DRAFT

full paper published in:

**Risk, Reliability and Societal Safety, Volume 2:
Thematic Topics, ed. Terje Aven, Jan Erik Vinnem,
Taylor and Francis, London 2007, pp. 1367-1374**

**Proceedings of the European Safety and Reliability
Conference 2007 (ESREL 2007), 25-27 June 2007,
Stavanger, Norway**

Paper published in the journal and presented at the conference

Supporting compliance with safety standards by trust case templates

Ł. Cyra & J. Górski

Technical University of Gdańsk, Narutowicza 11/12, 80-952 Gdańsk, Poland

ABSTRACT: *Standard Compliance (SC) Framework* presented in this paper encompasses methods and tools which provide support for application of standards. The framework is based on *trust case* methodology. A trust case is a data structure which represents a justification that an object (a system, an infrastructure, an organization) exhibits certain properties. It contains an argument and related evidence which support claimed properties. A trust case which argues the compliance with a standard is built, according to the framework, on the basis of a *trust case template*. Such a template is derived from the standard and is represented in a reusable format. The article describes SC Framework in more detail and presents a case study of its application. The case study demonstrates an example trust case template derived from *Medical devices - Application of risk management to medical devices* (ISO 14971:2000) standard. Some details of the web-based software tool supporting the presented approach are also given.

1 INTRODUCTION

Many organizations and companies are interested in being compliant with certain standards and/or regulations. Certificates of compliance can strengthen organization position and competitiveness and in some business contexts can be even obligatory. However, the compliance is often difficult to demonstrate and can involve significant costs. Standards can include myriads of interrelated requirements which need interpretation. Fulfilling the requirements necessitates documentation of very often surprising bulk. Enough evidence must be produced, gathered and then presented in a legible manner. The whole argumentation and the supporting documentation must be presented in a way to convince auditors or other assessors that all the requirements have been adequately addressed. And if the present assessment is successful, the whole burden has to be continuously maintained and updated as the compliance needs usually to be reassessed on a regular basis.

The article presents a systematic approach to application of standards. It supports the process of standard interpretation and achieving, demonstrating, assessing and maintaining the compliance. The approach is implemented in the *Standard Compliance Framework*. The framework is based on *trust case* methodology, which has been originally developed for assurance cases of critical systems (Górski et al. 2005, Górski 2005a, b). In this paper we describe how trust cases can be adopted to demonstrate the compliance with standards. First we present SC Framework itself and then we demonstrate how it can be applied to define a *trust case template* for ISO 14971:2000 standard. Such a template serves as a generic assurance case for the standard. Finally, we give some more details on the tool support for developing trust cases and in particular trust case templates.

2 STANDARD COMPLIANCE FRAMEWORK

Standard Compliance (SC) Framework supports demonstration of compliance with standards. It is composed of (1) the language to create templates, (2) the processes of creating templates, (3) the process of applying templates (at different stages of standard application), and (4) *TCT tool* which supports development and application of templates.

The objective of SC Framework is to support development and maintenance of a document which justifies the claim of compliance. Such a document is called *standard compliance case*. The framework functional architecture distinguishes three main areas of support (see Fig. 1):

– *Teamwork and Progress Measurement* area represents support for the issues related to standard compliance project execution and management. This area is supported by the TCT tool (presented in the next sections), which facilitates collaborative development of standard compliance cases. Standard compliance project planning and progress monitoring can be performed using information included in a template. Templates contain lists of items of work to be performed to achieve and demonstrate the compliance.

– *Presentation and Views* area represents support for project outcome communication. Deriving standard compliance cases from a template provides for uniformity of documents demonstrating compliance with the same standard, and (to less extent) uniformity of documents demonstrating compliance with different standards. Templates and standard compliance cases are expressed in the same (graphic) language which structures arguments and the supporting evidence in a similar way.

– *Achieving Compliance and Creating a Compliance Case* area represents support for the issues related to creating appropriate argument structures, indicating the necessary supporting evidence and collecting the evidence. In particular, this support encompasses identification of standard requirement interdependencies, checklists of the evidence documents which should be collected, interpretation of the requirements and the provisions for immediate feedback on the gathered evidence quality.

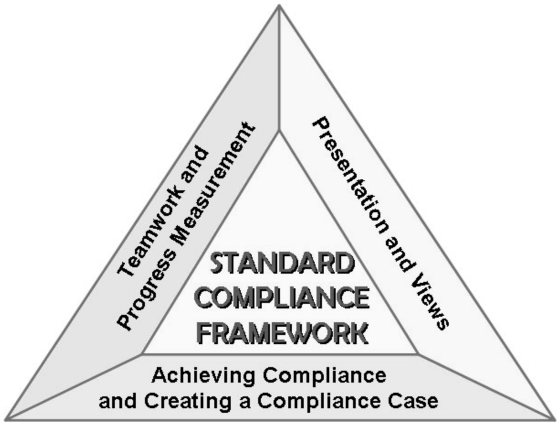

Teamwork and Progress Measurement
Presentation and Views
STANDARD COMPLIANCE FRAMEWORK
Achieving Compliance and Creating a Compliance Case

Figure 1. Standard Compliance Framework.

3 TRUST CASE

The approach to trust cases was described in (Górski et al. 2005, Górski 2005a, b). This approach is being developed at Gdansk University of Technology by Information Assurance Group (see http://iag.pg.gda.pl).

Trust case is a data structure which encompasses argument and related evidence, which together demonstrate that an object (a system, an infrastructure, an organization) exhibits certain precisely defined properties. Trust case documents are presented in a graphic form, which significantly boosts legibility and helps to maintain soundness of arguments. Trust cases have a tree-like structure. Every piece of information in the tree is represented by a node of appropriate type (for instance, *claim*, *fact*, *assumption*, *argument*, *information*). The structure of the argument, which can be recursively applied to build the whole trust case, is presented in Figure 2. The model of the argument is similar to Toulmin model of argument (Toulmin 1969) which was also followed in the models used in Goal Structuring Notation (Kelly & Weaver 2004) and Claims-Arguments-Evidence notation (Bishop & Bloomfield 1998).

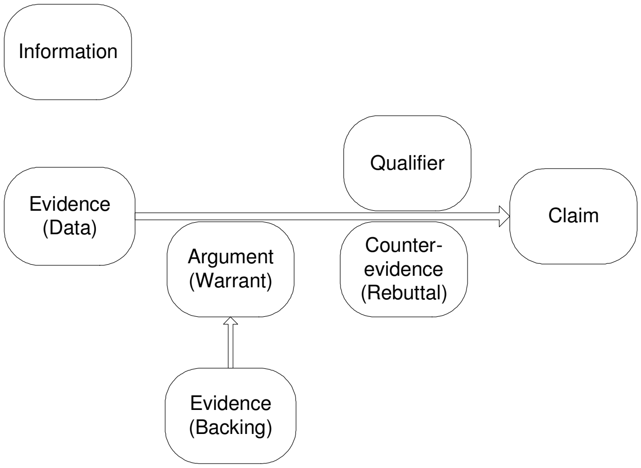


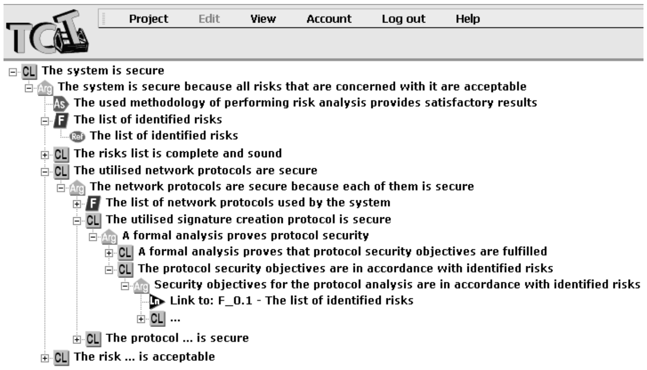
Figure 2. Model of the argument.

An instantiation of this model is depicted in Figure 3. It presents a tree (developing from left to right) where the subsequent layers of the tree are distinguished by indentation. The whole tree claims security of a system and provides its justification (to some level of detail).

Statements which postulate some properties and need appropriate arguments and supporting evidence are represented by nodes called *claims* (denoted CL). Every trust case tree has a claim in its root node. This claim postulates the main property to be justified. Every claim in a trust case is supported by an *argument* (denoted Arg). The argument justifies why the claim is true. Arguments can refer to *facts* (denoted F), assumptions (denoted AS) and (more specific) *claims*.

In the example in Figure 3, the main claim about security is justified by showing that all the risks concerned are acceptable. The argument is supported by other nodes which provide evidence. These include: the fact which contains the list of the risks identified during risk analysis, the assumption which states that the methodology used for risk analysis was adequate, the claim that the list of risks is complete, the claim that the risks are acceptable and the claim about security of system network connections.

Assumptions in a trust case contain information which is deemed to be true. They contain statements which are significant when credibility of the claimed properties of an examined object is considered, however, information which is not explicitly stated in documentation of the examined object.



```
⊟ CL The system is secure
  ⊟ Arg The system is secure because all risks that are concerned with it are acceptable
      As The used methodology of performing risk analysis provides satisfactory results
    ⊟ F The list of identified risks
        Ref The list of identified risks
    ⊞ CL The risks list is complete and sound
    ⊟ CL The utilised network protocols are secure
      ⊟ Arg The network protocols are secure because each of them is secure
        ⊞ F The list of network protocols used by the system
        ⊟ CL The utilised signature creation protocol is secure
          ⊟ Arg A formal analysis proves protocol security
            ⊞ CL A formal analysis proves that protocol security objectives are fulfilled
            ⊟ CL The protocol security objectives are in accordance with identified risks
              ⊟ Arg Security objectives for the protocol analysis are in accordance with identified risks
                  Ln Link to: F_0.1 - The list of identified risks
                ⊞ CL ...
        ⊞ CL The protocol ... is secure
    ⊞ CL The risk ... is acceptable
```

Figure 3. Example of a trust case.

Facts contain information which is demonstrated to be true by providing additional evidential material. Such material can contain information about the object, information about its environment, results of analyses and so on. Facts usually are linked with external documents by using *references* (denoted Ref).

In addition, *links* (denoted Ln) are used to provide for avoiding redundancies in a trust case. In Figure 3 a link is used to refer to the fact: *The list of the identified risks*.

Finally, *information* nodes (not shown in Figure 3) can contain additional explanations which help in understanding the trust case contents.

4 TRUST CASE TEMPLATES

A *trust case template* is composed of a generic argument structure (called the *template argument structure - TAS*) complemented with additional information which helps in converting this structure into a concrete trust case.

TAS can be interpreted as a data structure or as a document. When interpreted as a data structure it consists of arguments and evidence. The evidence is linked to the warrants of arguments and supports the validity of the arguments. Consequently, TAS is a template of *valid* arguments. The evidence referred to from the arguments is not included. Instead, the template identifies the places of TAS where such evidence should be included. Therefore, despite the fact that a valid argument for the topmost claim is provided, the question of the soundness of this argument is still open and depends on the ‘quality’ of the evidence to be provided.

When TAS is interpreted as a document it can be treated as a document structure definition indicating ‘gaps’ where the document content is to be included.

While applying the concept of trust case templates to standards, a TAS included in a trust case template represents argumentation scheme for claiming compliance with the standard. It includes information about the requirements of the standard, identifies the evidential material to be supplied to support the compliance and also historic information from assessment projects (if available). The template is constructed from a standard by applying the *template derivation procedure* which is a detailed description of the steps to be performed to create a template from other documents (Cyra & Górski 2006a, b). The requirements of the standard are represented as claims and facts of the template argument structure. The claims and facts postulate that certain requirements or sets of requirements are fulfilled. The claims are supported by arguments or remain *unsupported*. In the latter case a claim represents a ‘gap’ in the template, which must be filled in later with more specific evidence (available only during the process of achieving compliance with the standard). Similarly, unsupported facts are those which are not yet linked with the external evidential material (by the referencing mechanism). The nodes of the template are organized into an appropriate argument structure which is derived from the standard. Justifying the claims included in this structure is equivalent with demonstrating the compliance with the standard. Depending on the number of requirements included in the standard, the corresponding template may become a large data structure, consisting of hundreds of nodes.

A general model of a template is presented in Figure 4. It distinguishes three main layers:

– The top layer contains template metadata, including references to standard documents, standard description, lists of links to unsupported claims and facts in the template argument structure, lists of documents necessitated by the standard, and views. The layer contains general information which supports template utilisation as the whole.
– The middle layer which is depicted as two triangles, contains the template argument structures. A template can contain more then one such structure, each of which demonstrates different properties of the examined object (e.g. one demonstrates the compliance with the standard while the other demonstrates that assessment was performed in accordance with the criteria contained in the standard).
– The bottom layer of the template contains (in the form of information nodes) additional information which provides guidance on proving fulfilment of particular requirements of the standard. Except the detailed description and references to other documents, which can be useful while applying the template, the information nodes can contain examples of evidential structures taken from other assessment projects. Interdependencies among standard requirements are also identified and stated there.

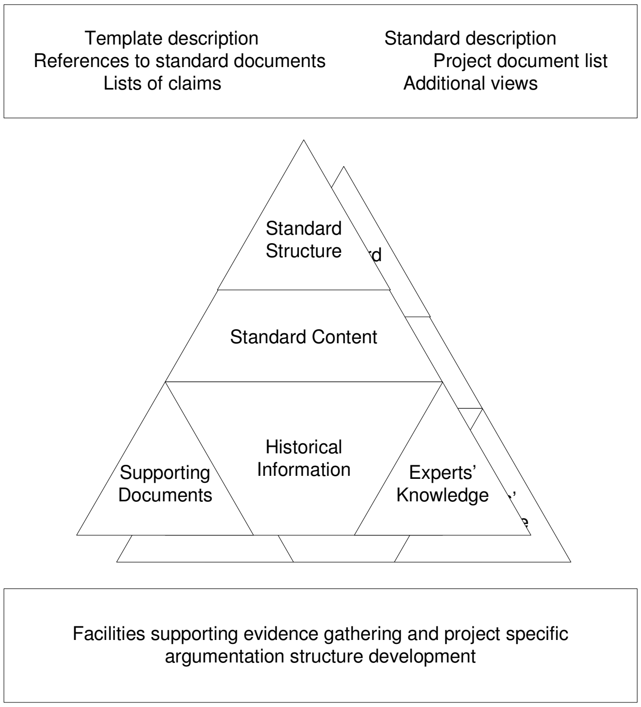


Figure 4. Trust case template structure.

As shown in Figure 4, TAS (included in the middle layer of the template) can be divided into three additional layers. The top layer is derived from the standard structure. The middle layer is derived from the standard content. The bottom layer contains arguments which are created using extra-standard information. Such arguments can be derived from documents which support the standard or can be proposed by experts who take into account the experiences from previous applications of the standard.

5 SUPPORT FOR APPLICATION OF STANDARDS

Proposed SC Framework distinguishes four different processes for application of standards. The processes map into the activities of the trust case template lifecycle, which are depicted in Figure 5 (represented as rounded rectangles).

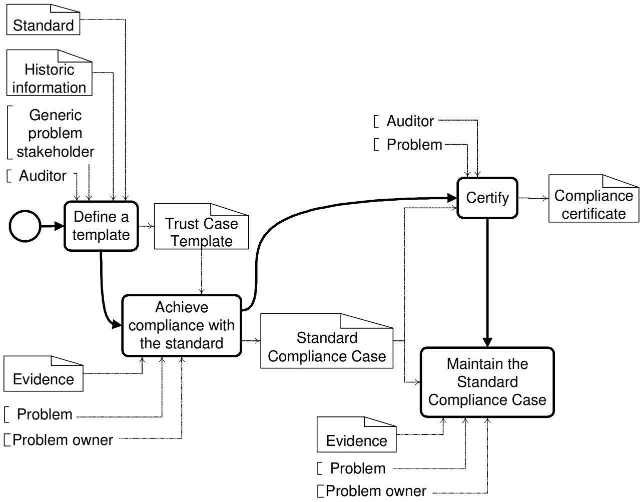


Figure 5. Trust case template lifecycle.

The first process refers to deriving *the definition of a template* from a given standard. This process is of particular importance as the quality of its result (the template) conditions the quality of the results of other processes. The template definition process includes a corrective feedback to provide for a continuing template improvement (see Figure 6).

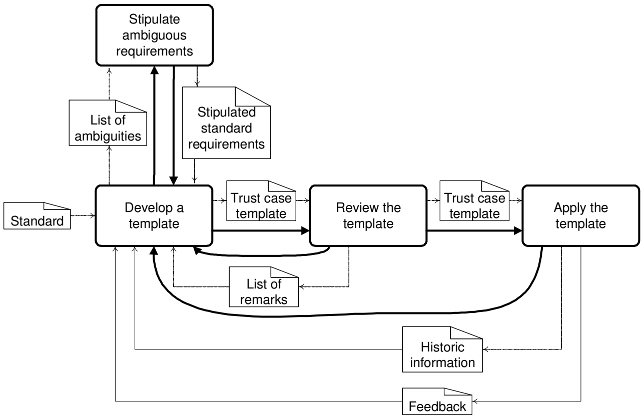


Figure 6. Defining a template.

A trust case template can be used as means of reconciling assessment criteria. Although, in general the assessment criteria can (and should) be derived from a standard, in most cases it is not that straightforward. Often, the requirements of the standard have to be interpreted to identify the compliance criteria. Creating templates forces early requirements interpretation which can have positive impact on the compliance achieving process. In particular, any ambiguities and controversies identified at this stage can be solved with the help of prospective auditors. The template structure can be also discussed and agreed with the auditors, which reduces the risk of the assessment failure. Additionally, a template can be enriched by attaching to it information about its previous applications (if such information is available). This way the template can serve as a mechanism for good practice promotion and for developing model solutions of compliance demonstration.

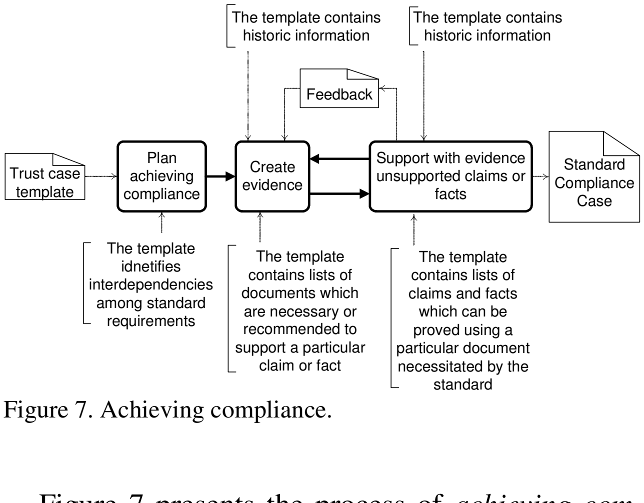

The template contains historic information
The template contains historic information
Feedback
Trust case template
Plan achieving compliance
Create evidence
Support with evidence unsupported claims or facts
Standard Compliance Case
The template idnetifies interdependencies among standard requirements
The template contains lists of documents which are necessary or recommended to support a particular claim or fact
The template contains lists of claims and facts which can be proved using a particular document necessitated by the standard

Figure 7. Achieving compliance.

Figure 7 presents the process of *achieving compliance*. The process starts with planning which can benefit from the fact that a template identifies interdependencies among standard requirements. These logical dependencies are then reflected in the schedule of actions necessary to achieve the compliance. In addition, the template contains lists of documents which must be created (and possibly examples of such documents) and shows how those documents support (if they are created) unsupported claims and facts in the template argument structure. This helps in better understanding the role of the documents and the evidential material they contain in the context of compliance supporting argumentation. Examples of argument structures, which are included in the template can ease the process and promote good practices. Finally, the template can help in monitoring the progress of the compliance achieving process by providing the base for various metrics. An example of such a metric can be the (normalized) number of still unsupported claims and facts in the template. The output of this process is a standard compliance case which follows the argument structure included in the template and includes all the necessary evidence supporting this argumentation (no claims and facts are left ‘unsupported’).

The third process is that of *compliance assessment*. Its internal structure is shown in Figure 8. A standard compliance case is given to (external) auditors for assessment. The auditors’ role is to verify the soundness of the compliance argumentation and in particular to assess the value of the supporting evidence. This process ends with the creation of appropriate reports.

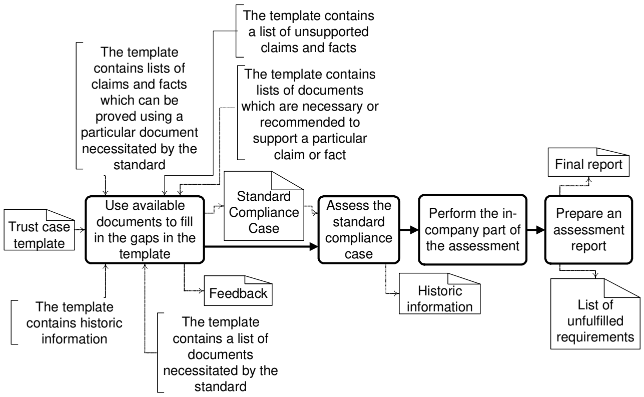

The template contains a list of unsupported claims and facts
The template contains lists of claims and facts which can be proved using a particular document necessitated by the standard
The template contains lists of documents which are necessary or recommended to support a particular claim or fact
Final report
Trust case template
Use available documents to fill in the gaps in the template
Standard Compliance Case
Assess the standard compliance case
Perform the in-company part of the assessment
Prepare an assessment report
Feedback
Historic information
List of unfulfilled requirements
The template contains historic information
The template contains a list of documents necessitated by the standard

Figure 8. Compliance assessment.

The last process is related to *maintaining the compliance*. It has been added in recognition of the fact that maintaining the compliance needs a continuous effort and periodic reassessment. This maintenance can be supported by the traceability information which is explicitly represented in the compliance case. This information is identified in the process of template definition and reflects the interdependencies among the requirements included in the standard. During maintenance, it can be used to identify the scope of change induced by a particular change of the evidence supporting a given requirement. The maintaining compliance process is depicted in Figure 9.

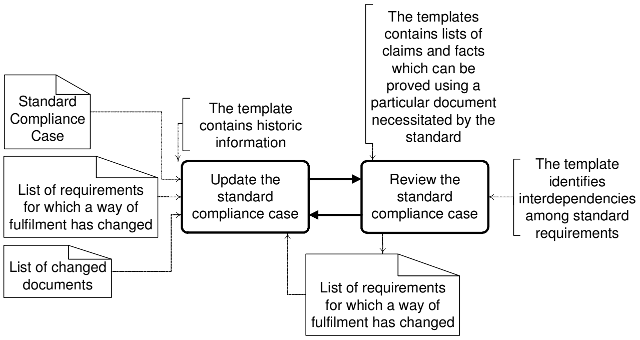
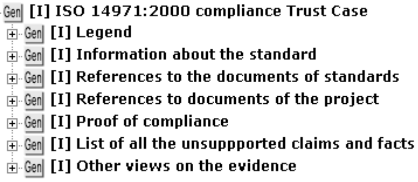

Standard Compliance Case
List of requirements for which a way of fulfilment has changed
List of changed documents
The template contains historic information
Update the standard compliance case
The templates contains lists of claims and facts which can be proved using a particular document necessitated by the standard
Review the standard compliance case
The template identifies interdependencies among standard requirements
List of requirements for which a way of fulfilment has changed

Figure 9. Maintaining compliance.

6 TC TEMPLATE FOR ISO 14971:2000

Applicability of the idea of using trust case templates to support compliance achieving and assessment has been validated in several case studies (Cyra & Górski 2006a, b). In this section we give more details on the case study of developing a template for the ISO 14971:2000 (ISO 2000).

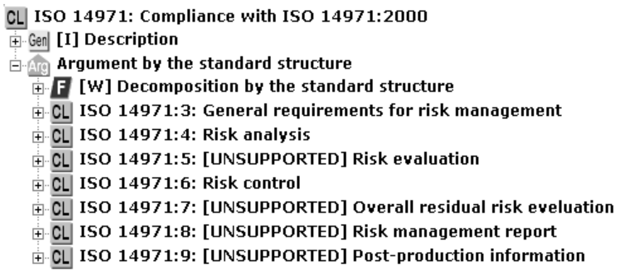
ISO 14971:2000 *Medical devices - Application of risk management to medical devices* is related to effective management by the manufacturer of the risks associated with the use of medical devices. It is a widely recognized international standard for risk management which contents are mostly generic and applicable to broader contexts than just medical devices.



Gen [I] ISO 14971:2000 compliance Trust Case
- Gen [I] Legend
- Gen [I] Information about the standard
- Gen [I] References to the documents of standards
- Gen [I] References to documents of the project
- Gen [I] Proof of compliance
- Gen [I] List of all the unsuppported claims and facts
- Gen [I] Other views on the evidence

Figure 10. TC template for ISO 14971:2000.

The main structure of the template for ISO 14971:2000 is shown in Figure 10. It is composed of seven parts, each playing a different role. The first two parts (*Legend* and *Information about the standard*) contain introductory information. The third (*References to the documents of the standard*) contains documents of the standard linked to the template by references to external files. The forth part (*References to documents of the project*) is a place where all the documents which are required to prove the compliance with the standard are detailed. Each of them is further associated with a list of unsupported nodes (claims and/or facts) which are to be supported by the evidence included in the document (this is not shown in Figure 10). Those lists provide for traceability from the documents to the nodes supported by those documents. The fifth part (*Proof of compliance*) contains the template argument structure and the seventh part *(Other views on the evidence*) contains a different view on it. Both parts are described in detail below. The sixth part (*List of all unsupported claims and facts*) includes a list of all unsupported nodes in order to provide for easy monitoring of the progress in the compliance case development (the number of yet unsupported nodes indicates how far we are from having a complete compliance case).



CL ISO 14971: Compliance with ISO 14971:2000
- Gen [I] Description
- Arg Argument by the standard structure
  - F [W] Decomposition by the standard structure
  - CL ISO 14971:3: General requirements for risk management
  - CL ISO 14971:4: Risk analysis
  - CL ISO 14971:5: [UNSUPPORTED] Risk evaluation
  - CL ISO 14971:6: Risk control
  - CL ISO 14971:7: [UNSUPPORTED] Overall residual risk eveluation
  - CL ISO 14971:8: [UNSUPPORTED] Risk management report
  - CL ISO 14971:9: [UNSUPPORTED] Post-production information

Figure 11. Template argument structure derived from the standard structure.

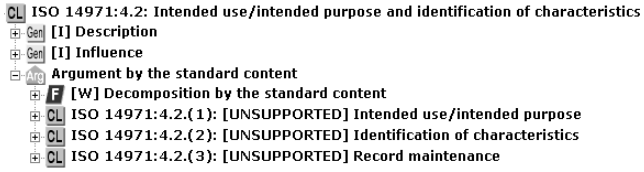
Figure 11 depicts the first level of the template argument structure (the contents of the *Proof of Compliance* branch from Figure 10). It contains the claim postulating the compliance with the standard and the supporting argument referring to the structure of the standard.

The argument which supports the topmost claim refers to seven sub-claims, each of which postulates that the requirements of the corresponding standard chapter are fulfilled.

Additionally, the argument is also supported by a fact: *Decomposition by the standard structure*. This fact describes the *warrant* of the argument, which is the inference rule used by it, which in this case assumes the equivalence between the requirements represented by the topmost claim and its sub-claims.

The sub-claims of Figure 11 can be further decomposed in an analogous way. Consequently, the resulting argument tree follows the structure of the requirements presented in the standard.

The initial structure of the template argument structure built according to the scheme described above was developed further using the standard content. One of the arguments created on this basis is shown in Figure 12.

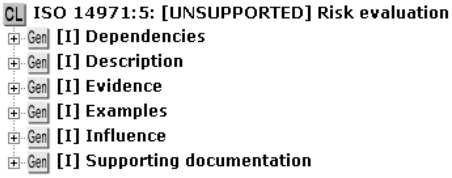


CL ISO 14971:4.2: Intended use/intended purpose and identification of characteristics
- Gen [I] Description
- Gen [I] Influence
- Arg Argument by the standard content
  - F [W] Decomposition by the standard content
  - CL ISO 14971:4.2.(1): [UNSUPPORTED] Intended use/intended purpose
  - CL ISO 14971:4.2.(2): [UNSUPPORTED] Identification of characteristics
  - CL ISO 14971:4.2.(3): [UNSUPPORTED] Record maintenance

Figure 12. Template argument structure derived from the standard content.

The presented argument was created using information from chapter 4.2 of the standard. It is supported here by a set of claims and a warrant (the fact: *Decomposition by the standard content*). In this case the decomposition of the argument is not driven by the standard structure (as in Figure 11), which has been signified by the fact title.

The bottom of the template argument structure includes unsupported claims and facts (see Figures 11 and 12). They represent gaps to be filled during the process of compliance demonstration by providing project specific evidence. Every such gap is associated with additional information which helps in identifying/producing such evidential material. An example referring to the *Risk analysis* claim from Figure 11 is shown in Figure 13.



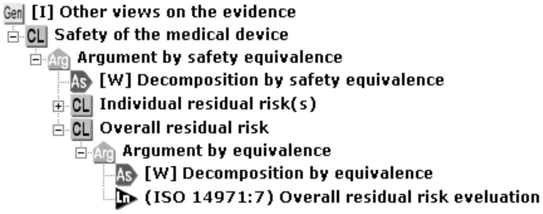
CL ISO 14971:5: [UNSUPPORTED] Risk evaluation
- Gen [I] Dependencies
- Gen [I] Description
- Gen [I] Evidence
- Gen [I] Examples
- Gen [I] Influence
- Gen [I] Supporting documentation

Figure 13. Additional information in unsupported nodes.

The claim in Figure 13 postulates that all the requirements from chapter 5 'Risk evaluation' of ISO 14971 are fulfilled. It is left unsupported in the template. To help in finding adequate support for this claim the template contains the following nodes:

– *Dependencies* – contains a list of other unsupported claims, which should be demonstrated before the present one.
– *Description* – contains a reference to the excerpt of the standard with a detailed description of the requirements represented by the claim.
– *Evidence* – contains a list of references to documents from the *References to documents of the project* part of the template (see Figure 10) which should be considered while seeking for the support for the claim.
– *Examples* – contains examples of arguments for the claim from historic projects.
– *Influence* – contains a list of other claims which, if demonstrated, should be reviewed when the way in which this claim is fulfilled changes.
– *Supporting documents* – contains a list of documents which can turn out to be useful in proving fulfilment of the claim.

The seventh part of the template (*Other views on evidence*, see Figure 10) structures the evidence gathered in TAS and demonstrates that a medical device is safe as the result of compliance with the standard. Excerpt from this view is shown in Figure 14.



Gen [I] Other views on the evidence
- CL Safety of the medical device
  - Arg Argument by safety equivalence
    - As [W] Decomposition by safety equivalence
    - CL Individual residual risk(s)
    - CL Overall residual risk
      - Arg Argument by equivalence
        - As [W] Decomposition by equivalence
        - Ln (ISO 14971:7) Overall residual risk eveluation

Figure 14. An example view.

The main claim (*Safety of the medical device*) is argued to be true if the two sub-claims (*Individual residual risk(s)* and *Overall residual risk*) which state that individual and overall residual risks are acceptable are true. Both of these claims are decomposed further. Figure 14 shows the argument for the *Overall residual risk* claim. Its warrant is included in the assumption *Decomposition by equivalence*. The argument is supported by the evidence pointed to by the link *Overall residual risk evaluation* (kept in a separate part of the template). If and when TAS is complemented with this evidence, the presented view, which argues safety of a medical device, becomes complete and sound.

7 TOOL SUPPORT

Trust case management, and in particular trust case template management is supported by *TCT Editor*, a tool developed and maintained at the Gdansk University of Technology. It serves as a platform for development, dissemination and maintenance of trust cases. The system is Web-based and can be accessed by using one of two currently supported browsers: Internet Explorer 5.5 or 6.x or Firefox 1.5. *TCT Editor* provides support to all types of actors involved in trust case development and use. It defines three roles: *Viewer*, *Editor* and *Manager*. Its functionality includes trust case browsing, exporting/importing trust cases to/from XML files, developing argument structures and managing user accounts.

The model of use cases for *TCT Editor* is given in Figure 15.

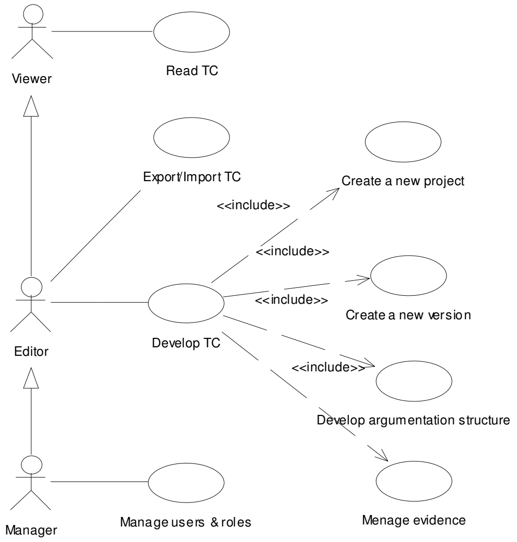
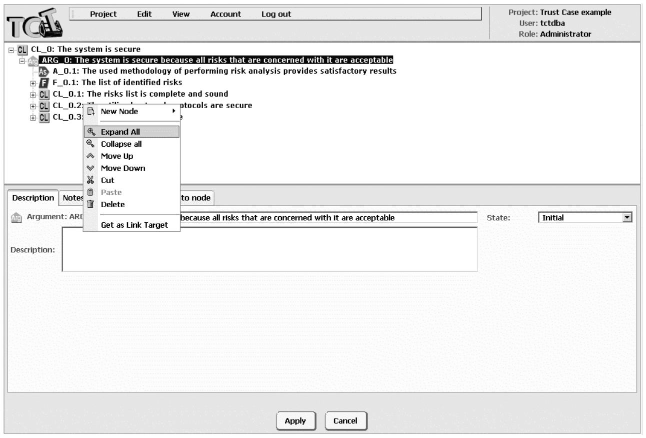


Figure 15. Use Cases of the TCT Editor.

An example screenshot showing the look and feel of *TCT Editor* interface is presented in Figure 16.



Project: Trust Case example
User: tctdba
Role: Administrator

CL_0: The system is secure
ARG_0: The system is secure because all risks that are concerned with it are acceptable
A_0.1: The used methodology of performing risk analysis provides satisfactory results
F_0.1: The list of identified risks
CL_0.1: The risks list is complete and sound
CL_0.2: otocols are secure
CL_0.3: e

Argument: ARG because all risks that are concerned with it are acceptable
State: Initial
Description:

Figure 16. TCT Editor user interface.

8 CONCLUSIONS

In the paper we presented the *Standard Compliance Framework* and its example application to the common standard on risk management for medical devices, ISO 14971:2000. We also provided some details on the present status of the tool supporting the framework.

The objective of the SC Framework is to support processes of achieving and assessing the compliance. The framework provides for representing the requirements of a standard in a form of a trust case template which includes a ‘schematic’ representation of the argumentation to be used to justify the compliance. Graphic presentation of the template increases legibility and usability. Organizing the template into a tree-like structure helps in structuring the argumentation into abstraction layers. The same template can be re-used in many concrete situations related to the application of a given standard. An additional benefit is that different compliance cases resulting from the application of a common template will have similar structure of arguments and will differ only in the evidence supporting the argumentation.

The tool supporting the framework provides for an effective management of the bulk of documentation which is usually required by standards. The ‘gaps’ in the pre-defined structure can be easily filled with evidence using mechanisms of the lists of unsupported claims and facts, the lists of claims and facts which can be justified by referring to specified documents, or the lists of documents recommended to be consulted while justifying compliance with certain requirements.

The Framework is able to accumulate knowledge from previous projects by storing examples of arguments and making them available to a user.

In addition, a template can provide extra argument structures, (which we call *views*), which argue some properties as a result of the compliance (for instance, such a view can demonstrate safety of a medical device as a result of being compliant with ISO 14971). Such views can be directly imported to safety cases.

Present experience with trust case templates includes experiments with ISO 14971:2000, BS 7799, and Common Criteria. The template for BS 7799 was applied in pre-assessment of a real system developed by an international institution. The project encompassed assessment of a part of the organization in which the system operated according to a defined security policy and procedures.

Trust case templates are also going to be applied in some new projects. Presently they are planned to be used in EU 6th FR Integrated Project PIPS (Personalized Information Platform for health and life Services) and in EU 6th STREP ANGEL (Advanced Networked embedded platform as a Gateway to Enhance quality of Life).

Other examples of trust case templates and more information about the subject can be found in (Cyra & Górski 2006a, b).

9 ACKNOWLEDGEMENT

This work has been partially supported by the EU 6th Framework projects PIPS (Contract N^o IST-507019) and ANGEL (Contract N^o IST-033506).

REFERENCES

Bishop, P. & Bloomfield, R. 1998. A methodology for safety case development. *Safety-critical systems symposium, Birmingham 1998.*

Cyra, Ł. & Górski, J. 2006a. Trust Case template support for working with Common Criteria standard. (in Polish) *Zeszyty Naukowe Wydziału ETI Politechniki Gdańskiej:* 615-622.

Cyra, Ł. & Górski, J. 2006b. Using Trust Case templates to facilitate BS 7799 utilisation. (in Polish) *ENIGMA 2006:* 305-319.

Górski, J. et al. 2005. Trust case: justifying trust in IT solution. *Reliability Engineering and System Safety, Volume 89, Elsevier*: 33-47.

Górski, J. 2005a. Trust Case – a case for trustworthiness of IT infrastructures. In Kowalik, J. & Gorski, J. & Sachenko, A. (Eds.), *Cyberspace Security and Defense: Research Issues, NATO ARW Series*: 125-142, Springer-Verlag.

Górski, J. 2005b. Collaborative approach to trustworthiness of infrastructures. *Proceedings of IEEE International Conference of Technologies for Homeland Security and Safety. TEHOSS 2005*: 137-142.

Kelly, T. & Weaver R. 2004. The goal structuring notation – a safety argument notation. *DSN 2004.*

Toulmin, S. 1969. *The Uses of Argument.* Cambridge: Cambridge University Press.

ISO, 2000. *ISO 14971:2000 Medical devices – Application of risk management to medical devices.* ISO.