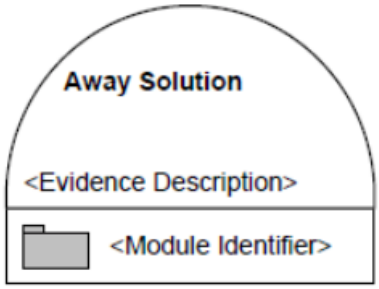

Figure 23: Example of the away solution GSN element.

```
<awaySolution id="Away Solution" solutionId="S2">
  <description> Evidence Description </description>
</awaySolution>
```

Figure 24: Sample of ACES document considering the `<awaySolution>` tag.

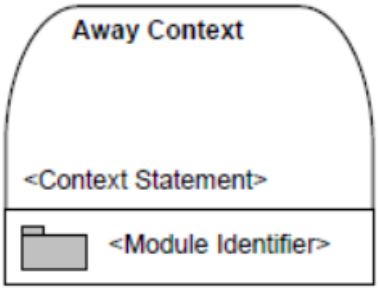

Figure 25: Example of the away context GSN element.

It is possible to use the elements `Away Goal`, `Away Solution`, and `Away Context` to reference `Goal`, `Solution`, and `Context` elements. ACES provides the attribute named `public` to apply the GSN `Public Indicator` element (Fig. 27 and Fig. 28)

```
13  <awayContext id="Away Context" contextId="C2">
14    <description> Context Statement </description>
15  </awayCOntext>
```

Figure 26: Sample of ACES document considering the `<awayContext>` tag.

for the tags `<goal>`, `<solution>`, and `<context>`. Fig. 29 illustrates a sample of ACES document considering the `<goal>` tag and `Public` attribute.

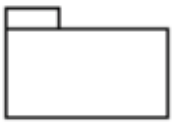

Figure 27: Public indicator GSN element.

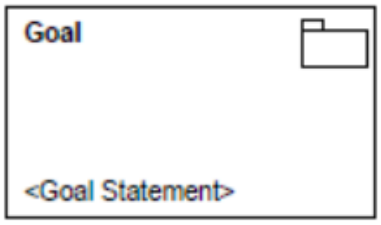

Figure 28: Example of the public indicator GSN element.

```
17  <goal id="Goal Identifier" public="true">
18    <description> Goal Statement </description>
19  </goal>
```

Figure 29: Sample of ACES document considering the `<goal>` tag and `Public` attribute.

For quality assessment, regulatory agencies can include evaluation results in the ACES document under analysis by the tags `<accepted>` and `<rejected>`. The evaluation of ACES documents relates to individual arguments. The body of the tag `<rejected>` contains a description of the rejection. Manufacturers and regulatory agencies can exchange documents until a final decision about the system's certification under evaluation. For example, the regulatory agency may ask for specific evidence before the approval of the system.

References

[1] The Assurance Case Working Group. Goal Structuring Notation Community Standard (Version 2). 2018.