This is a postprint of the paper presented at the 32nd International Conference on Computer Safety, Reliability and Security SAFECOMP 2013, September 24-27 2013, Toulouse and published by Springer: http://link.springer.com/chapter/10.1007%2F978-3-642-40793-2_2

Comparative conformance cases for monitoring multiple implementations of critical requirements

Janusz Górski[1,2], Aleksander Jarzębowicz[1,2], Jakub Miler[1,2]

[1]Department of Software Engineering, Gdansk University of Technology, Poland
[2]NOR-STA Project, Gdansk University of Technology, Poland, www.nor-sta.eu
{jango, olek, jakubm}@eti.pg.gda.pl

Abstract. The paper presents the concept and the mechanism of comparative conformance cases which support conformance monitoring in situations where a standard or other set of requirements are being implemented at multiple sites. The mechanism is enabled by NOR-STA services which implement the TRUST-IT methodology and are deployed in the cloud in accordance with the SaaS model. In the paper we introduce the concept of comparative conformance cases, explain the software services used to implement them and present a case study of monitoring the implementation of the EC Regulation No. 994/2010, related to risk management of gas supply infrastructures across Europe.

Keywords: conformance case, conformance monitoring, critical infrastructures protection, trust cases, NOR-STA services

1 Introduction

Regulations and standards are among the important mechanisms through which the European program of risk governance for the ICT and energy sectors is being implemented [1]. To make these mechanisms effective, it is important not only to promote implementation of standards and regulations but also to assess the actually achieved level of conformance and to continuously monitor the conformance across the different critical infrastructure stakeholders.

In this paper we introduce *comparative conformance case* – a mechanism that supports conformance monitoring in situations where a standard, directive or other set of requirements are implemented at multiple sites. Hereafter, we will call the source of conformance requirements a 'standard'. If used by the party in charge of supervising implementation of a standard, the mechanism provides means to review the evidence supporting conformance and to review and assess the related conformance cases against a selected assessment scale.

Comparative conformance case is based on the concept of a *trust case* [2, 3] which extends the concept of *safety case* [4] commonly used in the safety-critical domain to justify safety properties of various systems, for instance avionic, nuclear, automotive, medical, military and so on [5, 6]. The concept of safety case has been extended (under the name *assurance case*) to cover any critical property to be assured, like safety,

security, reliability and others [7]. Under the name of *trust case* it has been further generalized and refers to the situations where the focus is on a selected feature to be demonstrated, not necessarily being 'critical'.

We are particularly interested in situations where a common argumentation structure is shared by numerous concrete cases. As an example take a standard and the question of conformance demonstration. Then, the structure of the conformance case may be common for multiple implementations of the standard and the difference between particular implementations is mostly in the evidence supporting the argument. This observation led to the concept of the *conformance case template* which can have multiple instantiations where each instance, after attaching the relevant evidence, becomes a complete *conformance case* [8, 9]. The concept of comparative conformance case builds upon these notions.

In the paper we outline the TRUST-IT methodology of developing and assessing trust cases and the related NOR-STA platform which supports this methodology by offering a set of software services in the computing cloud. Next, we introduce the mechanism of comparative conformance cases and the related scenario of its application. Then, we present a case study demonstrating implementation of this scenario with the objective of supporting monitoring the conformance to the European Commission Regulation No. 994/2010 related to risk management of gas supply infrastructures in different EU Member States.

2 TRUST-IT methodology and NOR-STA services

TRUST-IT [2, 3, 8] is an approach to promoting trust by developing, maintaining and presenting on-line arguments demonstrating trustworthiness. An argument can be published, edited and assessed, and it is visualized in a graphical form together with the result of the assessment of its 'compelling power'. Evidence integrated with an argument is kept in digital documents of any form: text, graphics, image, web page, video, audio and so on. The evidence supports what an argument postulates about the state of the world. In TRUST-IT terminology, such postulates are called 'facts'. Depending on the support given by the evidence to the corresponding facts, the argument is more or less convincing. TRUST-IT introduces a model of an argument (following [10]), a graphical language for expressing arguments, and a technique for integrating arguments with evidence (see Fig. 1). The arrows linking the nodes shown in Fig. 1 represent the can-be-child-of relationship in the argument tree. The abstract argument model of TRUST-IT is similar to GSN [11] and CAE [12], the differences are more on a technical and representation levels.

Argument conclusion is represented by a *claim* node. A node of type *argumentation strategy* links the *claim* with the corresponding premises and uses a *rationale* to explain and justify the inference leading from the premises to the claim. A premise is a sort of assertion and can be of the following type: an *assumption* represented by an assertion assumed to be true which is not further justified; a *claim* represented by an assertion to be further justified by its own premises; and a *fact* represented by an assertion to be demonstrated by the supporting evidence. The evidence is integrated by

MOST WIEDZY Downloaded from mostwiedzy.pl

nodes of type *reference* which point to external resources (files of any type, web pages, etc.). In addition, *information* nodes (denoted) can be used in any place to provide explanatory information. This model can generate trees of arbitrary depth where the root of the tree is the top-most claim and the leaves are references pointing to the evidence supporting facts, assumptions and/or rationales of selected argumentation strategies (in our experience we are dealing with arguments of up to several thousand nodes).

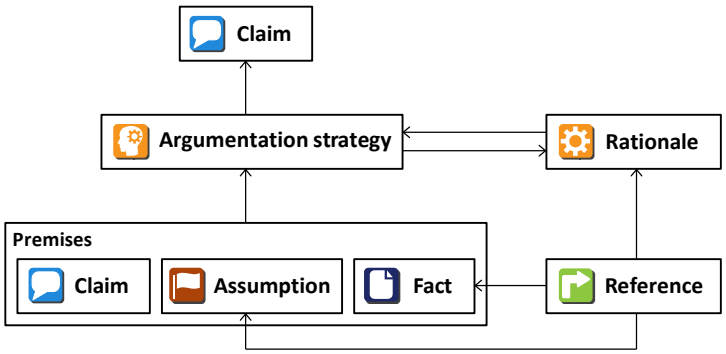

Fig. 1. The TRUST-IT model of argument

By analyzing the inferences and checking the evidence supporting facts, an auditor can work out his/her opinion about how strong the argument is towards the conclusion, and where its weaknesses and strengths are. TRUST-IT supports this activity in different ways. The most advanced is the argument appraisal mechanism based on Dempster-Shafer theory of evidence [13] and the corresponding mechanism of visualization of the argument compelling power [14]. Here, the auditor can express his/her appraisals referring to so called *opinion triangle* shown in Fig. 2.

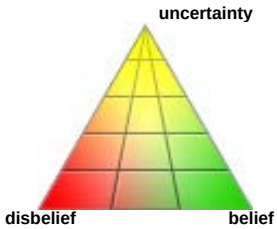

Fig. 2. The opinion triangle for issuing argument appraisals based on Dempster-Shafer theory

By choosing a position within the triangle, the auditor, after examining the evidence supporting a fact, decides to which extent he/she accepts/rejects the fact and what is the level of uncertainty associated with this opinion. Similar appraisals can be issued with respect to the inferences used in the argument, represented by the related nodes of *rationale* type. The aggregation rules (see [14] for the details) provide for automat-

MOST WIEDZY Downloaded from mostwiedzy.pl

ic appraisal of all claims of the argument (including the top-most one), provided the appraisals of all facts, assumptions and rationales have already been issued.

In addition to the above, TRUST-IT provides for other, user-defined argument appraisal mechanisms (involving different assessment scales and aggregation rules). These mechanisms can be activated according to the users' needs. For instance, in one of our case studies of arguments related to standards conformance the stakeholders decided that a simple three-state scale {non-compliant, partially-compliant, compliant} was in use.

TRUST-IT arguments have already been (among others) developed to: analyze safety, privacy and security of personalized health and lifestyle oriented services [15], monitor the environmental risks [16] and support standards conformance for health, business and administration sectors [17].

Application of TRUST-IT is supported by the NOR-STA platform of software services. The services are deployed in accordance with the SaaS (Software as a Service) cloud computing model. The scope of functionalities of NOR-STA services includes: argument representation and editing using the graphical symbols shown in Fig. 1, integration (through references) of various types of evidence, argument assessment and visualization of the assessment results, publishing of an argument, and evidence hosting in protected repositories.

3 Comparative conformance case

TRUST-IT approach is generic and can be applied in any context where evidence based argumentation brings added value to decision making processes and disputes. One such application area is standards conformance where a standard's user is expected to construct and present an argument demonstrating conformance. While applied to standards conformance, TRUST-IT introduces additional, more specific concepts [8, 9]. *Conformance case template* is an argumentation structure derived from a standard. This structure is common for all conformance cases related to the standard. It explicitly identifies placeholders for the supporting evidence and may indicate places where more specific, implementation dependent argumentation is to be provided. Template development involves domain experts representing the standard's owner and standard's auditor viewpoints. *Conformance case* is a complete argument which is developed from the template providing the required evidence and possibly by appending a more specific argumentation. *Conformance assessment* is an act of assigning appraisals to the conformance argument components to assess their 'compelling power'.

The relationship between the conformance case template and a conformance case following the structure of the template is shown in Fig.3. Filled rectangles denote nodes already included in the template, the hollow rectangles denote nodes added as more specific argumentation and the ovals represent the evidence supporting the conformance case. The concept of case template is similar to argument schemes/patterns [5, 6] used in safety cases (a template suggests how to demonstrate conformance to entire set of standard's requirements whereas a pattern suggests how to demonstrate a

MOST WIEDZY Downloaded from mostwiedzy.pl

single, specific type of claim). However, the conformance case template is far richer than just providing an argumentation scheme. In addition it includes the source documentation of the related standard, examples of good practices in structuring the evidence, single evidence placeholders referenced in multiple requirements, explicit interdependencies between standard fragments and many others.

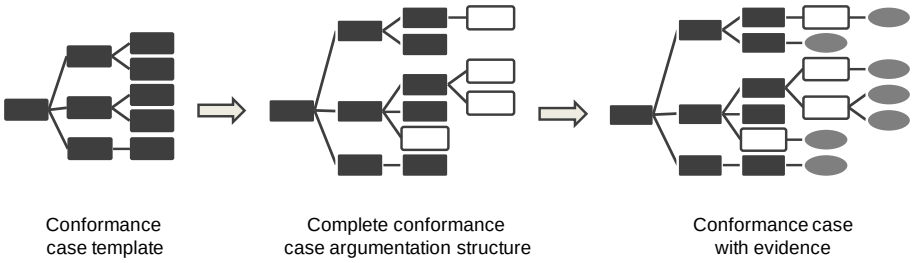

Fig. 3 The conformance case template – conformance case relationship.

Let us assume that a given conformance case template is being used by a number of users, and each of them has developed her/his own conformance case based on the template. Then, each of the cases can be reviewed in the node-by-node manner, for instance, by accessing the facts and verifying the evidence supporting each fact.

Now, let us assume that in addition to the users developing their own conformance cases, there is a separate body, call it *supervisor*, who is in charge of monitoring all the cases and possibly assessing how strongly the claims and facts listed in the conformance case template are supported in different cases.

The concept of *comparative conformance case* embodies the idea that having a conformance case template in an explicit form, one can point to a selected node of the template and in response will have access to the structure demonstrating how this node is represented in each conformance case derived from the template. For instance, by pointing to a given fact included in the template, the supervisor will be able to review, compare and assess the evidence submitted to demonstrate this fact in different conformance cases. And by pointing to a claim the supervisor will see the assessment results of this claim, for different conformance cases.

Implementing the concept of comparative conformance case would result in an interface with the following functionality:

- selecting the conformance cases to be compared;
- selecting a fact (claim) of the conformance case template which results in obtaining access to the evidence supporting this node in different conformance cases and to the appraisals of how strong this support is;
- accessing and browsing the evidence;
- issuing/changing appraisals of the support given by the evidence.

The above idea is illustrated in Fig. 4. The arrows shown in the picture point to a selected node of the conformance case template and to the corresponding nodes of the supervised conformance cases.

MOST WIEDZY Downloaded from mostwiedzy.pl

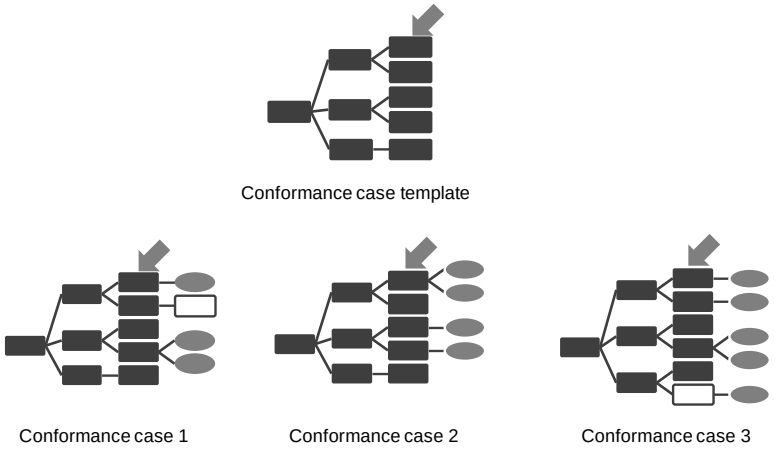

Fig. 4 Illustration of the comparative case concept

The concept of comparative conformance case brings added value in situations where monitoring the implementation of multiple conformance cases is of particular business relevance. In such situation, the supervising body can simply activate a comparative conformance case and by choosing different claims and facts can get immediate insight into the evidence supporting the chosen criterion across selected cases. In some cases it can also facilitate appraisals, especially if they are issued in relative terms.

The present scope of functionality of NOR-STA services covers: conformance case template management, conformance case management, management of evidence repositories, argument appraisal and appraisal comparison management.

4 Case study: monitoring implementation of EC Regulation 994

The functionality of comparative conformance cases has been built into NOR-STA services to provide support for the monitoring scenario outlined in the previous section. In this section we present this scenario applied to monitoring the implementation of the European Commission Regulation No. 994/2010 [18].

4.1 The Regulation

The Regulation 994/2010 refers to risk management of gas infrastructures in the EU Member States. Below are some citations from this document.

> *Natural gas is an essential component in the energy supply of the European Union, constituting one quarter of primary energy supply and contributing mainly to electricity generation, heating, feedstock for industry and fuel for transportation. [...] Given the importance of gas in the energy mix of the Union, the Regulation aims at demonstrating to gas cus-*

MOST WIEDZY Downloaded from mostwiedzy.pl

tomers that all the necessary measures are being taken to ensure their continuous supply, particularly in case of difficult climatic conditions and in the event of disruption. [...]

This Regulation establishes provisions aimed at safeguarding the security of gas supply by ensuring the proper and continuous functioning of the internal market in natural gas, by allowing for exceptional measures to be implemented when the market can no longer deliver the required gas supplies and by providing for a clear definition and attribution of responsibilities among natural gas undertakings, the Member States and the Union regarding both preventive action and the reaction to concrete disruptions of supply. This Regulation also provides transparent mechanisms, in a spirit of solidarity, for the coordination of planning for, and response to, an emergency at Member State, regional and Union levels.

The Regulation imposes several obligations on Member States as well as on EU administration. The obligations for Member States include: conducting a thorough Risk Assessment the results of which should be summarized in an adequate report, and establishing Preventive Action Plan and Emergency Plan to be presented to the European Commission. The responsibility of the Commission is to instantiate an effective mechanism of monitoring how the regulation is being implemented.

4.2 Comparative conformance case for Regulation 994/2010

The scenario of implementing the comparative conformance case for Regulation No. 994/2010 (hereafter called Regulation) involves the following steps (the Users are in Member States and the Supervisor acts on behalf of the EU Commission):

Step 1 - development of the conformance case template by the Supervisor;
Step 2 - submitting the conformance case template to the Users;
Step 3 - development of conformance cases by the Users;
Step 4 - monitoring of conformance cases by the Supervisor.

Below we illustrate how this scenario is implemented with NOR-STA services. To demonstrate the implementation of Step 1 we have developed the conformance case template deriving it from the text of the Regulation. Fig. 5 presents an overview of the template (the hierarchy of nodes develops from the left to the right) In Fig. 5, the fact labeled F1.1.4 is linked to two references labeled December 2011: Information about intergovernmental agreements and December 2011: Risk Assessment Report. These references point to the places where two different pieces of evidence are to be integrated, demonstrating that the party implementing the Regulation has already prepared a risk assessment report and that the necessary intergovernmental agreements are in place to reduce risk related to gas supply.

Implementation of Step 2 is demonstrated by creating, for each user of Regulation, a separate space where it can develop its own conformance case. In NOR-STA terminology, such space is called ‘project’. Each such project is initially filled with the conformance case template. In the following text we assume that three such projects have been created for three different conformance cases of ‘dummy’ countries A, B and C.

MOST WIEDZY Downloaded from mostwiedzy.pl

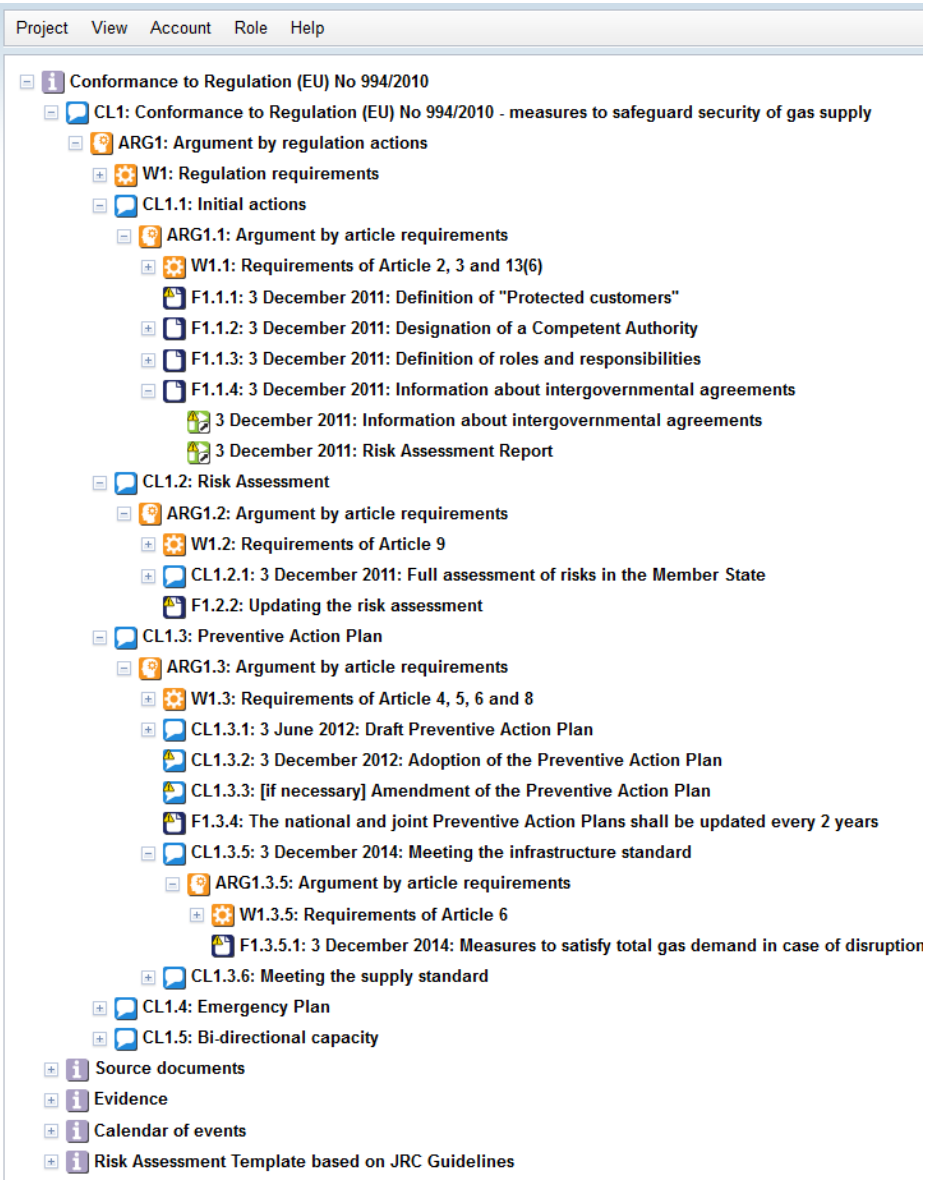

Fig. 5. Top-level decomposition of the Regulation conformance case template

Implementation of Step 3 is demonstrated by developing a separate conformance case, for each country. In Fig. 6 we can see the conformance case of Country A, where some pieces of evidence has been already integrated. In the figure, the reference December 2011: Risk Assessment Report has been selected which resulted in opening the window with the referred evidence – the document of the risk assessment

MOST WIEDZY Downloaded from mostwiedzy.pl

report. The remaining users (Country B and Country C) could have integrated their specific evidence in their own conformance cases in a similar way.

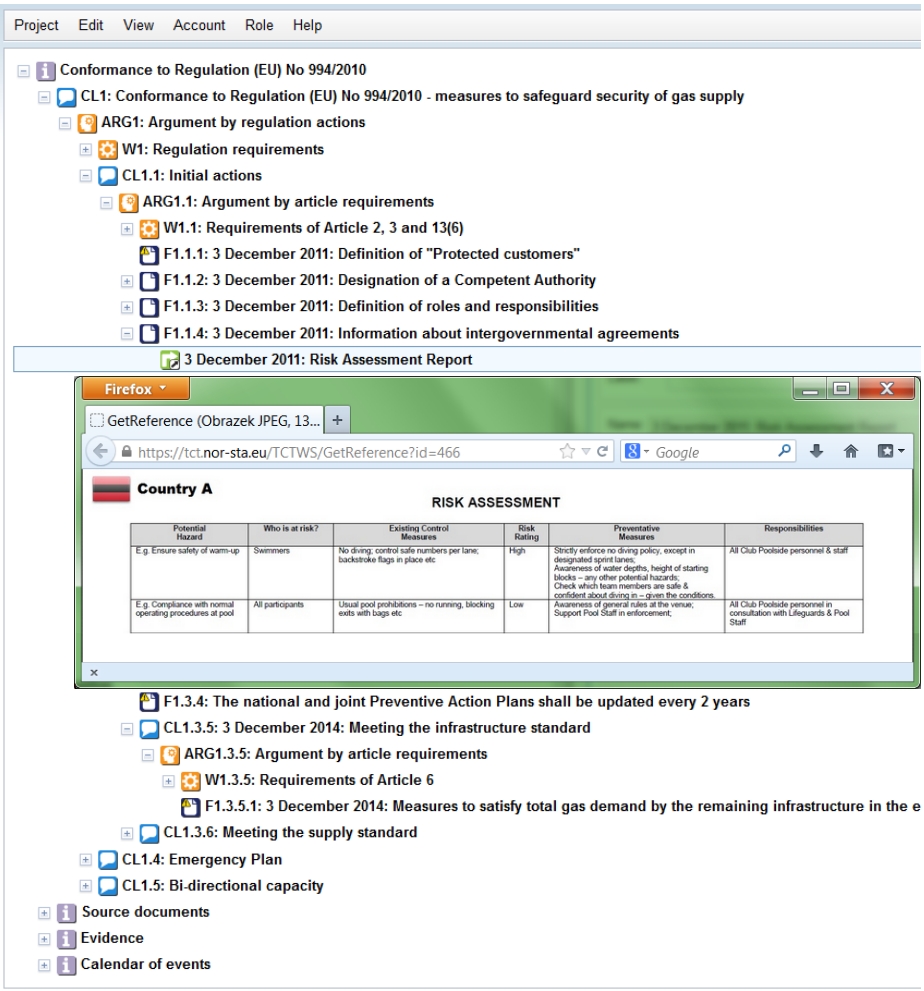

Fig. 6. An example evidence linked to fact F1.1.4

Implementation of Step 4 is demonstrated by opening the comparative panel for the fact F1.1.4. This is illustrated in Fig. 7. The panel gives the name of the related fact (region 1) and below (region 2) there are the evidence tiles, one for each country. The tiles indicate the format of the related evidence (an image for Country A, a .doc document for Country B and .pdf document for Country C). In addition, for each country, the assessment of how well the evidence supports the analyzed fact is shown in the form of a colored circle. The colors indicate: acceptance (green), rejection (red) and uncertainty (yellow). Region 3 shows the opinion triangle related to the assessment of the evidence provided by Country A. The actual assessment is represented by the

MOST WIEDZY Downloaded from mostwiedzy.pl

hollow circle in the triangle and the linguistic values corresponding to this assessment are presented beside the triangle (it reads: ‘with very high confidence the support given by the evidence is tolerable’). The evidence is shown in region 4.

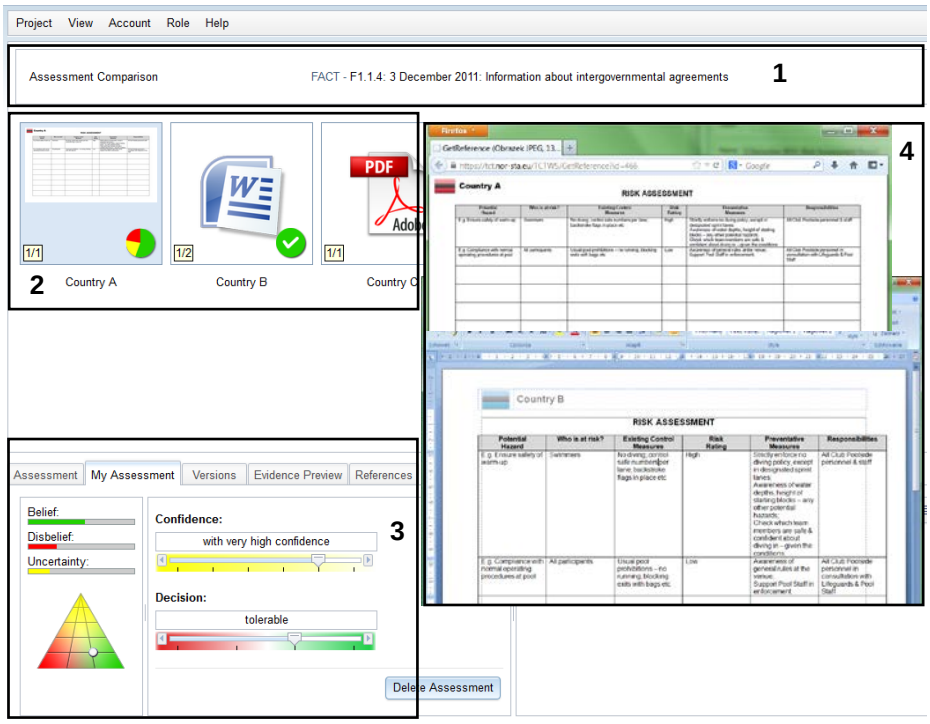

Fig. 7. Comparative panel for fact F1.1.4

The assessments of facts can be issued either from the comparative panel, or otherwise by opening a selected conformance case and browsing its structure. Fig. 8 presents the conformance case of Country A together with the assessment of the facts being the premises of claim CL1.1. The bottom part of the picture gives the details of the assessment of fact F1.1.4 which is currently pointed to.

5 Conclusion and Future Work

The case study presented in this paper was the starting point for common experiments conducted in cooperation with the Institute for Energy and Transport of Joint Research Centre (IET JRC) in Petten, the Netherlands, which is in charge of monitoring implementation of the Regulation 994/2010 in Member States, acting on behalf of the European Commission. The final conformance case template and the conformance cases for actual Member States are under development.

Gas distribution and supply is one of the key critical infrastructures requiring particular attention. With this example we demonstrated how the comparative conform-

MOST WIEDZY Downloaded from mostwiedzy.pl

ance cases could be used to monitor implementation of the Regulation. For a selected normative document, the initial step is to create a conformance case template for this document which becomes a sort of 'window' through which the supervising body can look at different implementations of the norm to assess and compare the submitted evidence. The investment needed to create the template is moderate: in case of Regulation 994/2010 the initial template consisted of some 212 nodes and the total effort in its creation consumed 18 person-hours.

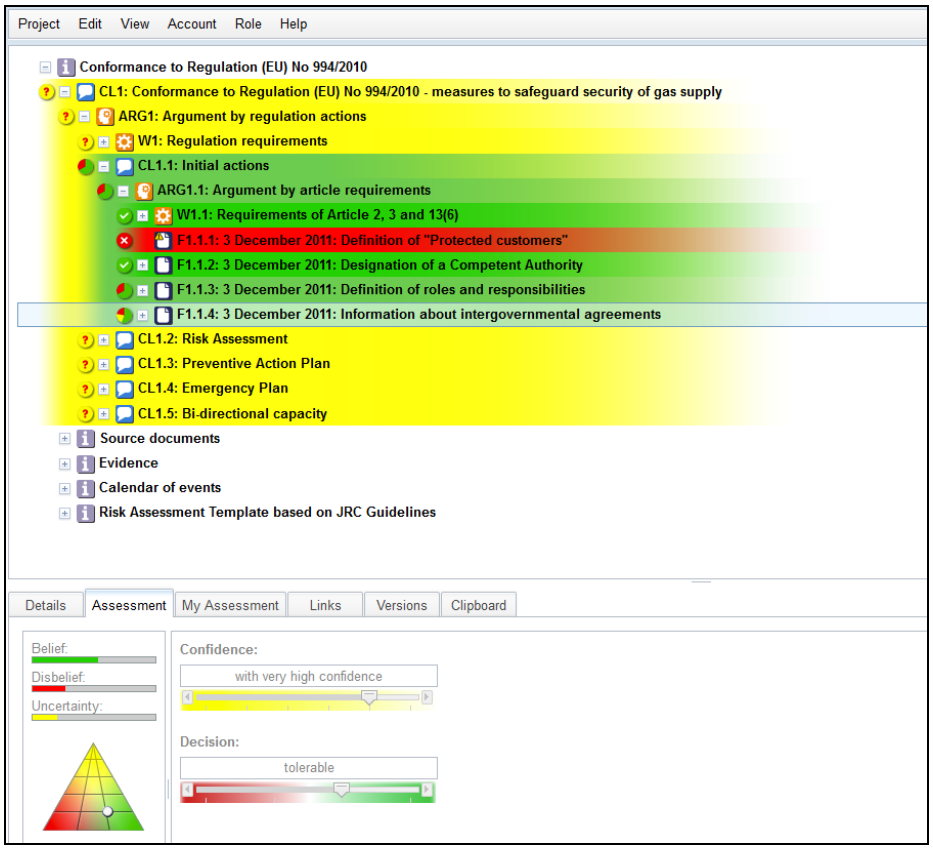

Fig. 8. Example assessment of the facts related to claim CL1.1

Conceptually, the user of a conformance case template can extend it by adding more specific argumentation (see Fig. 3). However, our experience with several standards (including healthcare related standards [17], standards for secure outsourcing, Common Assessment Framework [19] and others) shows that this option is rarely used. In majority of cases the template is being converted into a conformance case simply by supplying the evidence supporting particular facts.

Presently we are researching a possibility to use the comparative case concept to support monitoring of multiple cases related to the EU proposed legislation that

MOST WIEDZY Downloaded from mostwiedzy.pl

would require oil and natural gas companies to submit emergency response plans and potential hazard reports before being given a license to drill offshore.

Acknowledgments. This work was partially supported by the NOR-STA project (grant no. UDA POIG.01.03.01-22-142/09-03). Contribution of M. Witkowicz, J. Czyżnikiewicz and P. Jar to technical implementation of the NOR-STA services and cooperation of M. Masera from JRC, Institute for Energy and Transport in establishing experiments related to Regulation 994/2010 are to be acknowledged.

References

1. Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector, Final Report, AEA Technology, ED05761 (2009)
2. Górski, J. : Trust Case – a case for trustworthiness of IT infrastructures. In Cyberspace Security and Defense, NATO Science Series, 196, Springer-Verlag, 125-142 (2005)
3. Górski J., Jarzębowicz A., Leszczyna R., Miler J., Olszewski M.: Trust case: justifying trust in IT solution. Reliability Engineering and System Safety 89 (1), 33-47 (2005)
4. Ministry of Defence, Defence Standard 00-56 Issue 4: Safety Management Requirements for Defence Systems (2007)
5. Yuan T., Kelly T., Argument based approach to computer safety system engineering, Int. J. Critical Computer-Based Systems, 3 (3), 151-167 (2012).
6. Palin R., Habli I., Assurance of automotive safety – a safety case approach, Proc. SAFECOMP 2010, LNCS 6351, Springer, 82-96 (2010)
7. ISO/IEC 15026-2:2011: Systems and software engineering - Systems and software assurance - Part 2: Assurance case (2011)
8. Górski, J.: Trust-IT – a framework for trust cases, Workshop on Assurance Cases for Security - The Metrics Challenge. Proc. of DSN 2007, Edinburgh, UK, 204-209 (2007)
9. Cyra Ł., Górski J., Supporting Compliance with Safety Standards by Trust Case Templates, Proc. ESREL 2007, Stavanger, Norway, pp. 1367-1374 (2007)
10. Toulmin S.: The Uses of Argument, Cambridge University Press (1958)
11. Goal Structuring Notation community Standard version 1, 2011.
12. Adelard Safety Case Editor (ASCE) website, http://www.adelard.com/asce/
13. Shafer G.: Mathematical Theory of Evidence, Princetown University Press (1976)
14. Cyra Ł., Górski J.: Support for argument structures review and assessment, Reliability Engineering and System Safety 96, 26-37 (2011)
15. Górski J., Jarzębowicz A., Miler J., Witkowicz M., Czyżnikiewicz J., Jar P., Supporting Assurance by Evidence-Based Argument Services, LNCS 7613, Springer, 417-426 (2012)
16. Proceedings of the Workshop on Selected Problems in Environmental Risk Management and Emerging Threats, June 2009, Gdansk, Poland (http://kio.pg.gda.pl/ERM2009/)
17. Górski J., Jarzębowicz A., Miler J.: Validation of services supporting healthcare standards conformance, Metrology and Measurements Systems XIX (2), 269-282 (2012)
18. Regulation (EU) No 994/2010 of the European Parliament and of the Council of 20 October 2010 concerning measures to safeguard security of gas supply and repealing Council Directive 2004/67/EC (2010)
19. European Institute of Public Administration, CAF-Common Assessment Framework, http://www.eipa.eu/en/topic/show/&tid=191 (2012)

MOST WIEDZY Downloaded from mostwiedzy.pl