Introduction to NOR-STA

Janusz Górski
IAG, Gdańsk University of Technology

IoTSec meeting
NCC, Oslo, 6th June 2018
Focusing on trust and risk management of computerized systems and services

Experience with numerous standards, including the security domain (e.g. ISO 27001, IEC 62443 series)

Present international cooperation
- EWICS Security (European Workshop on Industrial Computer Systems)
- ISA99 Committee (International Society of Automation), standardy IEC 62443
- ICCF/ERNCIP (IACS components Cybersecurity Certification Framework)
- IoTSec (Internet of Things Security)

Authors of Trust-IT methodology and the NOR-STA tool supporting application of evidence-based arguments to analyse and demonstrate assurance and compliance
- Since 2014 NOR-STA is a commercial product offered by ARGEVIDE spin-off of GUT
  - Commercial clients in Oil&Gas, Medical, railways, automotive sectors
Trust-IT and NOR-STA
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)
  - ...

- **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.
Argument and trust

Convincing arguments can be used to support trust

- because they demonstrate trustworthiness

Example:

A convincing (based on evidence) argument that a service is secure increases trust in the service

Evidence:

- protective measures used,
- certification procedures passed,
- penetration tests results
- operating data etc.
Evidence based arguments

Trust cases

Assurance cases

Conformance cases

Safety

Security

Privacy

Others

Hospital accreditation

ISO 14971

IEC 62443

HACCP

ISO 27001

TCL - Trust Case Language
TCL argument model
A case study: Argument about testing

Tests confirm that this software module satisfies its requirements because test results are positive and test coverage is sufficient

Strategy of argumentation:
Argumentation by referring to test results and test coverage

Rationale:
Experience shows that positive results of tests of adequate coverage reliably demonstrate fulfillment of the requirements

Evidence:
Demonstrates a fact about test results and test coverage
A case study: Argument about testing

Tests confirm that this software module satisfies its requirements because tests results are positive and test coverage is sufficient

Strategy of argumentation:
Argumentation by referring to test results and test coverage

Rationale:
Experience shows that positive results of tests of adequate coverage reliably demonstrate fulfillment of the requirements

Evidence:
Demonstrates a fact about test results and test coverage
The argument model

- **Claim**
  - Argument
  - Argumentation strategy
  - Rationale
  - Fact
  - Assumption
  - Reference
  - Information

- **Premises**
  - Conclusion
  - Inference

- **Strategy**
  - Analysis
  - Evaluation
  - Synthesis
Example security-related argument
Security argument - example

Security of unsuccessful login attempts
Security argument - example

Facts

- Security of unsuccessful login attempts
- Argumentation by referring to the best practices recommendations
- Best practices represent proven protection mechanisms
- Password expiration settings management
- Design documentation explaining the password expiration mechanism
- Checking and handling login errors
- Design documentation explaining the mechanism for login errors handling
- Setting limit for unsuccessful logins
- Design documentation explaining the limit of unsuccessful logins
- Report from tests addressing the limit of unsuccessful logins

References to the evidence that demonstrates facts

- Raports from expert reviews and assessments
- Design documentation
- Tests and measurements
- Simulations
Argument assessment
Tests confirm that this software module satisfies its requirements because tests results are positive and test coverage is sufficient.

**Logic doubt:**
Do successful tests of right coverage really determine the success of testing?

**Epistemic doubt:**
Do we really have positive test results and the right coverage?

**Claim:**
Module meets requirements

**Fact:**
adequate coverage and positive test results

**Evidence**
The assessment process

Assess conclusions

Assess inferences (local)

Assess facts (local)
Can we automatically aggregate the local assessments (inferences, facts) into the assessment of the whole argument?
Presently NOR-STA supports 9 different assessment methods.
- 3 of them support automatic aggregation of local assessments.
- You can select an assessment method appropriate to your needs.
- It is possible to include additional, custom-specified assessment methods.
Different methods of argument assessment:

- Dempster-Shafer
- ISO 33000 (SPICE, Automotive SPICE, ...)
- Rating scale (numerical)
- Three-level assessment
- and others...
Support for Smart Grid security
SPD argument

S&P&D

Objectives

Logic decomposition into more specific objectives

Analytical and measurement layer – collecting evidence that demonstrates objectives

Smart grid of interest
SPD argument

S&P&D Objectives

Logic decomposition into more specific objectives

Analytical and measurement layer – collecting evidence that demonstrates objectives

Smart grid of interest
Argument Assessment based on Dempster-Shafer belief model
 „Small” case study: argument assessment

Tests confirm that this software module satisfies its requirements because tests results are positive and test coverage is sufficient

Logic doubt:
Do successful tests of the right coverage really determine the success of testing?

Epistemic doubt:
Do we really have positive test results of right coverage?

Claim:
Module meets requirements

Fact:
adequate coverage and positive test results

Evidence

Acceptance Uncertainty Rejection
Assessment of an argument

Assessment of evidence
- Fact: ‘test results are positive’
  - Test report of this module demonstrating that test results are positive
  - Test report of different module
  - Test report of this module demonstrating that tests failed
- Assessment
  
<table>
<thead>
<tr>
<th></th>
<th>Acceptance</th>
<th>Uncertainty</th>
<th>Rejection</th>
</tr>
</thead>
</table>

Assessment of inference
- ‘if we have positive test results and adequate tests coverage, then the module meets its requirements’
  - How reliable is such reasoning?
- Assessment
  
<table>
<thead>
<tr>
<th></th>
<th>Acceptance</th>
<th>Uncertainty</th>
<th>Rejection</th>
</tr>
</thead>
</table>
User interface

Scale: *the surface of the „opinion triangle”*

Linguistic values make the scale more human friendly:
Decision: *rejectable, opposable, tolerable, acceptable*
Confidence: *sure, very high, high, low, very low, uncertain*

Different types of inferences – different algorithms for aggregation of the assessments of premises

Automatic aggregation of assessments
Communicating the assessment results

- "Small" case study - Successful module test
  - Software module satisfies requirements
  - Argumentation by adequate tests coverage and positive test results
  - Positive results of testing the module by a testing process of adequate scope demonstrates that the module satisfies its requirements
  - Test plan covers requirements
    - Requirements specification
    - Test plan
  - No errors fund by tests
    - Tests report