POLITECHNIKA
GDAŃSKA

Introduction to NOR-STA

Janusz Górski
IAG, Gdańsk University of Technology

IoTSec meeting
NCC, Oslo, 6th June 2018

POLITECHNIKA GDAŃSKA

Information Assurance Group (IAG)

Research group at Faculty of Electronics, Telecommunications and Informatics, Gdansk University of Technoloty (http://iag.pg.gda.pl/)

- 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 asurance and compliance
  - Sice 2014 NOR-STA is a comercial produt offered by ARGEVIDE spin-off of GUT
    - Commercial clients in Oil&Gas, Medical, railways, automotive sectors

ARGEVIDE

Trust-IT and NOR-STA

POLITECHNIKA GDAŃSKA

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.

trust-it

Trust cases

Evidence based arguments

POLITECHNIKA

nor-sta

TCL argument model

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:

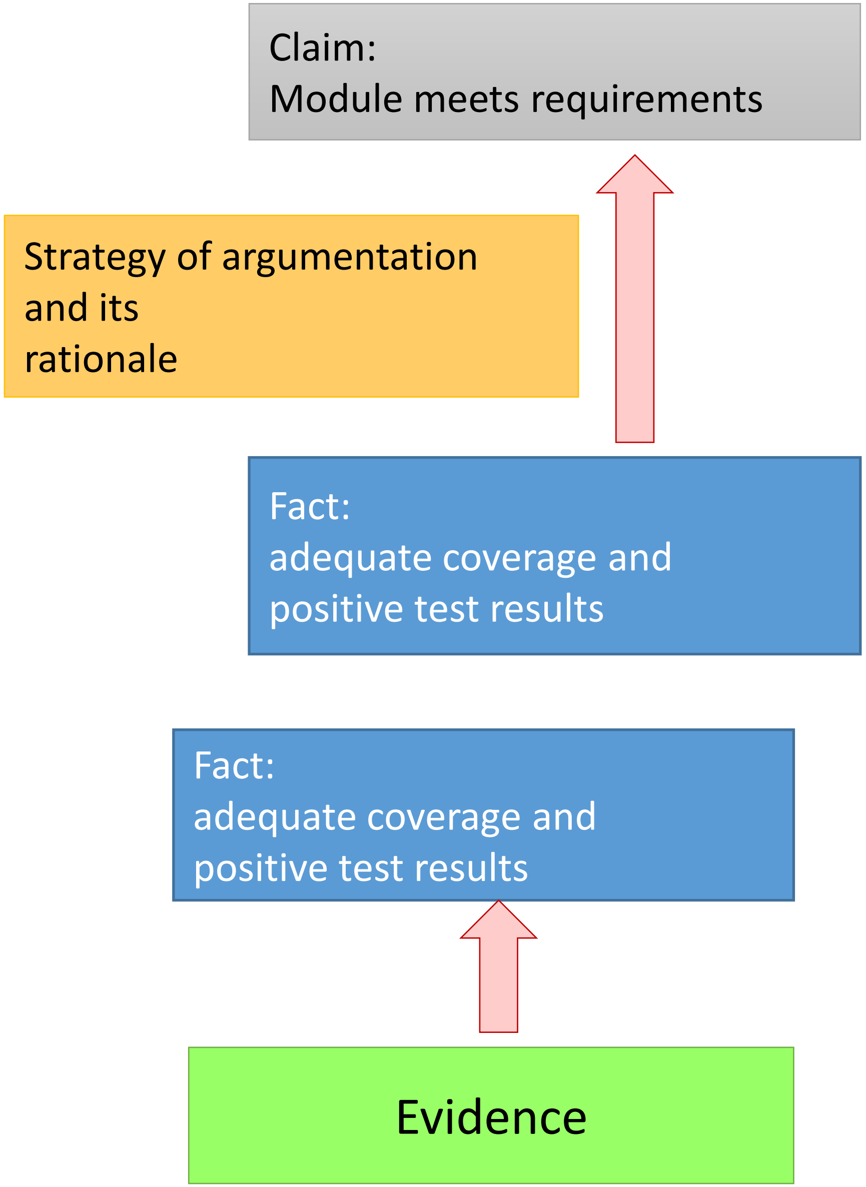
Argumentation by referring to test results and test coverage

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



Claim:
Module meets requirements

Strategy of argumentation and its rationale

Fact:
adequate coverage and positive test results

Fact:
adequate coverage and positive test results

Evidence

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:

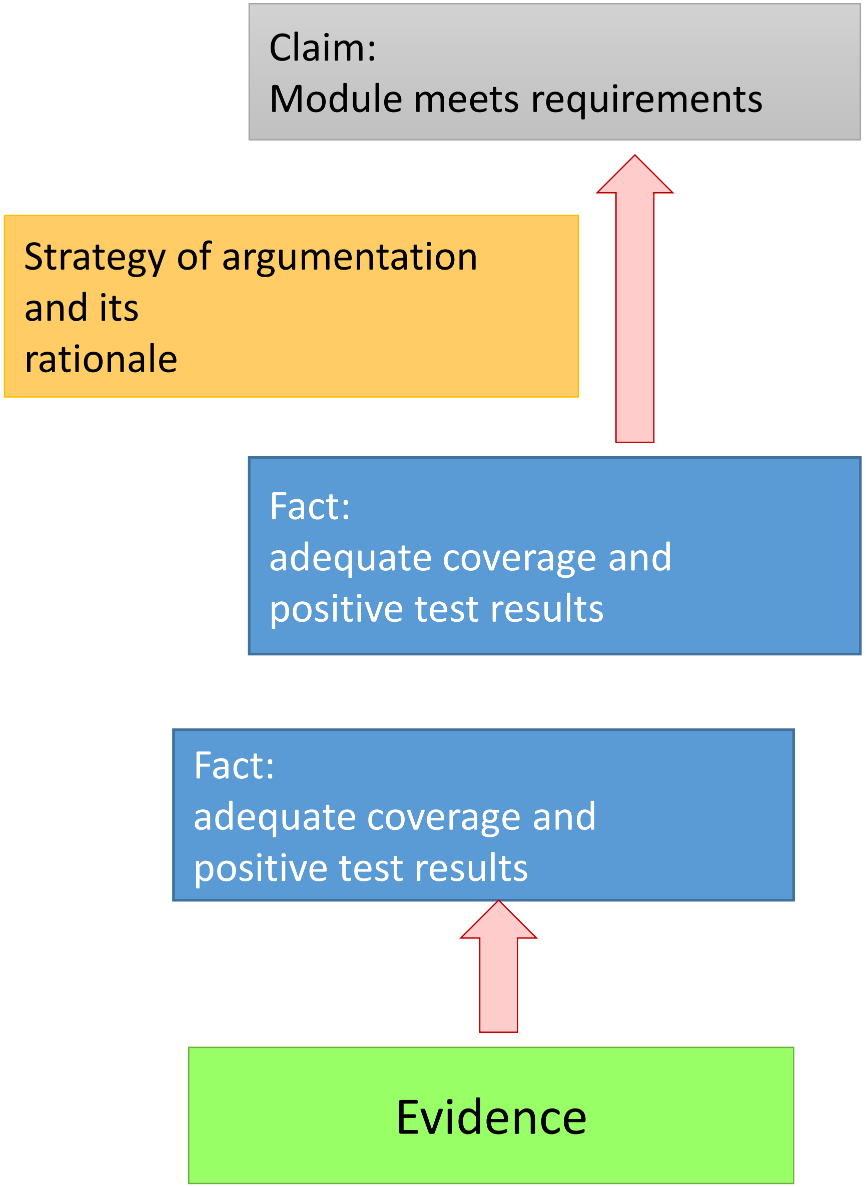
Argumentation by referring to test results and test coverage

Rationale:

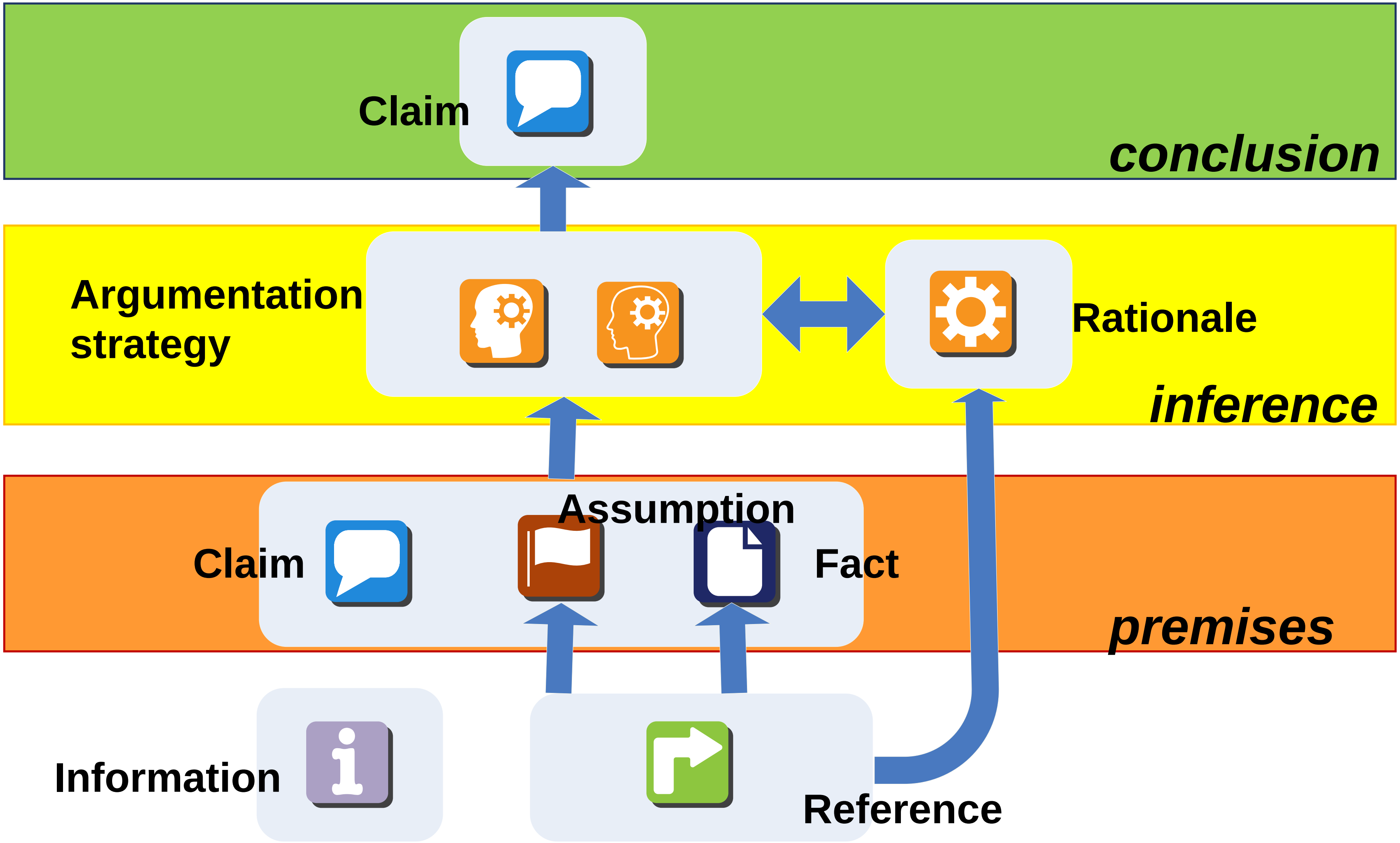
Experience shows that positive results of tests of adequate coverage reliably demonstrate fulfillment of the requirements

Evidence:

Demonstrates a fact about test results and test coverage

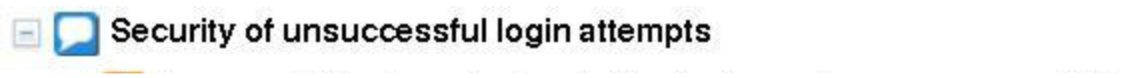

Claim:
Module meets requirements
Strategy of argumentation and its rationale
Fact:
adequate coverage and positive test results
Fact:
adequate coverage and positive test results
Evidence

The argument model



Example security-related argument

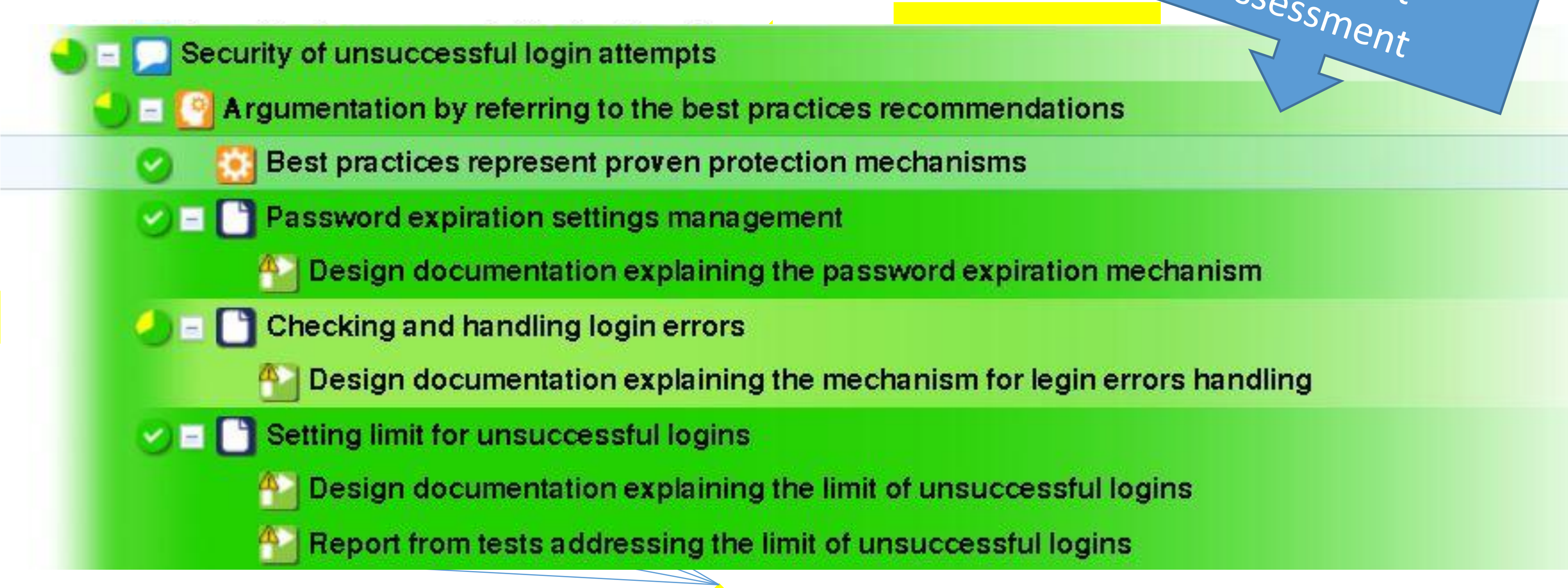
Security argument - example



Security of unsuccessful login attempts

Security argument - example

Argument assessment



- 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 legin errors handling
    - Setting limit for unsuccessful logins
      - Design documentation explaining the limit of unsuccessful logins
      - Report from tests addressing the limit of unsuccessful logins

Facts

References to the evidence that demonstrates facts

Raports from expert reviews and assessments

Design documentation

Tests and measure ments

Simulations

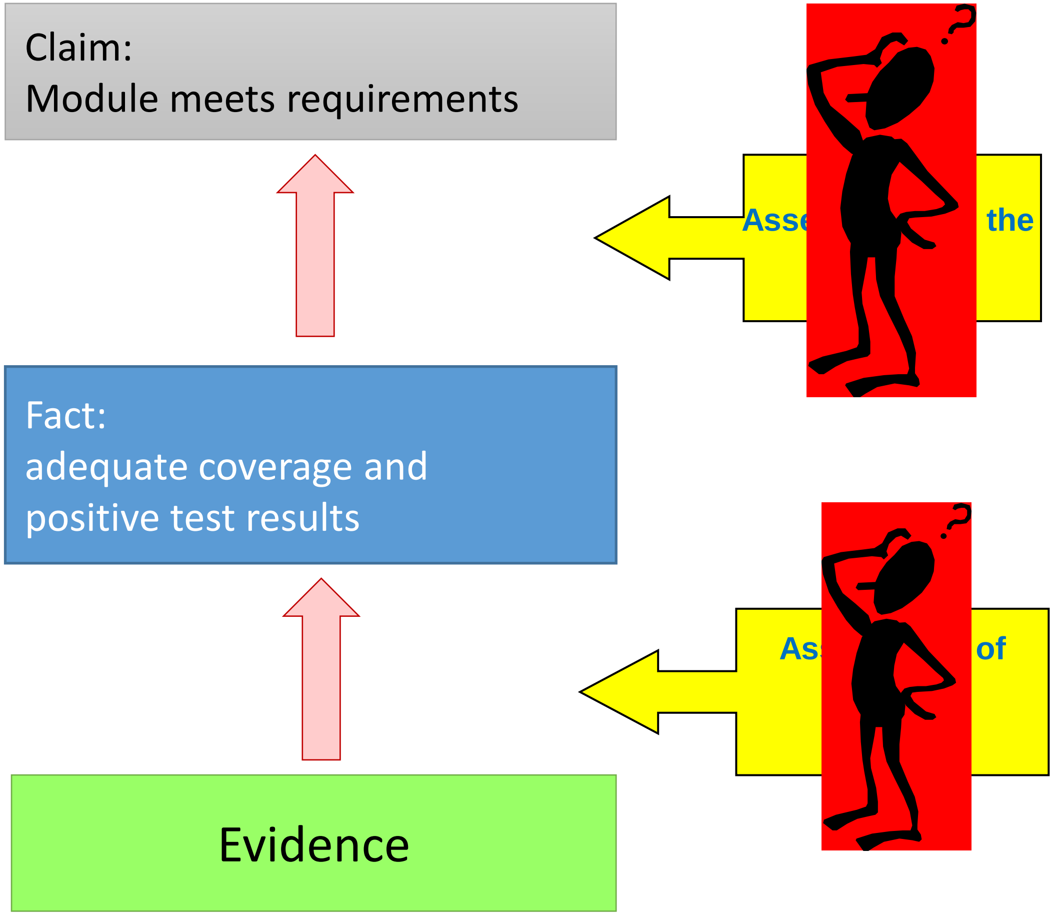
Argument assessment

Successful test *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?

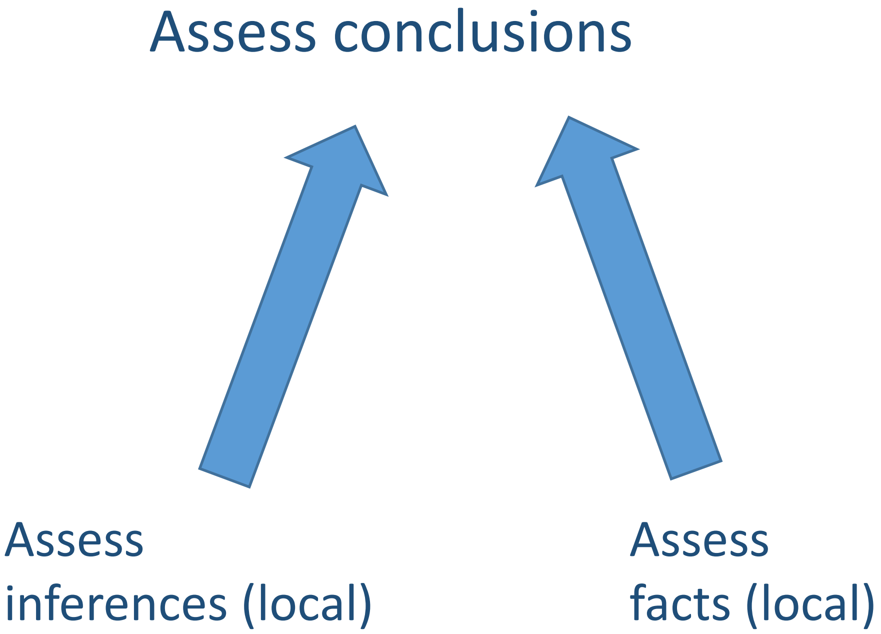


Claim:
Module meets requirements

Fact:
adequate coverage and
positive test results

Evidence

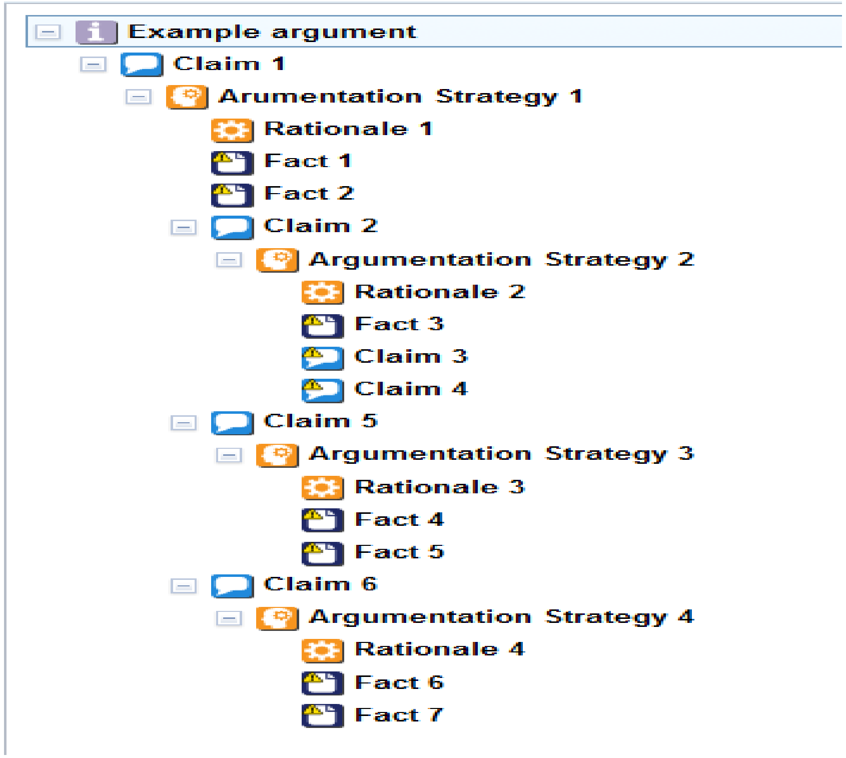
The assessment process



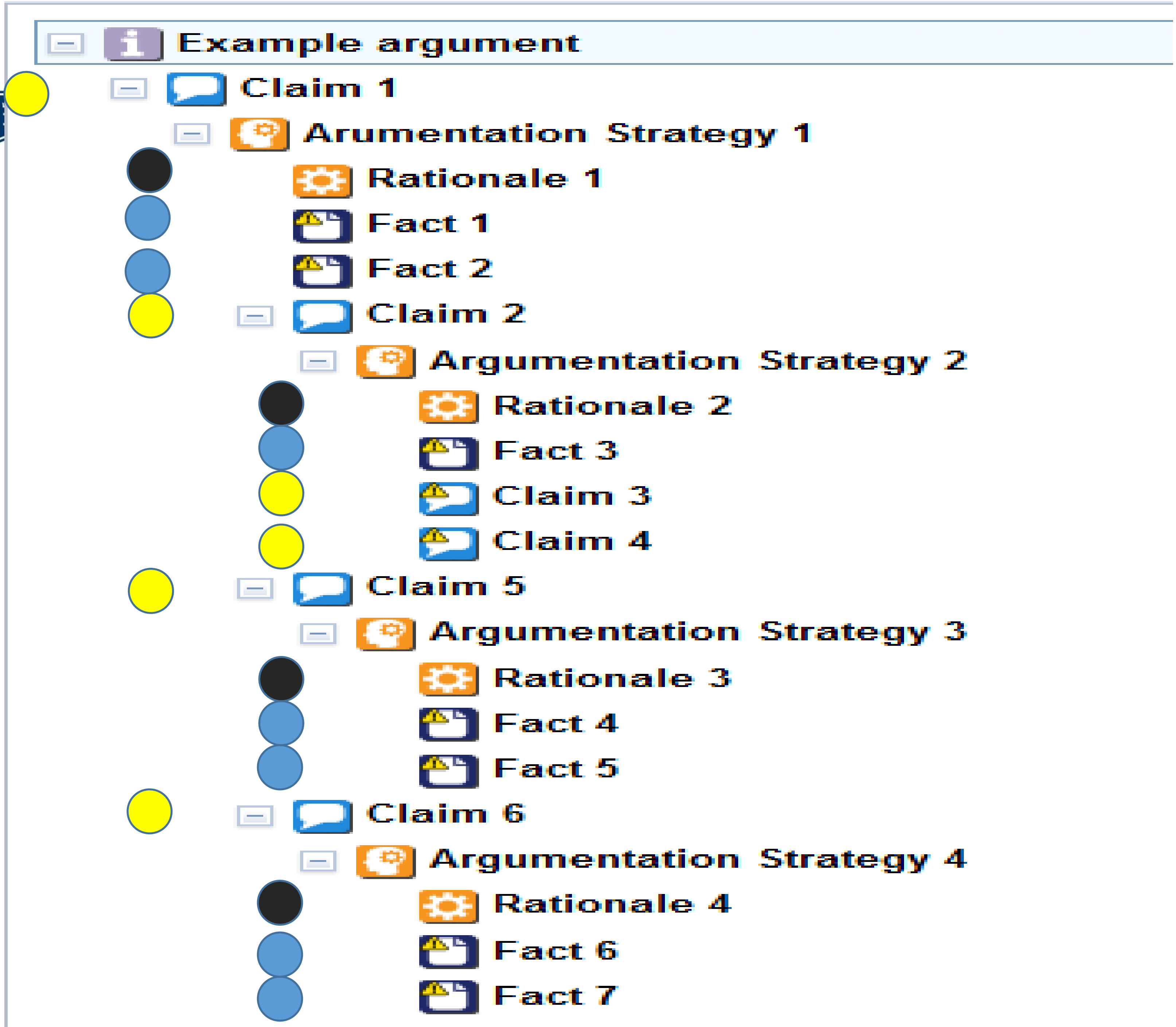
Assess conclusions

Assess inferences (local)

Assess facts (local)



- Example argument
  - Claim 1
    - Arumentation Strategy 1
      - Rationale 1
      - Fact 1
      - Fact 2
      - Claim 2
        - Argumentation Strategy 2
          - Rationale 2
          - Fact 3
          - Claim 3
          - Claim 4
      - Claim 5
        - Argumentation Strategy 3
          - Rationale 3
          - Fact 4
          - Fact 5
      - Claim 6
        - Argumentation Strategy 4
          - Rationale 4
          - Fact 6
          - Fact 7

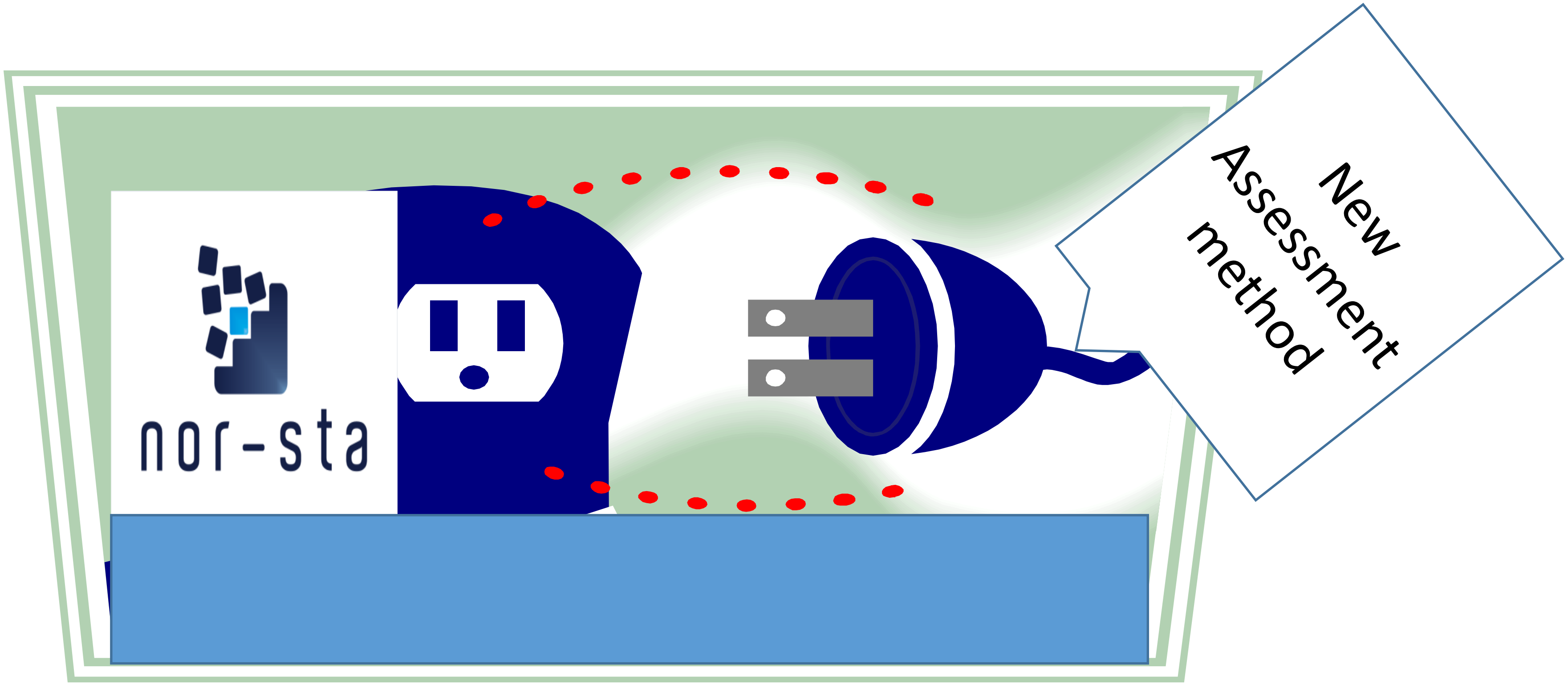


- Example argument
  - Claim 1
    - Arumentation Strategy 1
      - Rationale 1
      - Fact 1
      - Fact 2
      - Claim 2
        - Argumentation Strategy 2
          - Rationale 2
          - Fact 3
          - Claim 3
          - Claim 4
      - Claim 5
        - Argumentation Strategy 3
          - Rationale 3
          - Fact 4
          - Fact 5
      - Claim 6
        - Argumentation Strategy 4
          - Rationale 4
          - Fact 6
          - Fact 7

POLITECHNIKA GDAŃSKA

Assessment methods in NOR-STA

- 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

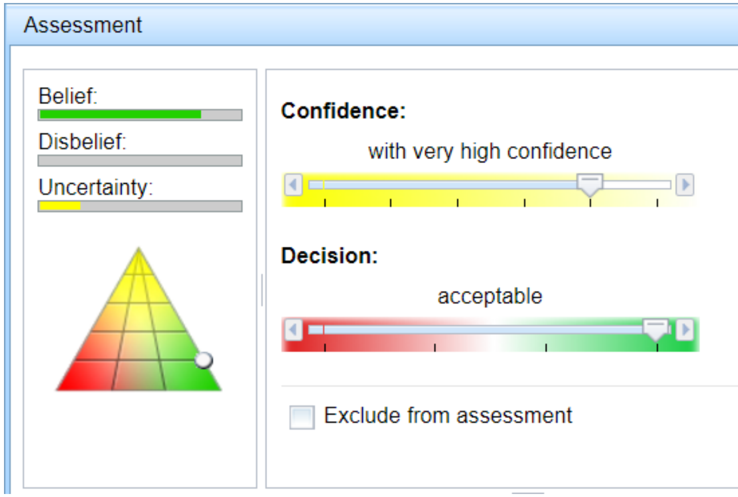


POLITECHNIKA GDAŃSKA

Assessment in NOR-STA

Different methods of argument assessment:

- Dempster-Shafer
- ISO 33000 (SPICE, Automotive SPICE, …)
- Rating scale (numerical)
- Three-level assessment
- and others…



Assessment

Belief:

Disbelief:

Uncertainty:

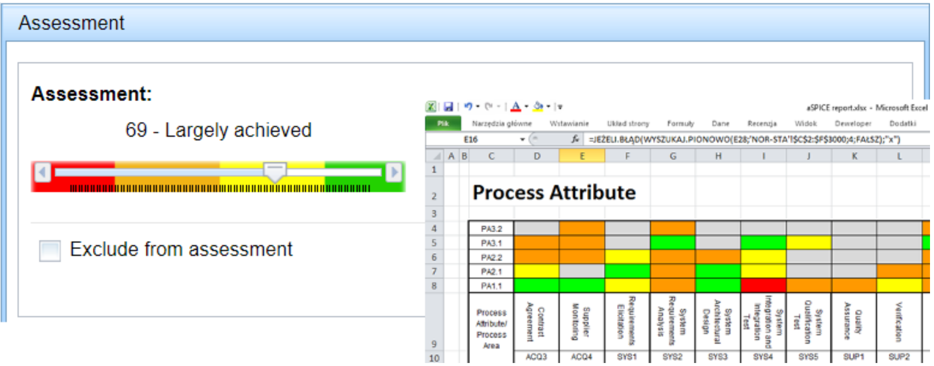
Confidence:

with very high confidence

Decision:

acceptable

□ Exclude from assessment



Assessment

Assessment:

69 - Largely achieved

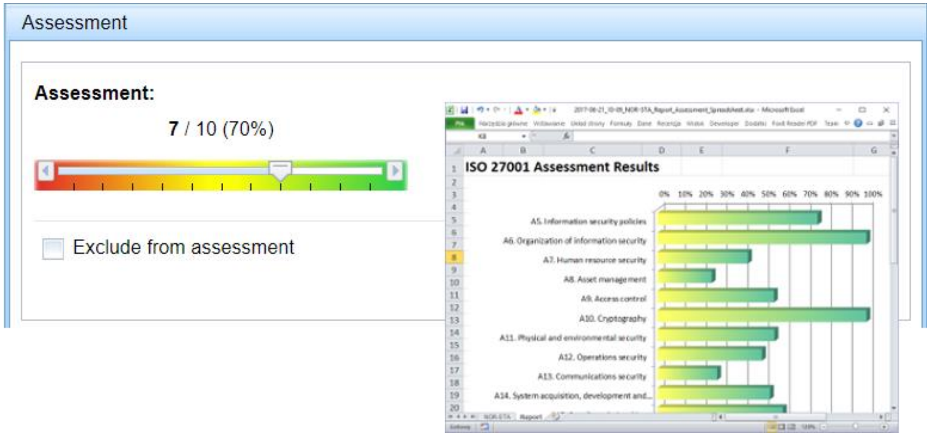
□ Exclude from assessment

aSPICE report.xlsx - Microsoft Excel

E16 =JEŻELI.BŁĄD(WYSZUKAJ.PIONOWO(E28;'NOR-STA'!$C$2:$F$3000;4;FAŁSZ);"x")

Process Attribute

PA3.2	⬜	🟧	⬜	🟧	⬜	⬜	⬜	⬜	⬜
PA3.1	🟧	🟧	⬜	🟩	⬜	🟩	🟨	⬜	⬜
PA2.2	🟧	🟧	🟨	🟧	🟧	🟨	⬜	⬜	⬜
PA2.1	🟨	⬜	🟩	🟧	🟩	🟨	⬜	⬜	🟧
PA1.1	🟩	🟩	🟨	🟧	🟩	🟥	🟧	🟧	🟨
Process Attribute/ Process Area	Contract Agreement	Supplier Monitoring	Requirements Elicitation	System Requirements Analysis	System Architectural Design	System Integration and Integration Test	System Qualification Test	Quality Assurance	Verification
	ACQ3	ACQ4	SYS1	SYS2	SYS3	SYS4	SYS5	SUP1	SUP2



Assessment

Assessment:

7 / 10 (70%)

□ Exclude from assessment

ISO 27001 Assessment Results

0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
A5. Information security policies
A6. Organization of information security
A7. Human resource security
A8. Asset management
A9. Access control
A10. Cryptography
A11. Physical and environmental security
A12. Operations security
A13. Communications security
A14. System acquisition, development and...
NOR-STA
Raport

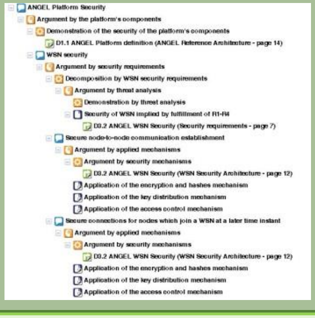
Support for Smart Grid security

SPD argument

S&P&D

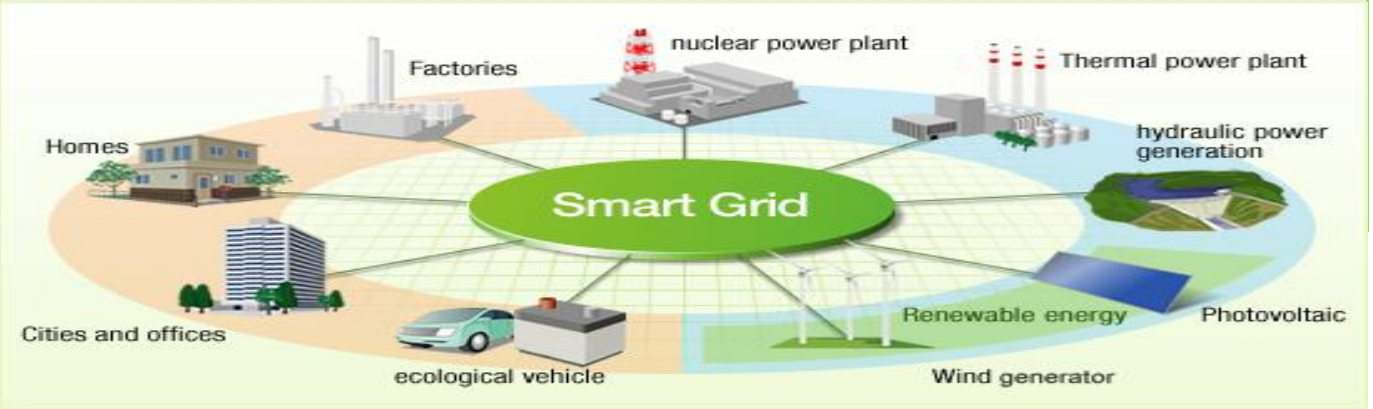
Objectives

Logic decomposition into more specific objectives



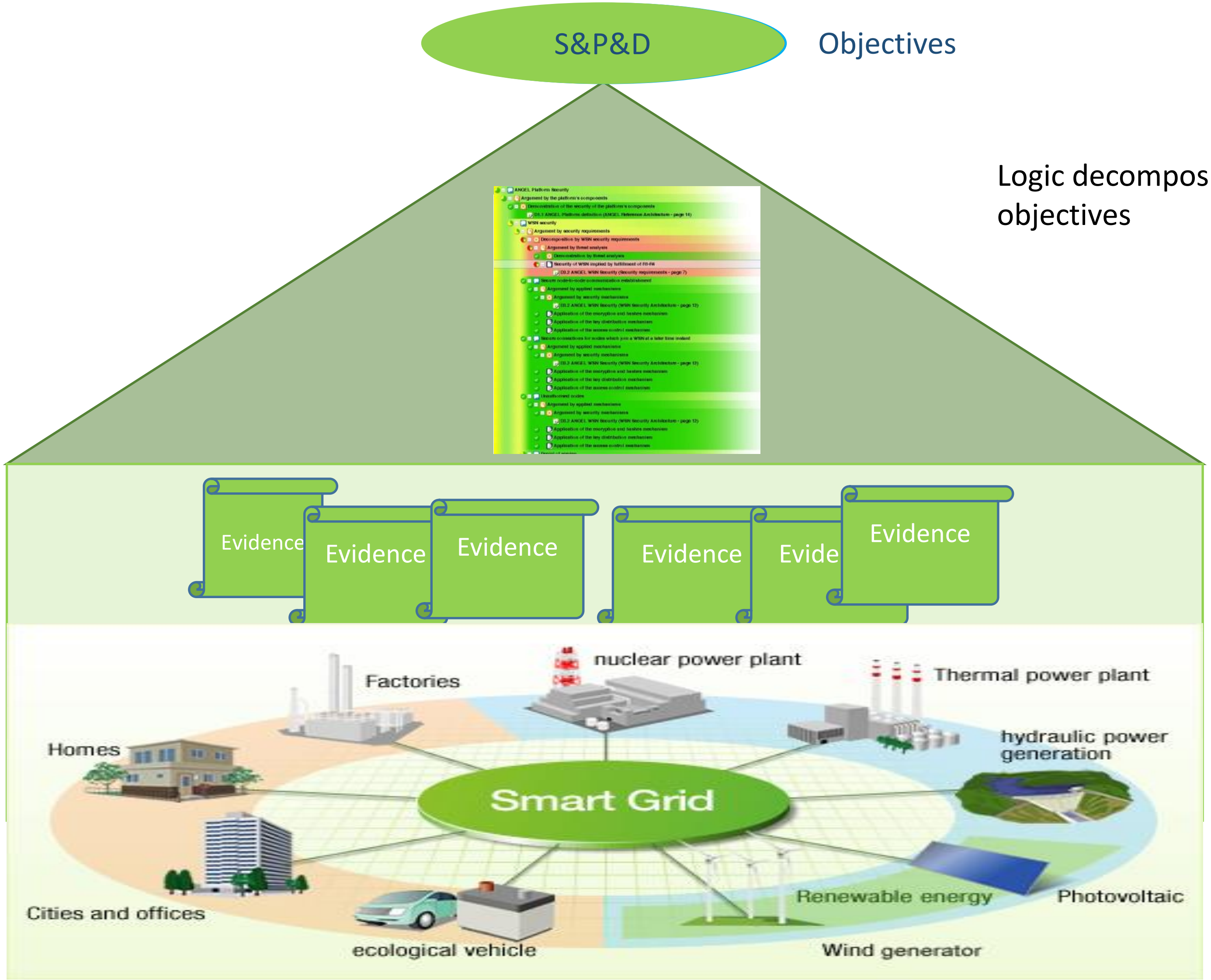
```
ANGEL Platform Security
  Argument by the platform's components
    Demonstration of the security of the platform's components
      D1.1 ANGEL Platform definition (ANGEL Reference Architecture - page 14)
    WSN security
      Argument by security requirements
        Decomposition by WSN security requirements
          Argument by threat analysis
            Demonstration by threat analysis
            Security of WSN implied by fulfillment of R1-R4
              D3.2 ANGEL WSN Security (Security requirements - page 7)
        Secure node-to-node communication establishment
          Argument by applied mechanisms
            Argument by security mechanisms
              D3.2 ANGEL WSN Security (WSN Security Architecture - page 12)
            Application of the encryption and hashes mechanism
            Application of the key distribution mechanism
            Application of the access control mechanism
        Secure connections for nodes which join a WSN at a later time instant
          Argument by applied mechanisms
            Argument by security mechanisms
              D3.2 ANGEL WSN Security (WSN Security Architecture - page 12)
            Application of the encryption and hashes mechanism
            Application of the key distribution mechanism
            Application of the access control mechanism
```

Analytical and measurement leyer – collecting evidence that demonstrates objectives



Smart grid of interest

SPD argument



- ANGEL Platform Security
  - Argument by the platform's components
    - Demonstration of the security of the platform's components
      - D1.1 ANGEL Platform definition (ANGEL Reference Architecture - page 14)
    - WSN security
      - Argument by security requirements
        - Decomposition by WSN security requirements
          - Argument by threat analysis
            - Demonstration by threat analysis
            - Security of WSN implied by fulfillment of R1-R4
              - D3.2 ANGEL WSN Security (Security requirements - page 7)
        - Secure node-to-node communication establishment
          - Argument by applied mechanisms
            - Argument by security mechanisms
              - D3.2 ANGEL WSN Security (WSN Security Architecture - page 12)
            - Application of the encryption and hashes mechanism
            - Application of the key distribution mechanism
            - Application of the access control mechanism
        - Secure connections for nodes which join a WSN at a later time instant
          - Argument by applied mechanisms
            - Argument by security mechanisms
              - D3.2 ANGEL WSN Security (WSN Security Architecture - page 12)
            - Application of the encryption and hashes mechanism
            - Application of the key distribution mechanism
            - Application of the access control mechanism
        - Unauthorised nodes
          - Argument by applied mechanisms
            - Argument by security mechanisms
              - D3.2 ANGEL WSN Security (WSN Security Architecture - page 12)
            - Application of the encryption and hashes mechanism
            - Application of the key distribution mechanism
            - Application of the access control mechanism
        - Denial of service

Objectives

Logic decomposition into more specific objectives

Analytical and measurement leyer – collecting evidence that demonstrates objectives

Smart grid of interest

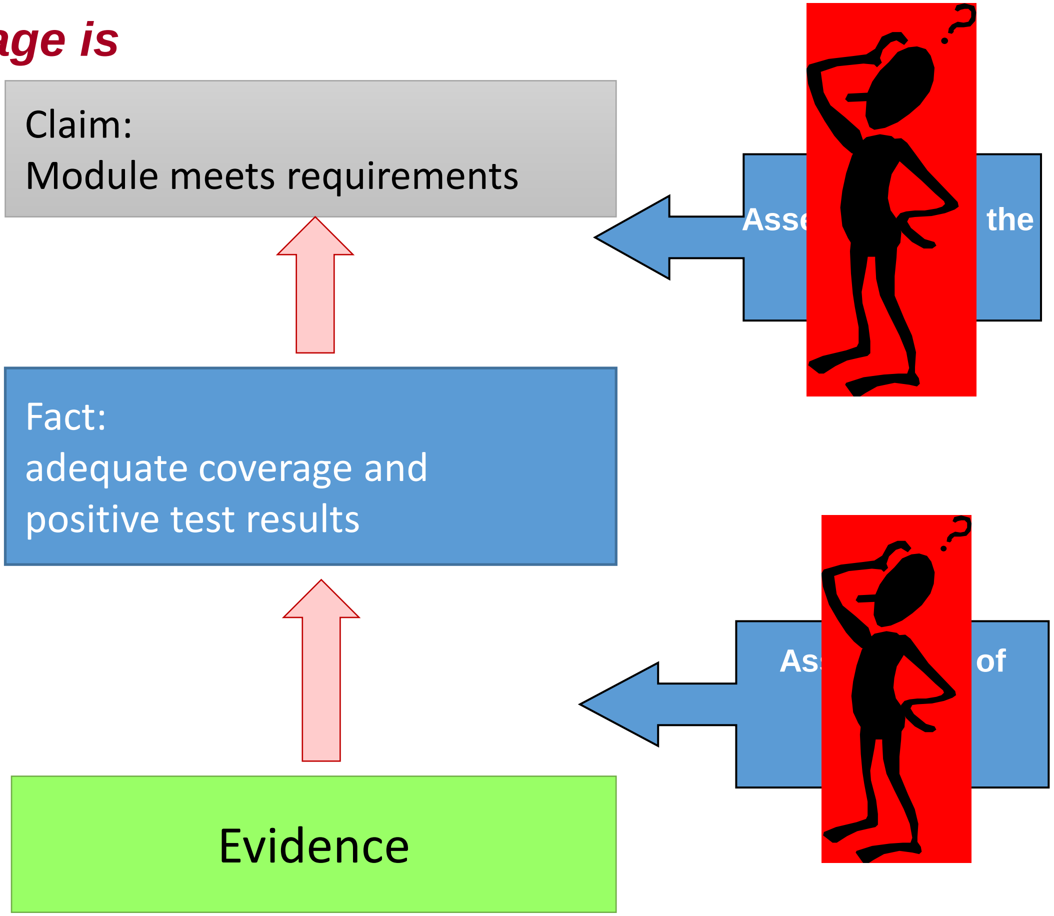
Argument Assessment *based on* *Dempster-Shafer* *belief model*

„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

  Acceptance Uncertainty Rejection

Assessment of inference

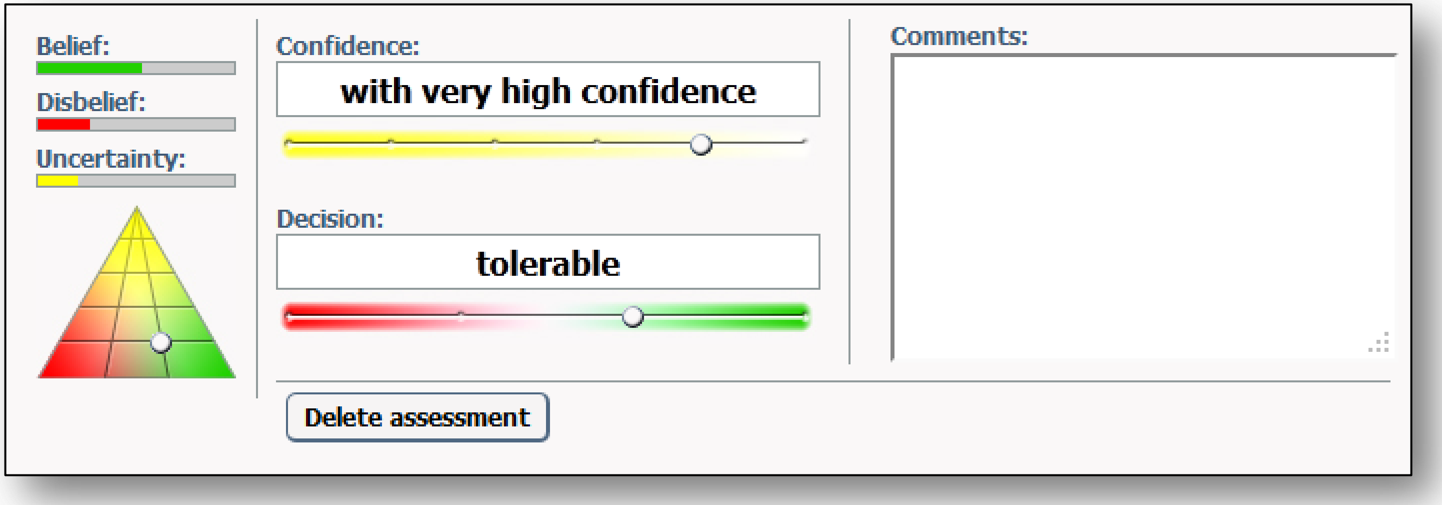
- ‘if we have positive test results and adequate tests coverage, then the module meets its requirements’

  How reliable is such reasoning?

- Assessment

  Acceptance Uncertainty Rejection

User interface



Confidence: with very high confidence

Decision: tolerable

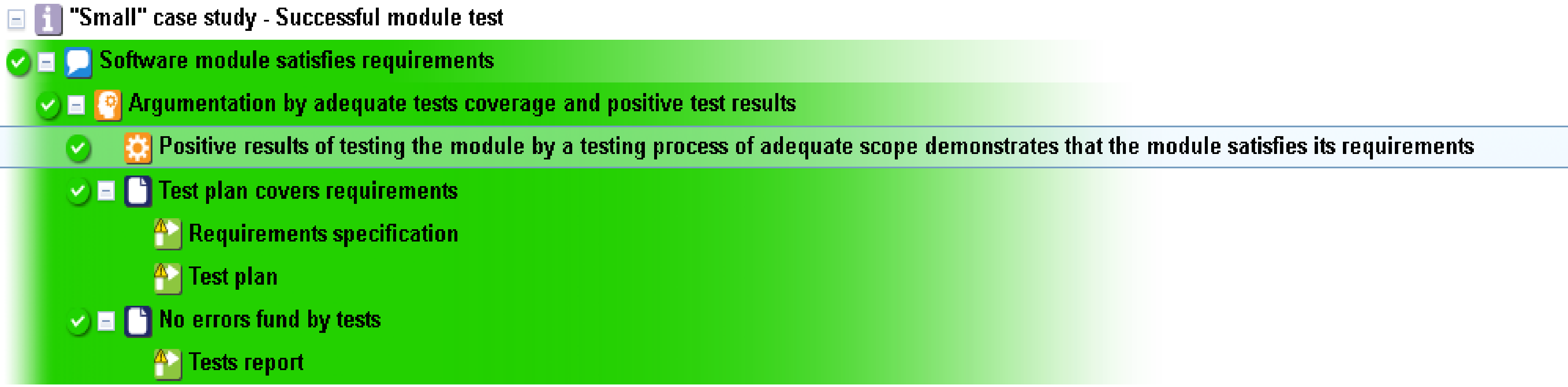
Scale: *the surface of the „opinion triangle”*

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