Post Print

The original publication is available at
www.springerlink.com

ERCIM-DECOS Workshop
(SAFECOMP 2012 associated event)
25-28 September 2012, Magdeburg, Germany
LNCS 7413, pp. 417-426

Supporting Assurance by Evidence-based Argument Services

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

Michał Witkowicz[2], Jakub Czyżnikiewicz[2], Patryk Jar[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, miwi, jakubc, patryk.jar}@eti.pg.gda.pl

Abstract. Structured arguments based on evidence are used in many domains, including systems engineering, quality assurance and standards conformance. Development, maintenance and assessment of such arguments is addressed by TRUST-IT methodology outlined in this paper. The effective usage of TRUST-IT requires an adequate tool support. We present a platform of software services, called NOR-STA, available in the Internet, supporting key activities related to argument editing, communication and assessment and demonstrate an example of its application based on real case study focusing on analyzing safety of an innovative IT system.

Keywords: evidence-based argument, standard conformance, safety case, TRUST-IT methodology, NOR-STA services

1 Introduction

Evidence-based arguments are widely recognized in the domain of systems engineering as means to demonstrate (required) system properties, for instance safety of critical applications like medical, avionic, military and others. In many cases it is required by the regulations that a *safety case* is explicitly presented, which in its essence is an argument supported by sufficient evidence [1]. Dedicated methods of developing and presenting safety cases are in use, e.g. [2, 3].

However, safety is not the only quality aspect to be argued for in an explicit way. Other properties, like security or reliability are also considered important in some application contexts which leads to the notions of *security case* or *reliability case*, or in more general terms, *assurance case* [4]. In even more general terms, a *trust case* can be considered, as an evidence-based argument that is used to strengthen trust in any postulated claim, not necessarily related to an IT system property [5]. An example of application of trust cases is demonstrating conformance to standards. In such situation, an evidence-based argument is used to justify the claim about standard conformance and such argument can then be assessed by independent auditors.

In this paper we first introduce a methodology of editing, assessing and presenting evidence-based arguments, called TRUST-IT, then describe a set of NOR-STA services which support application of this methodology in different contexts, and next present a demonstration scenario where the services are used to

represent and improve a safety argument related to a WSN based application supporting a patient in his/her home environment.

The argument model of TRUST-IT is based on [6] and its underlying concepts are similar to these of Claim-Argument-Evidence (CAE) [2] and Goal Structuring Notation (GSN) [3]. TRUST-IT distinguishes from other approaches by its argument assessment mechanism [7] and by the concept of conformance argument template which is presently used to support implementation of different standards [8]. The existing tools, commercial (e.g. ASCE [9] and ISCaDE [10]) and resulting from research projects (e.g. Visio add-on by University of York [11] and ACCESS by University of Virginia [12]) do not support group work and remote access. The tools [9], [11] and [12] are desktop applications and provide little, if any, support for sharing arguments and sharing the supporting evidence. The tool [10] is based on IBM Telelogic DOORS environment and provides a limited multi-user work mode using thick-client. Each of these tools require an installation process dedicated for each user. NOR-STA services supporting TRUST-IT are offered in a cloud accessible for any Internet user and can be used without any prior investment in infrastructure. The services provide full support for argument creation and maintenance, for argument assessment and for integration of the supporting evidence residing in user chosen repositories.

The paper is structured as follows. Section 2 introduces TRUST-IT methodology and explains the underlying argument model. Section 3 describes how the methodology is implemented by NOR-STA services. Section 4 presents a demonstration scenario of applying TRUST-IT and NOR-STA in developing a safety argument for a WSN-based system. Other areas of application are outlined in Section 5. The paper is concluded in Section 6, which also provides directions of future work.

2 Evidence based arguments – the TRUST-IT model

TRUST-IT [5, 13, 14] is a method of representing arguments based on the generic Toulmin's argument model [6]. An argument includes: a *conclusion* to be justified, *premises* the conclusion is reasoned from and a *warrant* which establishes the relationship between the premises and the conclusion.

In TRUST-IT, an evidence-based argument is a tree-like structure and is composed of different types of nodes which define the language for representing arguments. The model of an argument (including node types and their relationships) is shown in Fig. 1, where an arrow represents the *can-be-child-of* relationship.

Argument conclusion is represented by a *claim* node. A node of type *argument* links the *claim* to the corresponding premises and uses the *warrant* to explain how the premises justify the *claim*. A premise can be of the following type: an *assumption* represents a premise which is not further justified; a *claim* represents a premise to be further justified by its own premises; and a *fact* represents a premise which is supported by some evidence. The evidence is provided in external documents which are pointed to by nodes of type *reference*. As *claim* can represent both, the conclusion and a premise, the model allows to represent complex tree-like structures (in our experience up to several thousands of elements).

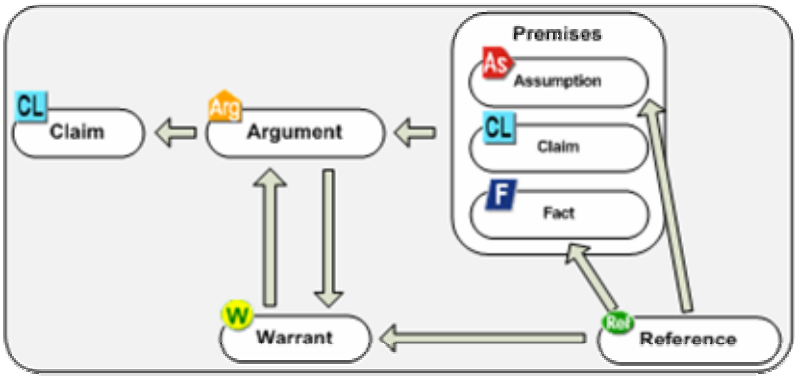

Fig. 1. The TRUST-IT argument model

An argument represented in accordance with TRUST-IT explicitly shows how the topmost conclusion is justified by the evidence through a possibly long chain of reasoning. The 'compelling power' of such argument can be assessed by a human who can analyze and assess both, the support given by the evidence and the validity of the reasoning included in the argument. In [7] an argument assessment method based on Dempster-Shafer theory of belief functions [15] and its application to TRUST-IT type arguments is presented. In addition to this method, other more specific assessment schemes can be applied, for instance in some

applications we use a simple scale of three values: *accept*, *partially accept*, *reject* to assess the support given by the evidence to a fact and the support given by the premises to the related conclusion.

3 Tool support – NOR-STA services

In this section, we present the functional scope of the NOR-STA services, the architecture and technology of their implementation, and finally their quality assurance.

3.1 Scope

The scope of functionalities of NOR-STA services include:

- argument representation and editing using the graphical symbols shown in Fig. 1;
- integration (through references) of various types evidence, including textual documents, graphics, images, web pages, video and so on;
- argument assessment and visualization of the assessment results;
- publishing of an argument;
- evidence hosting in protected repositories.

In addition to the above, the services provide for version control and handling of multiple arguments. Quality of service, in particular in relation to security, is guaranteed by declaring and implementing an adequate security policy.

The usage context depends on the business processes within which the services are embedded. For example - one party can develop an argument, submit the supporting evidence and publish the argument, while another party conducts an audit and assesses the argument. The evidence can by maintained at the premises of its owner, or otherwise it can be hosted at a leased space accessible through NOR-STA service.

3.2 Implementation

Implementation of NOR-STA services is based on the RIA (Rich Internet Application) concept and uses modern technologies, in particular AJAX, FLOSS, VMware and others. The main screen interfacing to NOR-STA services is shown in Fig. 2.

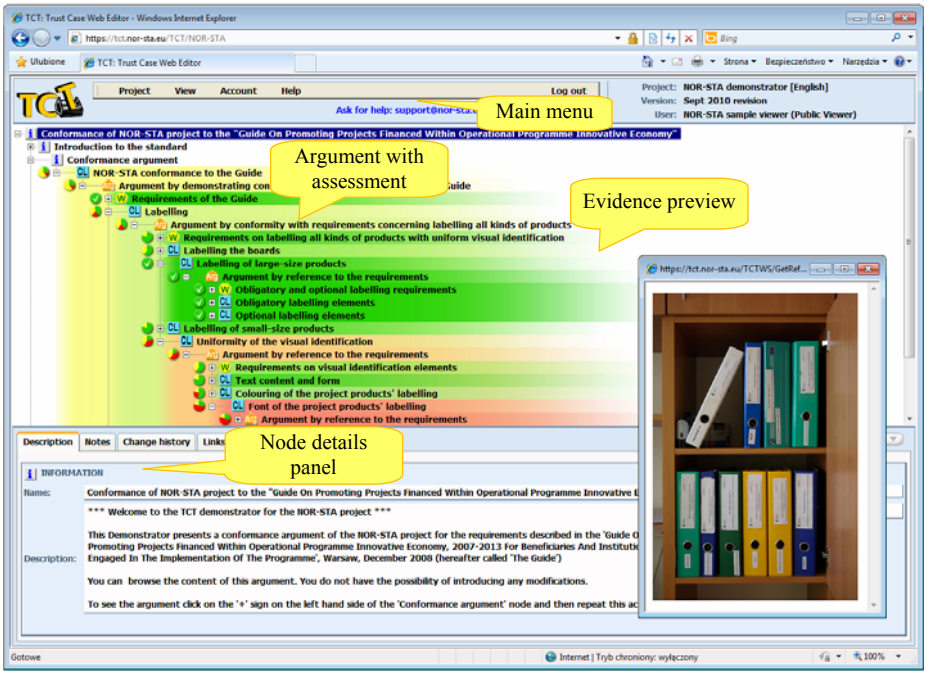

Fig. 2. The NOR-STA services window in an Internet browser

The architecture of NOR-STA services follows the rich client-server model which is illustrated in Fig. 3. The model includes three layers: database server PostgreSQL, application server JBoss and a client written in JavaScript in accordance with AJAX (Asynchronous JavaScript and XML). The lowest layer (the database) implements the business logic as a set of stored procedures. The intermediate layer is based on JEE and links the database with the client. Communication between these layers is based on RESTful Web Services and JSON (JavaScript Object Notation).

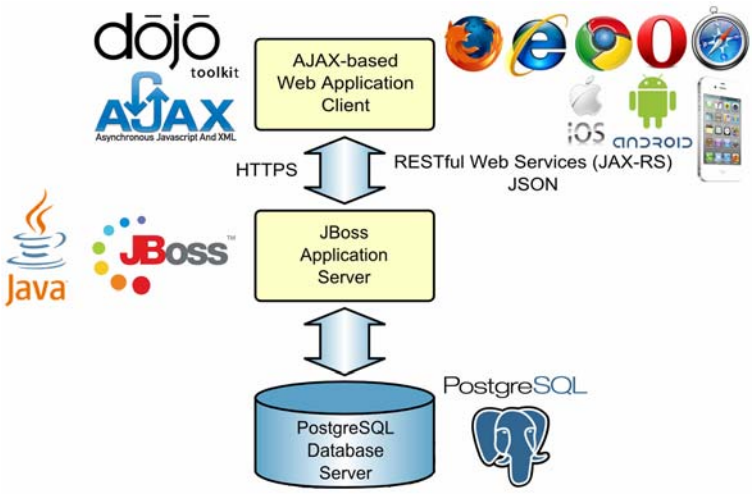

Fig. 3. The architecture of NOR-STA services

The services are deployed in a cloud in accordance with the Software-as-a-Service model. Due to this model they can be used as needed, without any prior investment in a specialized IT infrastructure. End users do not need to install any software and simply access the services with a standard Internet browser. SaaS model was chosen because it provides for high accessibility and maintainability of the services, straightforward integration with other Internet services, low distribution costs and flexible charging.

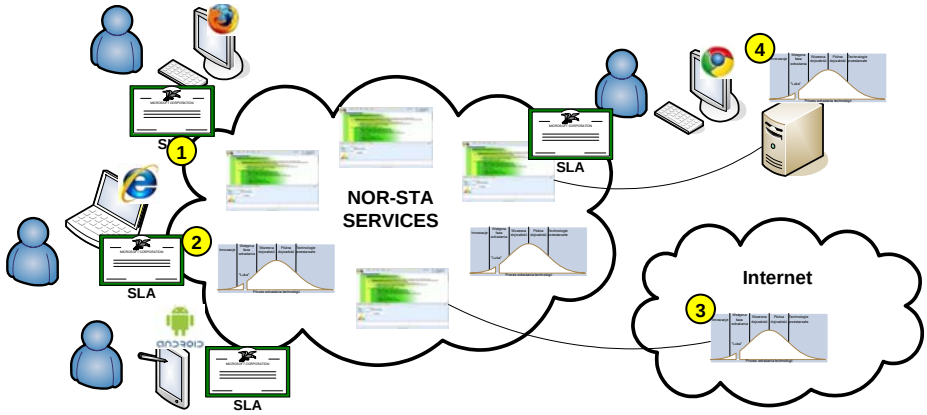

Fig. 4. NOR-STA services as a cloud

Fig. 4. explains the NOR-STA services deployment model where the key architectural elements are marked with numbers in circles. It is possible to integrate the argument (1) with both, internal (i.e. being a part of NOR-STA services - 2) or external repositories where the evidence is stored. An external repository can be located in the Internet (3) or in a private infrastructure of a user (4). NOR-STA services are available from a wide variety of hardware and software platforms including desktop PCs, laptops, iOS or Android tablets and smartphones with Firefox, Internet Explorer, Chrome, Opera and other Internet browsers.

3.3 Service quality

Quality of service, in particular in relation to security, is guaranteed by signing a Service Level Agreement (SLA) with the users. It refers to the Information Security Policy (ISP) which explains how security of arguments and the related evidence is being guaranteed by organizational, logical and physical measures. The security measures include Role Based Access Control (RBAC), encrypted data transmission between browser and server (SSL), encrypted passwords, input data validation, intrusion detection system, data replication techniques and advanced means of physical protection of servers. User's data remain under exclusive control of the user who can decide who and under which conditions can access the data.

Virtualization technologies provide for delivering a reliable, scalable and highly available platform of services. Service availability is continuously monitored by on-line tools. The measurements show that the availability of NOR-STA services was at the level 99.7% over a period of six months [8].

The services are under continuous development for more than five years, following the incremental and evolutionary software development model. The testing strategy applied in this process is described in [16]. A new release of NOR-STA services will provide enhanced cross-browser compatibility which includes support for mobile web browsers.

4 Demonstration scenario: safety assurance

The objective of this scenario is to demonstrate how an argument can be improved by providing additional evidence and how the services help in identifying the place where this evidence is to be included.

NOR-STA services were used, among others, to analyze trustworthiness of the ANGEL platform (an embedded software platform supporting Wireless Sensor Networks based applications) and the ANGEL system – an application demonstrating platform's usability for patient monitoring in his/her home environment [17][1]. Two groups of evidence based arguments (called *trust cases*) were built, one for the system and another for the platform. Each covered three quality related aspects: patient's safety, patient's privacy and security of critical information assets.

In this demonstration scenario we focus on the safety aspect of ANGEL system. The argument focuses on the safety hazards that were identified by analyzing possible system usage scenarios. All identified hazards were then assessed with respect to their severity and likelihood of occurrence. An example of a hazard together with the resulting safety requirement is given below:

Hazard: Alarm message is not correctly and timely delivered

Requirement: ANGEL system has to assure that in case of unexpected event (e.g. health state deterioration or smoke detected in the apartment), the related alarm message is correctly delivered to the recipient (*Correctness of alarms*).

The identified safety requirements were documented as argument claims and subjected to further analysis investigating their possible design solutions leading to implementation of the requirement (documented as sub-claims). Actual implementation of such solution provided the evidence that was referred to while arguing a fact that a given hazard has been successfully mitigated.

The completed safety argument was evaluated by an auditor who assessed the support given by the evidence to the facts listed in the argument. The assessment of the claims was then calculated automatically following the algorithm based on Dempster-Shaffer belief functions presented in [7]. A part of the evaluated argument is shown in Fig. 5. The colors represent the result of argument evaluation: red color shows the parts which are weakly supported by the available evidence whereas these parts which are strongly supported are shown in green color. [2]

As can be seen in Fig. 5, the fact *Alarm management system reliably handles alarms in ANGEL application* is (in the eyes of the auditor) weakly supported by the evidence item *D5.5 Integration of the demonstrator components (section 2.3.4)* being an extract from the system design report. This weak support was then propagated to all higher level claims presented in Fig. 5.

[1] 6th FR STREP Project ANGEL (Advanced Networked embedded platform as a Gateway to Enhance quality of Life) Contract number IST-033506

[2] Figures 4 and 5 are extracts from the screens presenting the argument in the browser window.

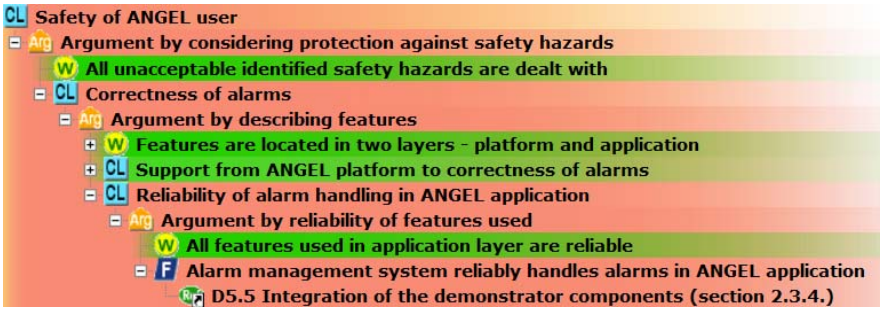

Fig. 5. Initial assessment of *Safety of ANGEL user* argument

The weakness indicated in Fig. 5 resulted in the decision to strengthen safety assurance by carrying additional tests aiming at validation of the safety alarm mechanism present in the system. The resulting evidence (test plans and test results) was added to the argument to better support the *Alarm management system reliably handles alarms in ANGEL application* fact. The result is presented in Fig. 6, where an additional piece of evidence *Experimental validation of the safety alarm* is included to support the fact. Fig. 6 also shows the result of the argument re-assessment: in this case sufficient support is given to the fact and this positive appraisal is propagated to all higher level claims.

Fig. 6. *Safety of ANGEL user* argument strengthened with additional evidence

5 Present experience

TRUST-IT methodology and the NOR-STA services were already used to build arguments in many different applications contexts, such as:

- analyzing trustworthiness of systems and services, including safety, security and privacy claims,
- analyzing conformance to standards,
- justifying the selection of metrics supporting the stated measurement objective,
- building validation arguments for systems and services.

The ideas, methods and tools underpinning TRUST-IT and NOR-STA services were developed over the last few years while participating in three 5th and 6th FR research and development projects: 5th FR STREP Project DRIVE, 6th FR Integrated Project PIPS and 6th FR STREP Project ANGEL.

Presently NOR-STA services are being applied to develop standards conformance arguments, in relation to standards in healthcare, standards related to security of outsourcing and standards related to self-assessment of public administration institutions. A formal cooperation involves more than 30 institutions which signed formal contracts as NOR-STA services users. The services are also experimented with in relation to monitoring of implementation of Regulation (EU) No 994/2010 of the European Parliament and of the Council concerning measures to safeguard security of gas supply Member States.

6 Conclusions

Our services for evidence based arguments were successfully applied to build, assess and communicate very large and complex arguments in various application contexts. In relation to standards conformance,

NOR-STA services are highly evaluated by their users for both, their quality and business value [8]. The users particularly appreciate improvement in evidence management, better preparation to the audit, better visibility of conformance status, easier conformance maintenance as well as high availability and reliability of the services.

Future work is directed towards researching new application areas, identification of suitable business models as well as further extension of the scope of services and improvement of their quality. In particular, a new version of the services is planned for release in mid-2012, which will particularly focus on usability, personalization, flexibility, effective interaction, and browser and platform compatibility. The progress, user assessment and development plans are constantly presented at the NOR-STA portal www.nor-sta.eu/en. Among the main directions of future research and development are comparative conformance cases (e.g. for monitoring implementation of common regulations at different sites), domain specific argument patterns, dynamic arguments for automatic monitoring of changing evidence, automatic detection of events (e.g. ageing evidence, evidence changes requiring re-evaluation of the argument, and so on) and full support for version control and reporting.

Acknowledgments. This work was partially supported by the NOR-STA project co-financed by the European Union under the European Regional Development Fund within the Operational Programme Innovative Economy (grant no. UDA-POIG.01.03.01-22-142/09-03).

References

1. Ministry of Defence, Defence Standard 00-56 Issue 4: Safety Management Requirements for Defence Systems (2007)
2. Emmet L., Guerra S.: Application of a Commercial Assurance Case Tool to Support Software Certification Services, In: Proceedings of the 2005 Automated Software Engineering Workshop on Software Certificate Management SoftCeMent'05, ACM, New York (2005)
3. Kelly T., Weaver R.: The Goal Structuring Notation - A Safety Argument Notation, Proceedings of the Dependable Systems and Networks Workshop on Assurance Cases (2004)
4. Rhodes T., Boland F., Fong E., Kass M.: Software Assurance Using Structured Assurance Case Models, NIST Interagency Report 7608, US Department of Commerce (2009)
5. Górski, J. : Trust Case – a case for trustworthiness of IT infrastructures. In Cyberspace Security and Defense: Research Issues, NATO Science Series II: Mathematics, Physics and Chemistry, 196, Springer-Verlag, 125-142 (2005)
6. Toulmin S.: The Uses of Argument, Cambridge University Press (1958)
7. Cyra Ł., Górski J.: Support for argument structures review and assessment, Reliability Engineering and System Safety 96, 26-37 (2011)
8. Górski J., Jarzębowicz A., Miler J.: Validation of services supporting healthcare standards conformance, Metrology and Measurements Systems, 19 (2) 269-282 (2012)
9. ASCE home page, http://www.adelard.com/asce/, visited 2012.06.27
10. ISCaDE home page, http://www.iscade.co.uk/, visited 2012.06.27
11. GSN add-on for Visio home page, http://www-users.cs.york.ac.uk/~tpk/gsn/, visited 2012.06.27
12. Steele P., Collins K., Knight J., ACCESS: A Toolset for Safety Case Creation and Management, Proc. of 29th International Systems Safety Conference, Las Vegas, NV. (2011)
13. 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)
14. Gorski J., Jarzebowicz A., Leszczyna R., Miler J., Olszewski M.: Trust case: justifying trust in IT solution. Reliability Engineering and System Safety 89 (1), 33-47 (2005)
15. Shafer G.: Mathematical Theory of Evidence, Princetown University Press (1976)
16. Górski J., Witkowicz M.: Experience with instantiating an automated testing process in the context of incremental and evolutionary software development, E-informatica: Software Engineering Journal 5 (1) 51-63 (2011)
17. Górski J., Jarzębowicz A., Miler J., Gołaszewski G., Cyra Ł., Witkowicz M.: Deliverable D5.4: Trust Case for ANGEL platform demonstrator, ANGEL STREP Project deliverable, project no. IST-5-033506-STP (2008)