Evidence-based arguments as a tool supporting risk management of critical infrastructures

Janusz Górski
jango@eti.pg.gda.pl

Department of Software Engineering
Gdańsk University of Technology, Poland

ARGEVIDE sp. z o.o., Gdańsk, Poland

2nd ERNCIP Conference, 15-17 April 2015, Brussels
Topics

- Evidence based arguments
- What is TRUST-IT and NOR-STA?
- Argument model and argument assessment
- How NOR-STA supports conformance/compliance and assurance
  - Experiences with using NOR-STA
- Conformance Case Study: EU Regulation 994/2010
- NOR-STA demo
Evidence-based Arguments

- **Argument** is an attempt to persuade someone of something, by giving reasons and/or evidence for accepting a particular conclusion.

- **This 'something'** can be:
  - assurance of some important property (safety, security, privacy, reliability, …)
  - conformance with a stated set of criteria (standard, norm, directive, recommendation and so on)
  - ranking in fulfillment of the agreed requirements
  - …

- **Evidence** in its broadest sense includes everything that is used to determine or demonstrate the truth of an assertion.
  - Evidence can be used to support arguments — by demonstrating the truth of the premises

**Assumption:**
Evidence is delivered in electronic documents of any form: text, graphics, image, video, audio etc.
Evidence based arguments

Assurance cases
- Safety
- Privacy
- Security

Conformance cases
- Hospital accreditation
- CAF
- HACCP
- ISO

Rating cases
- H&S+E+Q

Comparative cases
Evidence based arguments
Deployment in the cloud

Application specific packages

Generic Argument Management Services
Deployment in the cloud

Generic Argument

Management

Services

Application specific packages

nor-sta
NOR-STA argument model
Case study – a meeting
An argument about the meeting

- **We will have a successful meeting because true experts participate**

**Strategy of argumentation:**
Argumentation by referring to competencies of participants

**Rationale:**
Case studies reveal that success of a meeting depends on the expertise of its participants

**Evidence:**
Demonstrates a fact that we have true experts at the conference
NOR-STA argument model

Claim

Inference

Argumentation strategy

Rationale

Premises

Claim

Assumption

Fact

Information

Reference
Example: Successful meeting

- Argument about success of a meeting
- The meeting will be successful
- Argument by referring to competencies of participants
  - Case studies reveal that success of a meeting depends on competencies of participants
  - Natalie is an expert
    - Natalie's CV
  - Ricky is an expert
    - Ricky's CV
  - Martin is an expert
    - Martin's CV
Example: Successful meeting
Example:
Successful meeting

- Argument about success of a meeting
- The meeting will be successful
  - Argument by referring to competencies of participants
    - Case studies reveal that success of a meeting depends on competencies of participants
- Natalie is an expert
- Natalie's CV
- Ricky is an expert

Natalie Shah
1 Any Road, Anytown AN1 1CV
Telephone: 01632 960 941; Mobile: 07700 900 935; Fax: 01632 960 316
Email: natalieshah@example.com

PROFESSIONAL PROFILE

- A versatile and results-oriented professional who specialises in sourcing and buying products from UK and overseas markets requiring strong supplier relationships
- Familiar with all aspects of the consumer electronics market with particular emphasis on buying, marketing and e-commerce
Argument Assessment
We will have a successful meeting because true experts participate

- Logic doubt:
  Does participation of true experts really determine the success of a meeting?

- Epistemic doubt:
  Do we really have experts at this meeting?
Communication the assessment results

- The meeting will be successful
  - Argument by referring to competencies of participants
    - Case studies reveal that success of a meeting depends on competencies
    - Natalie is an expert
      - Natalie's CV
    - Ricky is an expert
      - Ricky's CV
    - Martin is an expert
      - Martin's CV
Presently NOR-STA supports 7 different assessment methods

- You can select an assessment method appropriate to your needs

- It is possible to include additional, customer-specified assessment methods
Presently NOR-STA supports 7 different assessment methods. You can select an assessment method appropriate to your needs. It is possible to include additional, customer-specified assessment methods.
HOW NOR-STA SUPPORTS CONFORMANCE/COMPLIANCE?

- Prescriptive approach - standards/regulations impose explicit requirements to be met
- Conformance Case = evidence-based argument demonstrating conformance to the requirements
  - Conformance Argument Template = a pattern of argumentation derived from the standard

- NOR-STA has been already applied to develop conformance cases for the following standards:
  - Commercial applications
    - Hospital accreditation
    - HACCP (Hazard Analysis and Critical Control Point system)
    - CAF (Common Assessment Framework)
    - SSB (Outsourcing risk management)
  - R&D applications
    - ISO 27001 (Information Security Management)
    - ISO/IEC 15408 (Common Criteria)
    - EU Regulation 994/2010 (Measures to safeguard security of gas supply)
HOW NOR-STA SUPPORTS CONFORMANCE/COMPLIANCE?

- Prescriptive approach - standards/regulations impose explicit requirements to be met

- Conformance Case = evidence-based argument demonstrating conformance to the requirements
  - Conformance Argument Template = a pattern of argumentation derived from the standard

- NOR-STA has been already applied to develop conformance cases for the following standards:
  - Commercial applications
    - Hospital accreditation
    - HACCP (Hazard Analysis and Critical Control Point system)
    - CAF (Common Assessment Framework)
    - SSB (Outsourcing risk management)
  - R&D applications
    - ISO 27001 (Information Security Management)
    - ISO/IEC 15408 (Common Criteria)
    - EU Regulation 994/2010 (Measures to safeguard security of gas supply)
HOW NOR-STA SUPPORTS ASSURANCE?

- Goal-setting approach – performance oriented objectives to be demonstrated
- Assurance Case = evidence-based argument demonstrating achieving of the assumed goals
  - User-chosen strategy of argumentation
    - e.g. risk-based decomposition, architecture-based decomposition
  - Explicit justification of confidence

NOR-STA has been already applied to develop assurance cases in relation to the following documents:

- Commercial applications:
  - ISO 17065 (Conformity assessment -- Requirements for bodies certifying products, processes and services) – technology qualification
  - ISO 26262 (Road vehicles – Functional safety)
  - IEC 61511 (Functional safety - Safety instrumented systems for the process industry)
  - IEC 61508 (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems)

- R&D applications:
  - HIPAA (Health Insurance Portability and Accountability Act)
  - Safety of medical devices (FDA Open PCA Pump)
Case study: EU Regulation 994/2010
We start the argument with a claim about being conformant to the Regulation (EU) No 994/2010 - measures to safeguard security of gas supply.
Claim should be supported by a justified argumentation strategy.

**Argumentation strategy** explains the inference rule

- Conformance to Regulation (EU) 994/2010 - measures to safeguard security of gas supply
- Argument by referring to mandatory actions required by the regulation
- Regulation requirements explicitly enumerate mandatory actions

**Rationale** justifies why the rule is appropriate and valid
Adding premises

Conformance to Regulation (EU) No 994/2010 - measures to safeguard security of gas supply

Argument by referring to mandatory actions required by the regulation

Initial actions

Risk Assessment

Preventive Action Plan

Emergency Plan

Claims to be supported by more detailed argumentation
Adding premises

Initial actions

Argument by article requirements (Article 2, 3 and 13(6))

Definition of "Protected customers"

Designation of a Competent Authority

Definition of roles and responsibilities

Information about intergovernmental agreements

Facts
to be supported by evidence
Adding references to evidence

**Reference** – points to an external resource (evidence container)

Designation of a Competent Authority

Competent Authority designation act

A warning sign ⚠️ is used to denote incomplete elements, e.g. references without any evidence
Adding references to evidence

Reference – points to an external resource (evidence container)

Designation of a Competent Authority

Competent Authority designation act

Competent Authority Designation Act
Complete argument for 994/2010

Conformance to Regulation (EU) No 994/2010

CL1: Conformance to Regulation (EU) No 994/2010 - measures to safeguard security of gas supply

ARG1: Argument by regulation actions

W1: Regulation requirements

ARG1.1: Argument by article requirements

W1.1: Requirements of Article 2, 3 and 13(6)

Regulation (EU) No 994/2010 Article 2

Regulation (EU) No 994/2010 Article 3

Regulation (EU) No 994/2010 Article 13

F1.1.1: 3 December 2011: Definition of "Protected customers"

F1.1.2: 3 December 2011: Designation of a Competent Authority

3 December 2011: Competent Authority designation act

F1.1.3: 3 December 2011: Definition of roles and responsibilities

F1.1.4: 3 December 2011: Information about intergovernmental agreements

CL1.2: Risk Assessment

CL1.3: Preventive Action Plan

CL1.4: Emergency Plan

CL1.5: Bi-directional capacity
Assessment of the argument for 994/2010

- Conformance to Regulation (EU) No 994/2010
  - CL1: Conformance to Regulation (EU) No 994/2010 - measures to safeguard security of gas supply
    - ARG1: Argument by regulation actions
      - W1: Regulation requirements
        - Regulation (EU) No 994/2010
      - CL1.1: Initial actions
        - ARG1.1: Argument by article requirements
          - W1.1: Requirements of Article 2, 3 and 13(6)
            - Regulation (EU) No 994/2010 Article 2
            - Regulation (EU) No 994/2010 Article 3
            - Regulation (EU) No 994/2010 Article 13
  - F1.1.1: 3 December 2011: Definition of "Protected customers"
  - F1.1.2: 3 December 2011: Designation of a Competent Authority
    - 3 December 2011: Competent Authority designation act
  - F1.1.3: 3 December 2011: Definition of roles and responsibilities
    - 3 December 2011: Definition of roles and responsibilities
  - F1.1.4: 3 December 2011: Information about intergovernmental agreements
    - 3 December 2011: Information about intergovernmental agreements
  - CL1.2: Risk Assessment
  - CL1.3: Preventive Action Plan
  - CL1.4: Emergency Plan
  - CL1.5: Bi-directional capacity
NOR-STA DEMO
How NOR-STA supports CIP?

- Regulator’s viewpoint
  - imposing a common structure of compliance demonstration
  - continuous monitoring of compliance achievement by different users

- Operator’s viewpoint
  - demonstrating conformance with standards and regulations
  - support for internal and external audit
  - support for assuring specific CIP objectives
  - support for vertical communication (management information and decisions)
  - support for responsibilities assignment
Where can I find more information?
Products and services

Argewe offers NOR-STA software to support:

- conformance and compliance management with the help of conformance cases for standards and regulations in sectors such as healthcare, automotive, energy, food, medical devices and security;
- assurance management with the help of assurance cases to demonstrate system safety, dependability, security or other properties.

NOR-STA supports:

- uniform representation of standards requirements and assurance objectives,
- reuse by applying argumentation patterns and templates,
- evidence and documentation integration,
- change management and baselines,
- audits and self-assessments,
- diverse assessment methods,
- customizable reports,
- role-based access control,
- cooperation and communication of all involved parties.

You can use NOR-STA online (hosted by Argevide) or installed on your own server.

Read more on our products

Argewe offers support and training services on the methodology of using NOR-STA to help our users effectively and efficiently manage conformance and assurance processes.

Read more on our services

Benefits for NOR-STA users

Using NOR-STA in conformance and assurance management will enable you to gain benefits such as:

- effort reduction,
- strengthening users' involvement,
- risk reduction for conformance/assurance objectives.

Who we are?

Argewe is a company created to deliver solutions for managing system assurance and standard conformance with use of evidence-based arguments. The products offered to customers resulted from research projects of Information Assurance Group in the Department of Software Engineering at Gdańsk University of Technology.

Read more about us

Our Mission

To help system and service suppliers, auditors and certification bodies to effectively manage conformance and assurance processes by using structured evidence-based arguments.

Our Customers

Our products and services are used by institutions interested in:

- achieving and/or assessing conformance with stated requirements (standards, regulations and other normative criteria);
- analysis and demonstrating system assurance for safety, security, reliability, maintainability and other goals.

Read more on customers

Selected Argevide customers:

DNV-GL

NEWS

2015-03-05
Argewe NOR-STA 6.5 released

2014-11-10
EUCI Protection Unit Meeting

2014-10-31
NOR-STA at IMBSA 2014

NOR-STA FEATURES

- Workgroup collaboration
- Working with large arguments
- Evidence management
- Assessment and visualisation
- Change management
Questions & Answers