Supporting Expert Assessment of Argument Structures in Trust Cases

Łukasz Cyra

Janusz Górski

Information Assurance Group

Department of Software Engineering

Gdańsk University of Technology, Poland

INFORMATION ASSURANCE GROUP

Contents

- What is ‘trust case’?
- The Trust-IT framework
- Example argument
- The appraisal scale
- Appraisal example
- The aggregation mechanism
- Conclusions

Trust *vs* Trustworthiness

- **Trust**
  - ***trust*** **is the notion referring to a belief in some postulated property of a trusted object considered in a specific context**
- **Trustworthiness**
  - ***Trustworthiness*** **is the notion referring to the *justification* explaining *why* we should trust that the object exhibits the posulated property in this context**
- **Trustworthiness** *can imply* **Trust**

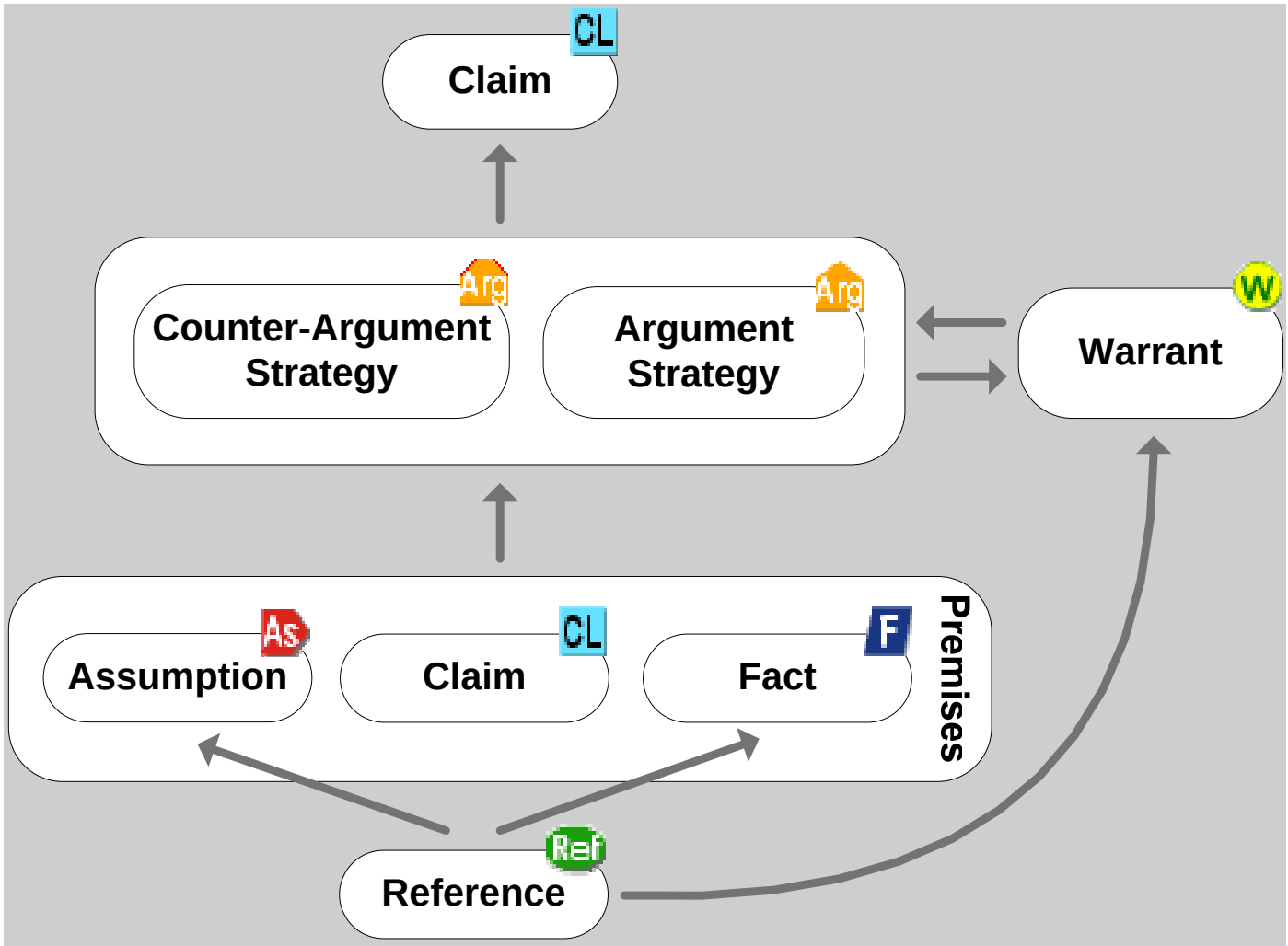
Trust Case

Trust Case is an argument that provides a satisfactory (from a selected viewpoint) justification for a specified set of properties to make a judgement about the trustworthiness of the chosen object

Trust Case integrates argumentation with the evidence that supports this argumentation

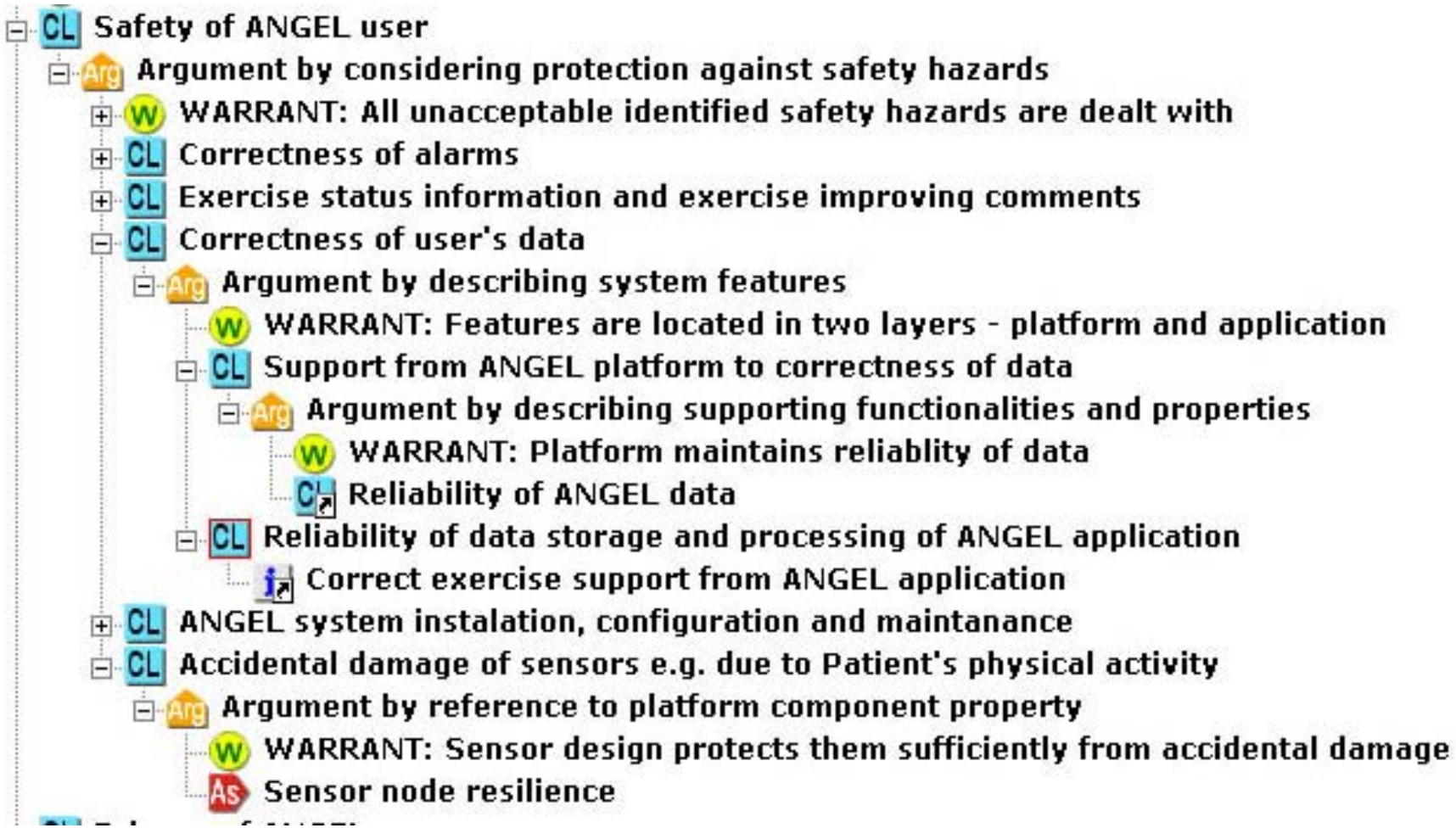
The notion of *Trust Case* is a generalization of the common notion of *Safety Case*

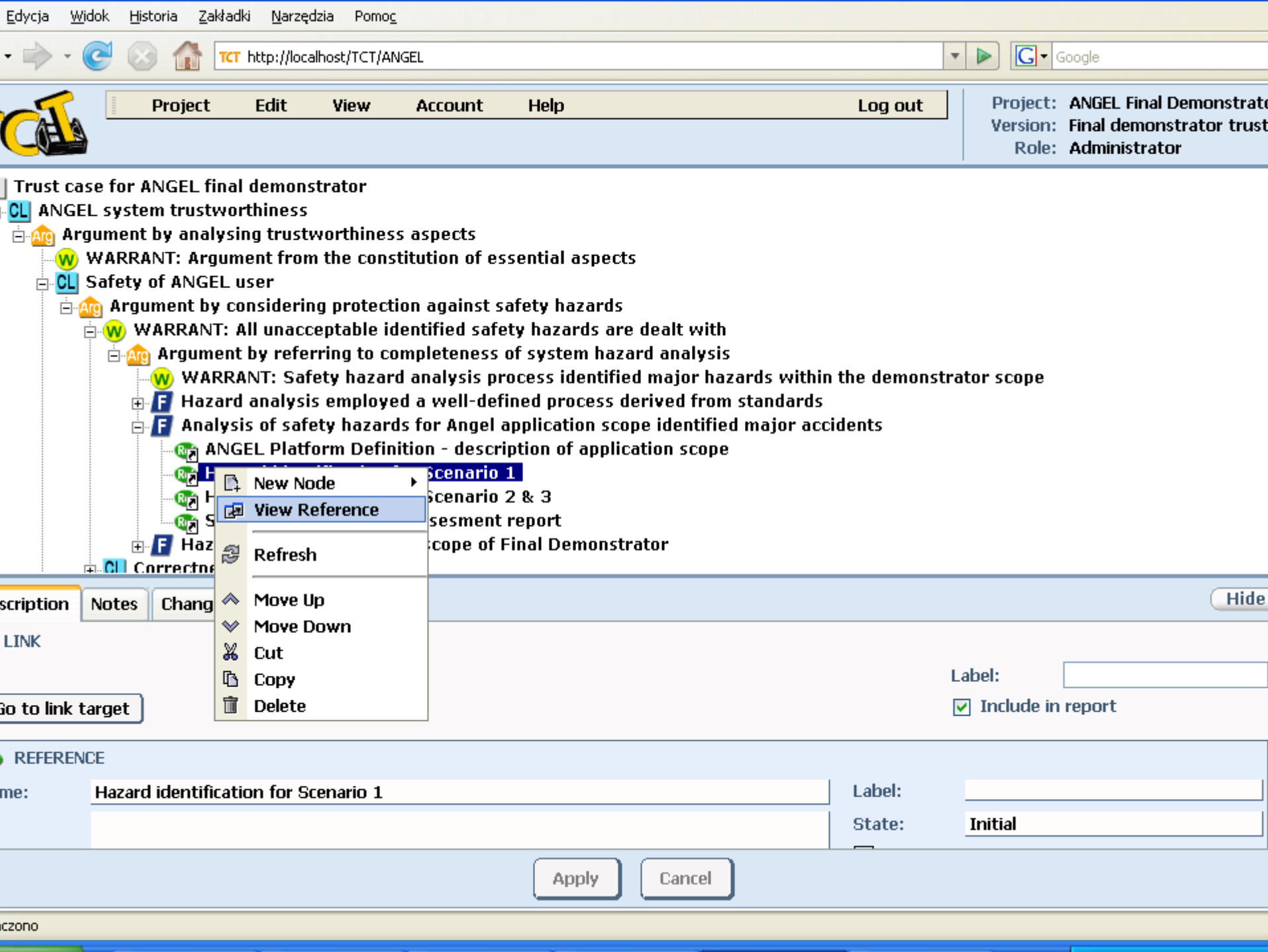
Language for representing trust cases

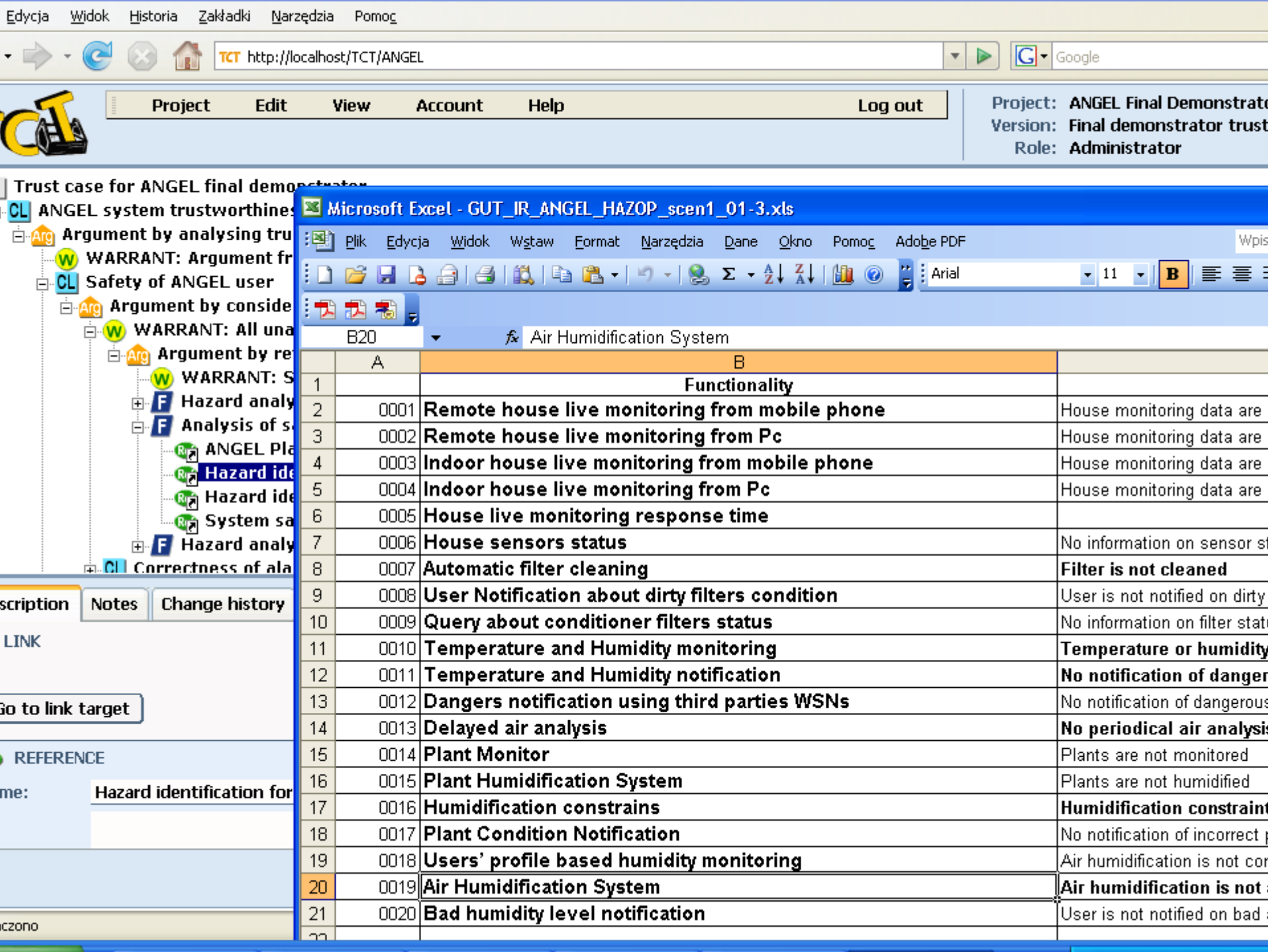


INFORMATION ASSURANCE GROUP

Trust Case example




Edycja Widok Historia Zakładki Narzędzia Pomoc
TCT http://localhost/TCT/ANGEL
Google
Project Edit View Account Help Log out
Project: ANGEL Final Demonstrato
Version: Final demonstrator trust
Role: Administrator
Trust case for ANGEL final demonstrator
ANGEL system trustworthiness
Argument by analysing trustworthiness aspects
WARRANT: Argument from the constitution of essential aspects
Safety of ANGEL user
Argument by considering protection against safety hazards
WARRANT: All unacceptable identified safety hazards are dealt with
Argument by referring to completeness of system hazard analysis
WARRANT: Safety hazard analysis process identified major hazards within the demonstrator scope
Hazard analysis employed a well-defined process derived from standards
Analysis of safety hazards for Angel application scope identified major accidents
ANGEL Platform Definition - description of application scope
New Node
View Reference
Refresh
Move Up
Move Down
Cut
Copy
Delete
scription
Notes
Chang
Hide
LINK
Go to link target
Label:
Include in report
REFERENCE
me:
Hazard identification for Scenario 1
Label:
State:
Initial
Apply
Cancel


Edycja Widok Historia Zakładki Narzędzia Pomoc
http://localhost/TCT/ANGEL
Google
Project Edit View Account Help Log out
Project: ANGEL Final Demonstrat
Version: Final demonstrator trust
Role: Administrator
Trust case for ANGEL final demonstrator
ANGEL system trustworthines
Argument by analysing tru
WARRANT: Argument fr
Safety of ANGEL user
Argument by conside
WARRANT: All una
Argument by re
WARRANT: S
Hazard analy
Analysis of s
ANGEL Pla
Hazard ide
Hazard ide
System sa
Hazard analy
Correctness of ala
scription
Notes
Change history
LINK
Go to link target
REFERENCE
me:
Hazard identification for
Microsoft Excel - GUT_IR_ANGEL_HAZOP_scen1_01-3.xls
Plik Edycja Widok Wstaw Format Narzędzia Dane Okno Pomoc Adobe PDF
Arial
11
B20
Air Humidification System
A
B
1 Functionality
2 0001 Remote house live monitoring from mobile phone House monitoring data are
3 0002 Remote house live monitoring from Pc House monitoring data are
4 0003 Indoor house live monitoring from mobile phone House monitoring data are
5 0004 Indoor house live monitoring from Pc House monitoring data are
6 0005 House live monitoring response time
7 0006 House sensors status No information on sensor st
8 0007 Automatic filter cleaning Filter is not cleaned
9 0008 User Notification about dirty filters condition User is not notified on dirty
10 0009 Query about conditioner filters status No information on filter statu
11 0010 Temperature and Humidity monitoring Temperature or humidity
12 0011 Temperature and Humidity notification No notification of danger
13 0012 Dangers notification using third parties WSNs No notification of dangerous
14 0013 Delayed air analysis No periodical air analysis
15 0014 Plant Monitor Plants are not monitored
16 0015 Plant Humidification System Plants are not humidified
17 0016 Humidification constrains Humidification constraint
18 0017 Plant Condition Notification No notification of incorrect
19 0018 Users' profile based humidity monitoring Air humidification is not cor
20 0019 Air Humidification System Air humidification is not
21 0020 Bad humidity level notification User is not notified on bad

Language for representing trust cases

Scenarios for using trust cases

Trust case processes

Templates Patterns

Trust case system

Trust-IT framework

Problem

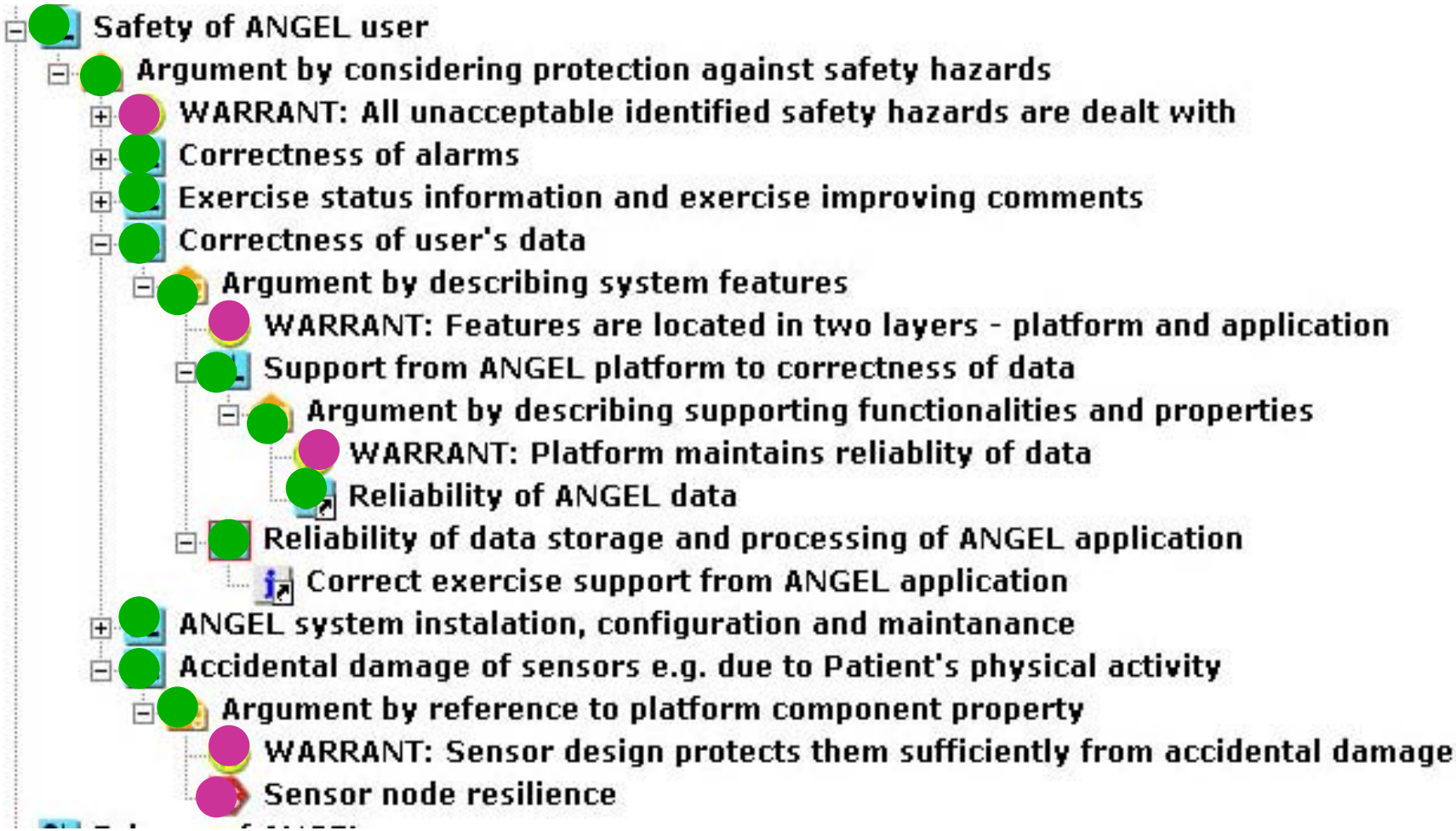
How to assess the ‘strength’ of the argument in a trust case and how to communicate it to the relevant stakeholders

Solution

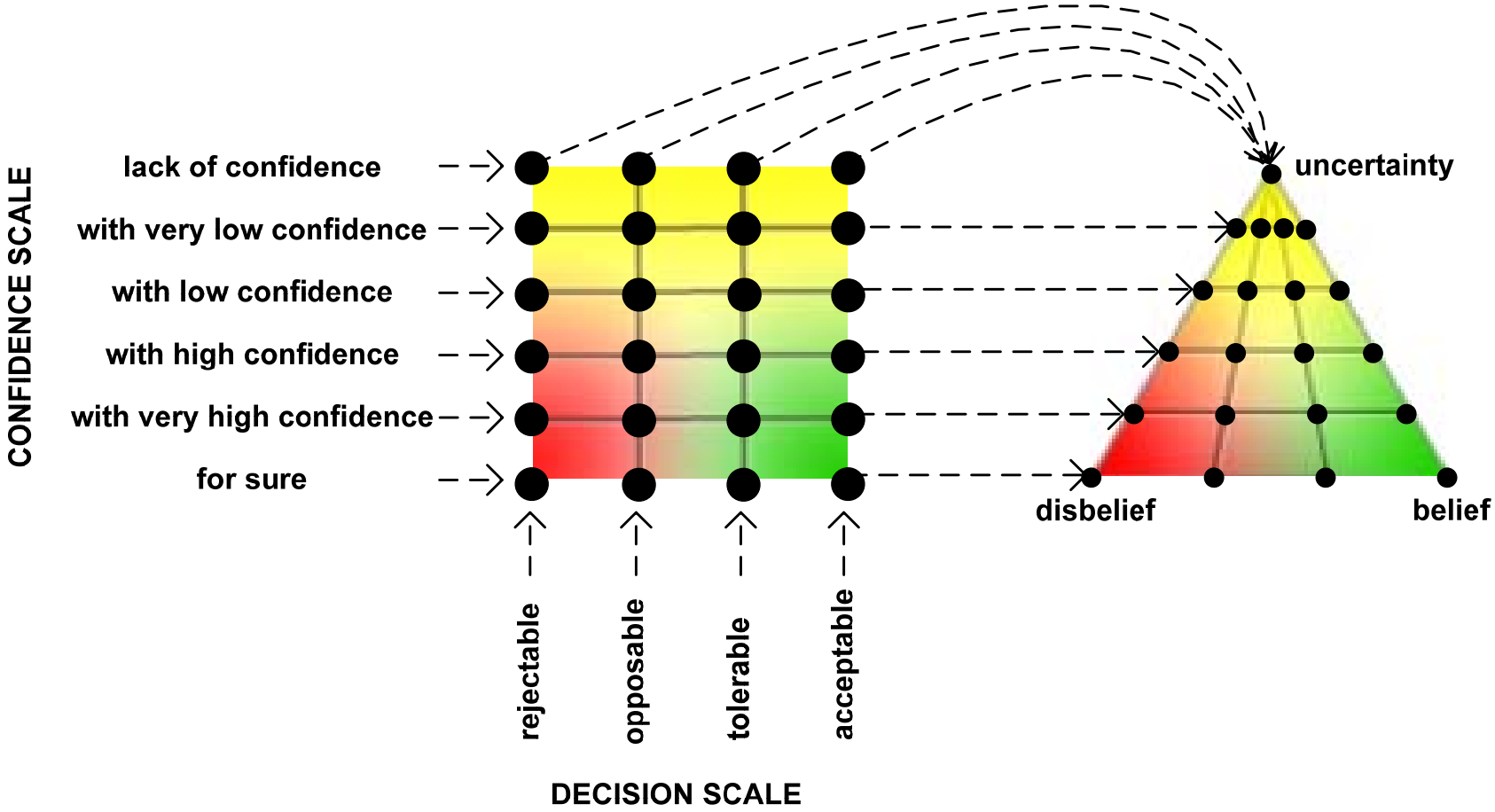
Provide an argumentation appraisal mechanism which starts from assessments of the facts and inferences in the argument and aggregates them to an assessment of the topmost claim

INFORMATION ASSURANCE GROUP

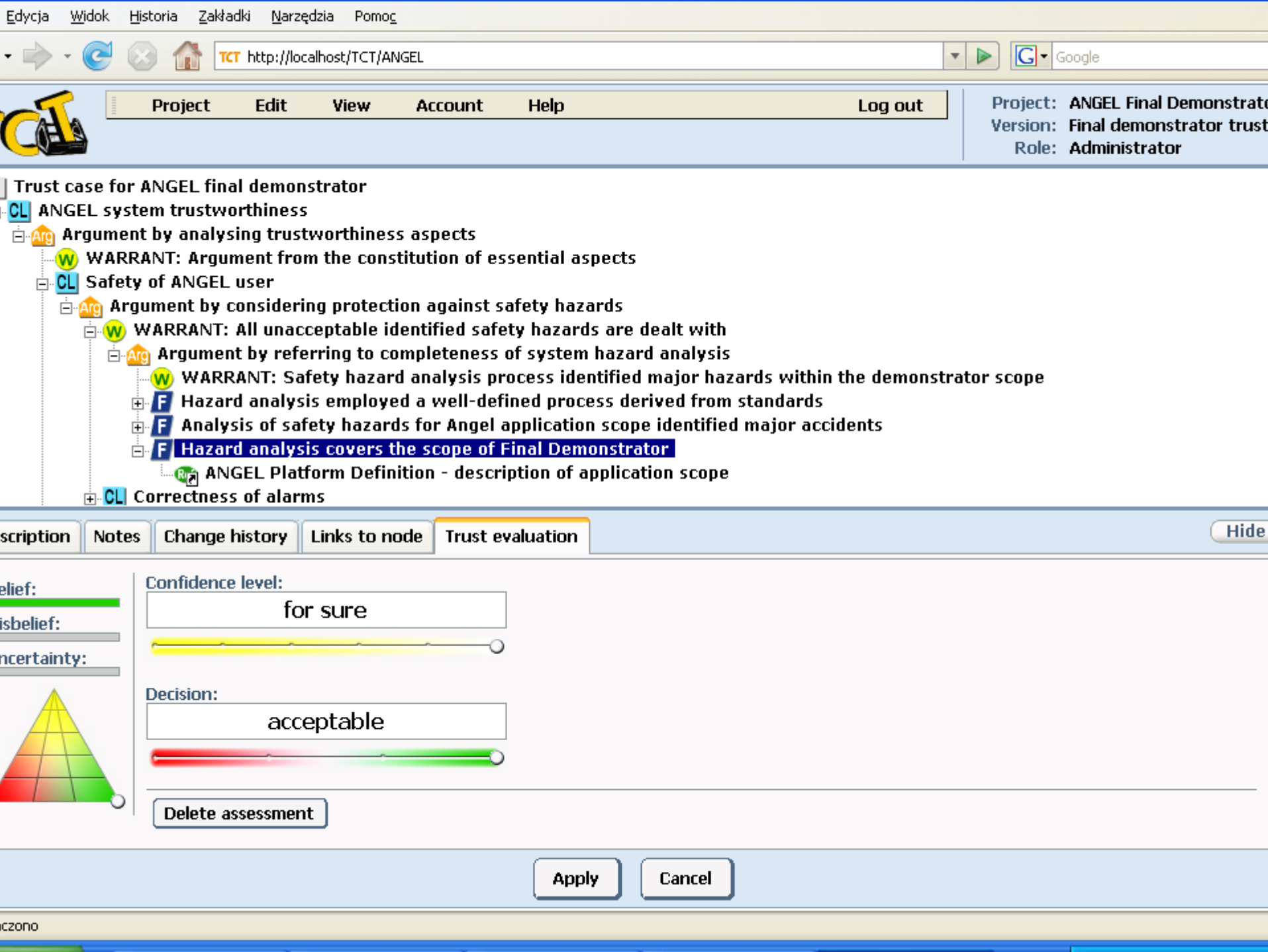
Trust Case example

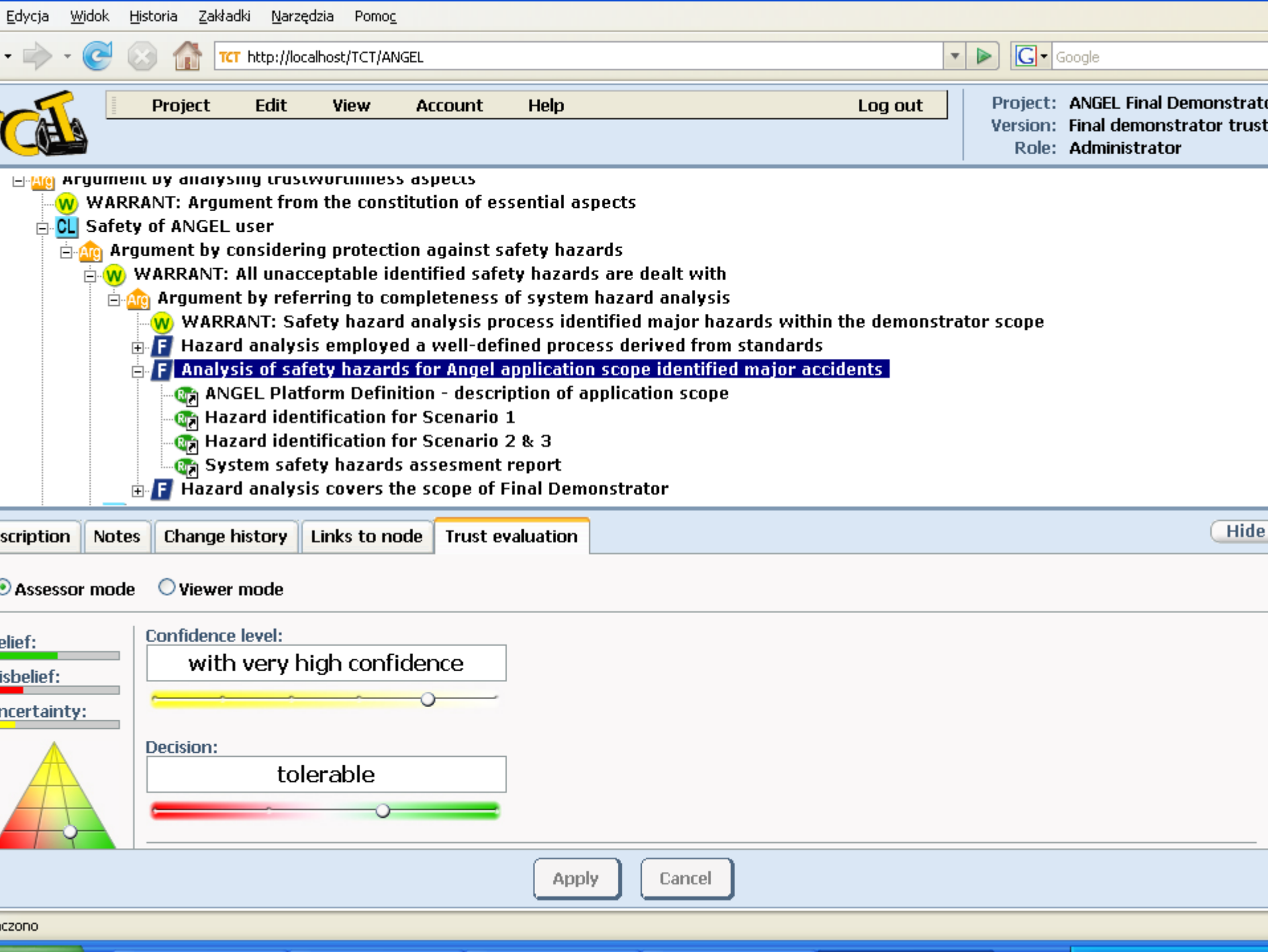


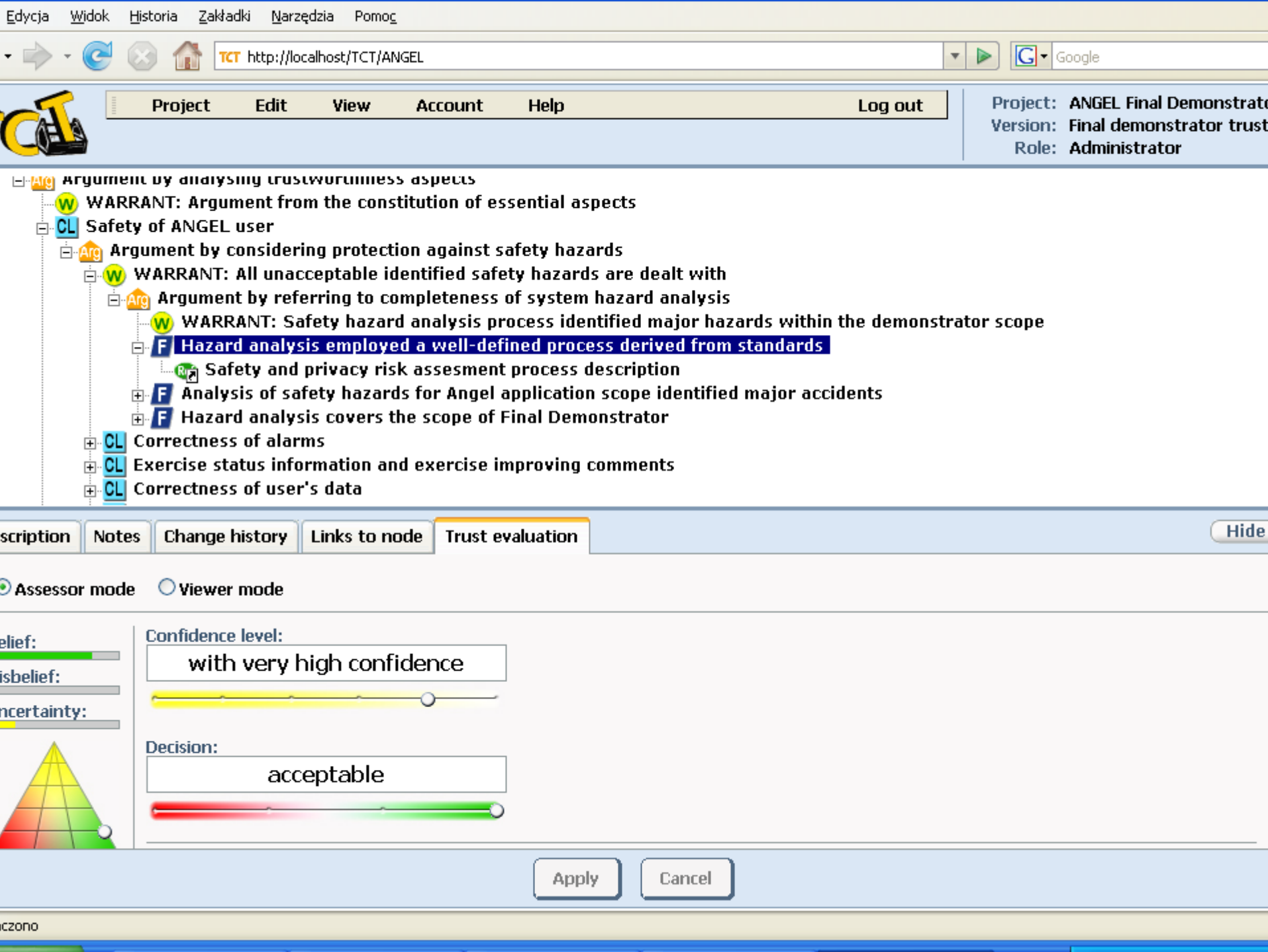
The appraisal scale

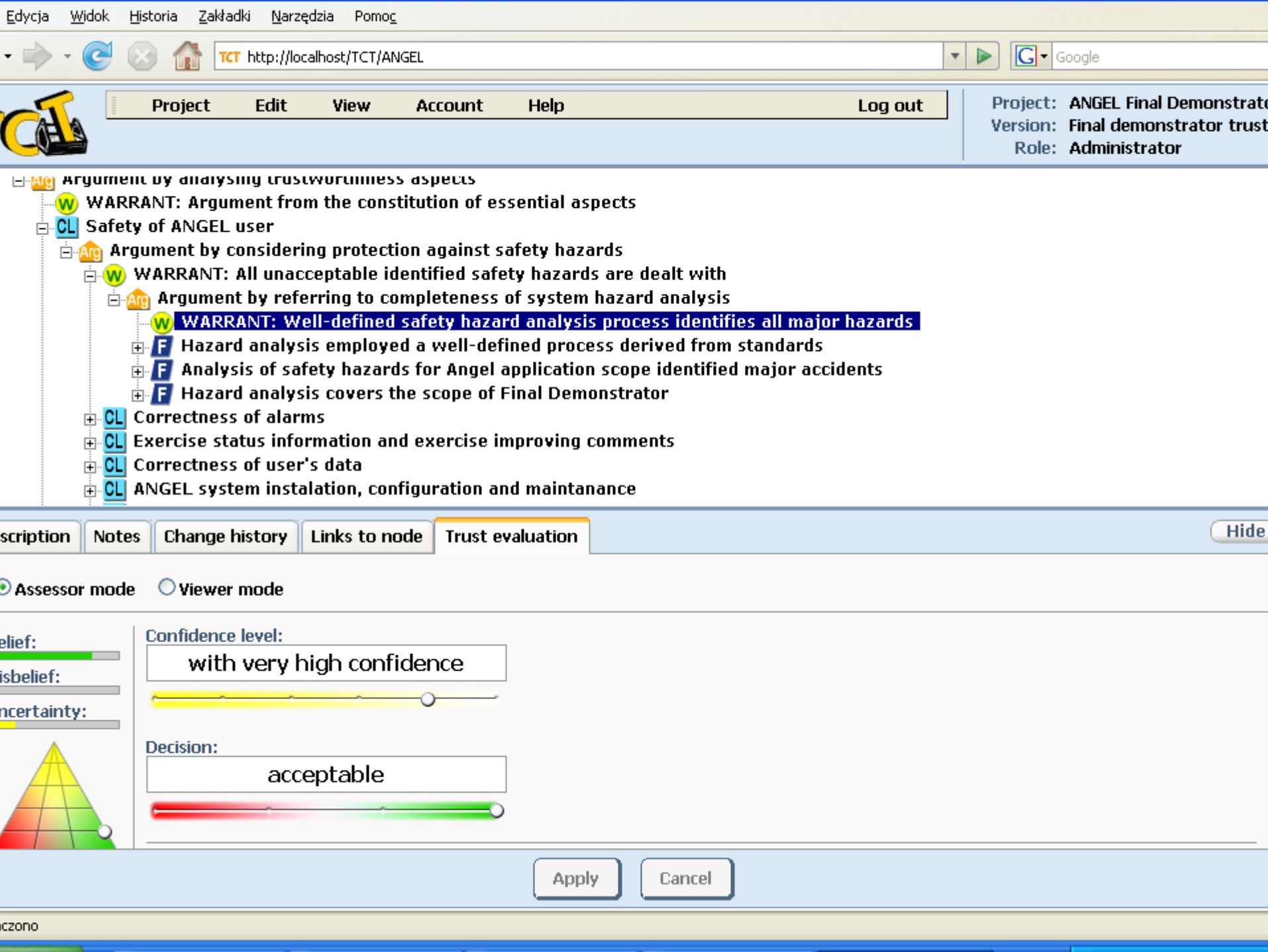


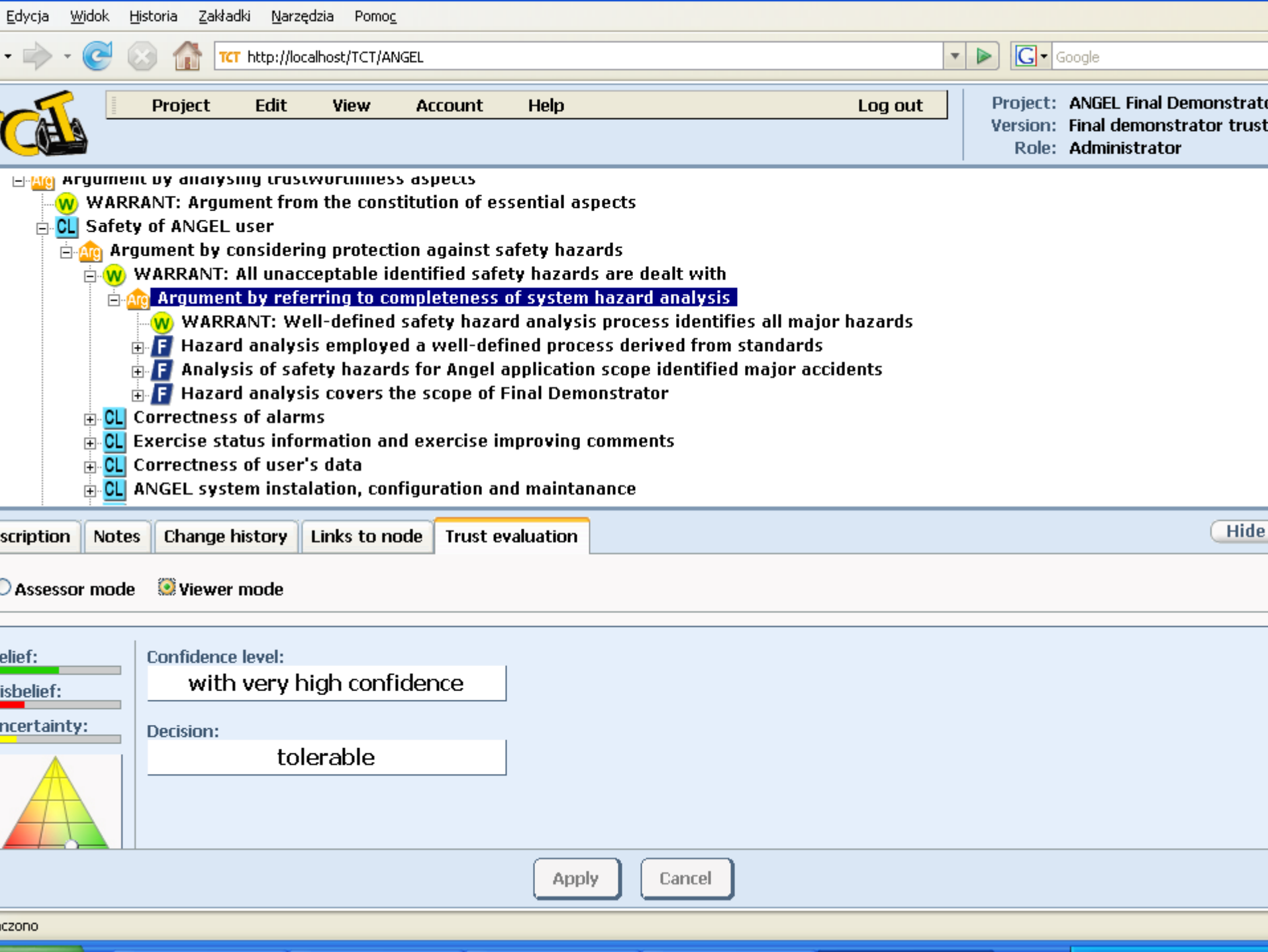
Appraisal example

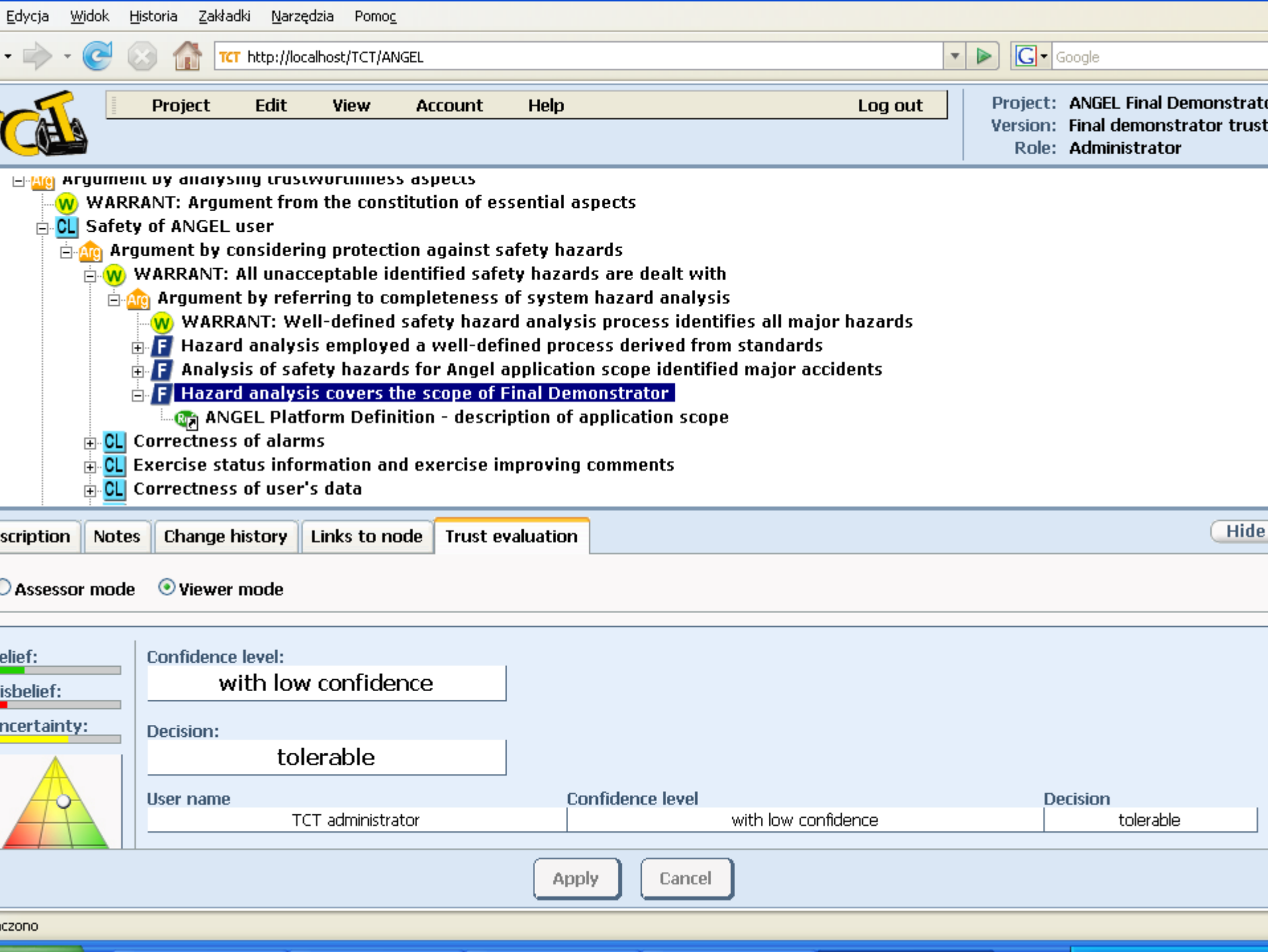

Edycja Widok Historia Zakładki Narzędzia Pomoc
TCT http://localhost/TCT/ANGEL
Google
Project Edit View Account Help Log out
Project: ANGEL Final Demonstrato
Version: Final demonstrator trust
Role: Administrator
Trust case for ANGEL final demonstrator
CL ANGEL system trustworthiness
Arg Argument by analysing trustworthiness aspects
W WARRANT: Argument from the constitution of essential aspects
CL Safety of ANGEL user
Arg Argument by considering protection against safety hazards
W WARRANT: All unacceptable identified safety hazards are dealt with
Arg Argument by referring to completeness of system hazard analysis
W WARRANT: Safety hazard analysis process identified major hazards within the demonstrator scope
F Hazard analysis employed a well-defined process derived from standards
F Analysis of safety hazards for Angel application scope identified major accidents
F Hazard analysis covers the scope of Final Demonstrator
ANGEL Platform Definition - description of application scope
CL Correctness of alarms
scription
Notes
Change history
Links to node
Trust evaluation
Hide
elief:
isbelief:
ncertainty:
Confidence level:
for sure
Decision:
acceptable
Delete assessment
Apply
Cancel
czono

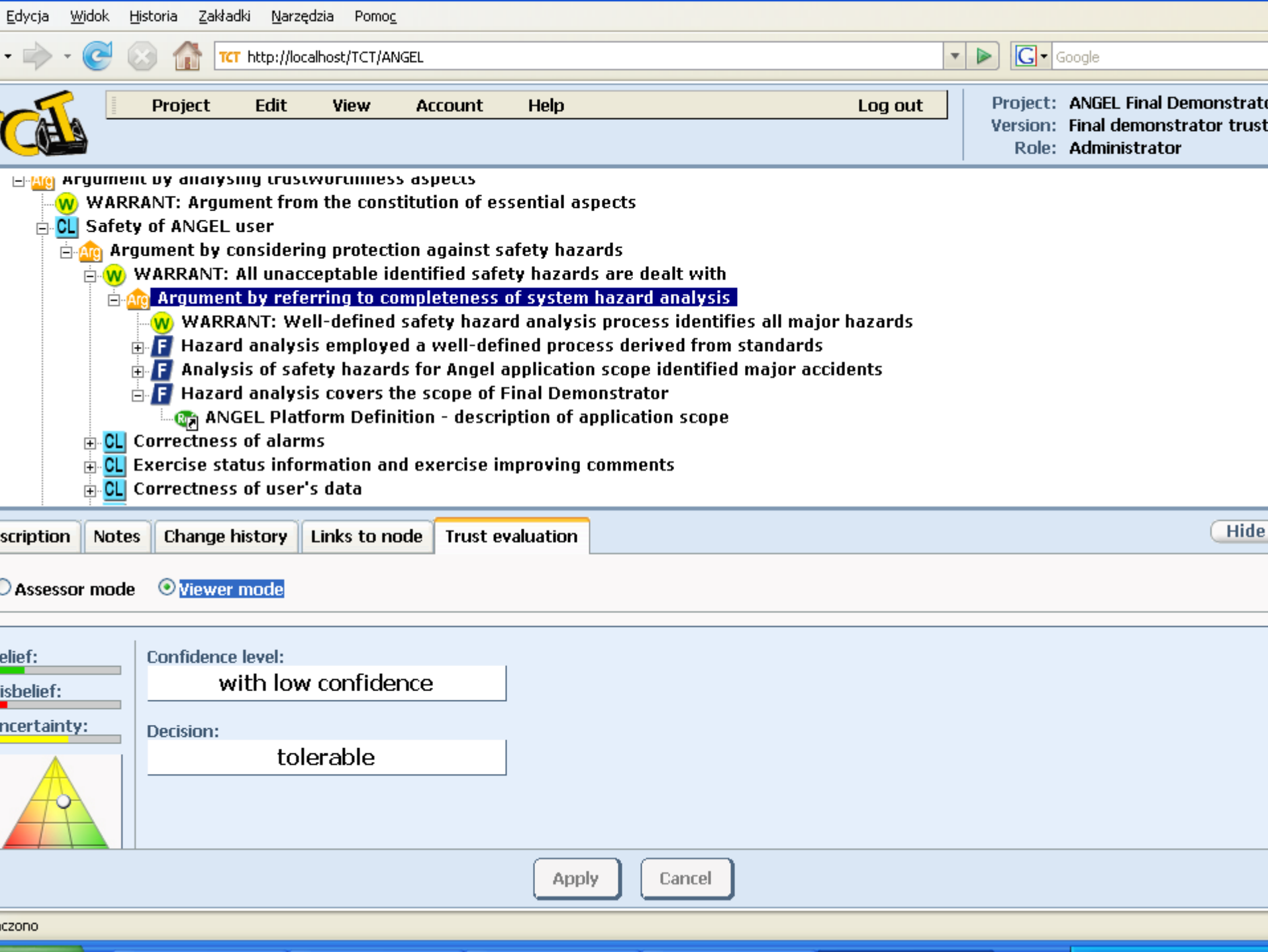

Edycja Widok Historia Zakładki Narzędzia Pomoc
TCT http://localhost/TCT/ANGEL
Google
Project Edit View Account Help Log out
Project: ANGEL Final Demonstrato
Version: Final demonstrator trust
Role: Administrator
Argument by analysing trustworthiness aspects
WARRANT: Argument from the constitution of essential aspects
Safety of ANGEL user
Argument by considering protection against safety hazards
WARRANT: All unacceptable identified safety hazards are dealt with
Argument by referring to completeness of system hazard analysis
WARRANT: Safety hazard analysis process identified major hazards within the demonstrator scope
Hazard analysis employed a well-defined process derived from standards
Analysis of safety hazards for Angel application scope identified major accidents
ANGEL Platform Definition - description of application scope
Hazard identification for Scenario 1
Hazard identification for Scenario 2 & 3
System safety hazards assesment report
Hazard analysis covers the scope of Final Demonstrator
scription
Notes
Change history
Links to node
Trust evaluation
Hide
Assessor mode
Viewer mode
elief:
isbelief:
ncertainty:
Confidence level:
with very high confidence
Decision:
tolerable
Apply
Cancel
czono


Edycja Widok Historia Zakładki Narzędzia Pomoc
TCT http://localhost/TCT/ANGEL
Google
Project Edit View Account Help Log out
Project: ANGEL Final Demonstrato
Version: Final demonstrator trust
Role: Administrator
Argument by analysing trustworthiness aspects
WARRANT: Argument from the constitution of essential aspects
Safety of ANGEL user
Argument by considering protection against safety hazards
WARRANT: All unacceptable identified safety hazards are dealt with
Argument by referring to completeness of system hazard analysis
WARRANT: Safety hazard analysis process identified major hazards within the demonstrator scope
Hazard analysis employed a well-defined process derived from standards
Safety and privacy risk assesment process description
Analysis of safety hazards for Angel application scope identified major accidents
Hazard analysis covers the scope of Final Demonstrator
Correctness of alarms
Exercise status information and exercise improving comments
Correctness of user's data
scription
Notes
Change history
Links to node
Trust evaluation
Hide
Assessor mode
Viewer mode
elief:
isbelief:
ncertainty:
Confidence level:
with very high confidence
Decision:
acceptable
Apply
Cancel
czono


Edycja Widok Historia Zakładki Narzędzia Pomoc
TCT http://localhost/TCT/ANGEL
Google
Project Edit View Account Help Log out
Project: ANGEL Final Demonstrato
Version: Final demonstrator trust
Role: Administrator
Argument by analysing trustworthiness aspects
WARRANT: Argument from the constitution of essential aspects
Safety of ANGEL user
Argument by considering protection against safety hazards
WARRANT: All unacceptable identified safety hazards are dealt with
Argument by referring to completeness of system hazard analysis
WARRANT: Well-defined safety hazard analysis process identifies all major hazards
Hazard analysis employed a well-defined process derived from standards
Analysis of safety hazards for Angel application scope identified major accidents
Hazard analysis covers the scope of Final Demonstrator
Correctness of alarms
Exercise status information and exercise improving comments
Correctness of user's data
ANGEL system instalation, configuration and maintanance
scription
Notes
Change history
Links to node
Trust evaluation
Hide
Assessor mode
Viewer mode
elief:
isbelief:
ncertainty:
Confidence level:
with very high confidence
Decision:
acceptable
Apply
Cancel
czono


Edycja Widok Historia Zakładki Narzędzia Pomoc
TCT http://localhost/TCT/ANGEL
Google
Project Edit View Account Help Log out
Project: ANGEL Final Demonstrato
Version: Final demonstrator trust
Role: Administrator
Argument by analysing trustworthiness aspects
WARRANT: Argument from the constitution of essential aspects
Safety of ANGEL user
Argument by considering protection against safety hazards
WARRANT: All unacceptable identified safety hazards are dealt with
Argument by referring to completeness of system hazard analysis
WARRANT: Well-defined safety hazard analysis process identifies all major hazards
Hazard analysis employed a well-defined process derived from standards
Analysis of safety hazards for Angel application scope identified major accidents
Hazard analysis covers the scope of Final Demonstrator
Correctness of alarms
Exercise status information and exercise improving comments
Correctness of user's data
ANGEL system instalation, configuration and maintanance
scription
Notes
Change history
Links to node
Trust evaluation
Hide
Assessor mode
Viewer mode
elief:
isbelief:
ncertainty:
Confidence level:
with very high confidence
Decision:
tolerable
Apply
Cancel
czono


Edycja Widok Historia Zakładki Narzędzia Pomoc
TCT http://localhost/TCT/ANGEL
Google
Project Edit View Account Help Log out
Project: ANGEL Final Demonstrato
Version: Final demonstrator trust
Role: Administrator
Argument by analysing trustworthiness aspects
WARRANT: Argument from the constitution of essential aspects
Safety of ANGEL user
Argument by considering protection against safety hazards
WARRANT: All unacceptable identified safety hazards are dealt with
Argument by referring to completeness of system hazard analysis
WARRANT: Well-defined safety hazard analysis process identifies all major hazards
Hazard analysis employed a well-defined process derived from standards
Analysis of safety hazards for Angel application scope identified major accidents
Hazard analysis covers the scope of Final Demonstrator
ANGEL Platform Definition - description of application scope
Correctness of alarms
Exercise status information and exercise improving comments
Correctness of user's data
scription
Notes
Change history
Links to node
Trust evaluation
Hide
Assessor mode
Viewer mode
elief:
isbelief:
ncertainty:
Confidence level:
with low confidence
Decision:
tolerable
User name
Confidence level
Decision
TCT administrator
with low confidence
tolerable
Apply
Cancel
czono


Edycja Widok Historia Zakładki Narzędzia Pomoc
TCT http://localhost/TCT/ANGEL
Google
Project Edit View Account Help Log out
Project: ANGEL Final Demonstrato
Version: Final demonstrator trust
Role: Administrator
Argument by analysing trustworthiness aspects
WARRANT: Argument from the constitution of essential aspects
Safety of ANGEL user
Argument by considering protection against safety hazards
WARRANT: All unacceptable identified safety hazards are dealt with
Argument by referring to completeness of system hazard analysis
WARRANT: Well-defined safety hazard analysis process identifies all major hazards
Hazard analysis employed a well-defined process derived from standards
Analysis of safety hazards for Angel application scope identified major accidents
Hazard analysis covers the scope of Final Demonstrator
ANGEL Platform Definition - description of application scope
Correctness of alarms
Exercise status information and exercise improving comments
Correctness of user's data
scription
Notes
Change history
Links to node
Trust evaluation
Hide
Assessor mode
Viewer mode
elief:
isbelief:
ncertainty:
Confidence level:
with low confidence
Decision:
tolerable
Apply
Cancel
czono

The aggregation mechanism

- **Different argument types depending on how the premises contribute to the conclusion**
- **Different aggregation rule for each argument type**
- **Mapping of the linguistic values on Dempster-Shaffer belief and plausability functions**

A-argument rule

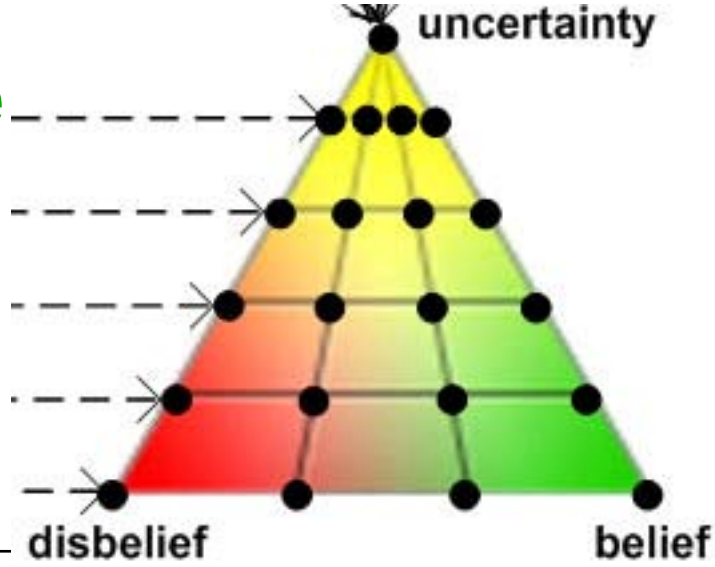
Yager's modification of Dempster's rule of combination

$$Bel(c) = Bel(a_1) \cdot Bel(a_2) + Bel(a_1) \cdot (Pl(a_2) - Bel(a_2)) + Bel(a_2) \cdot (Pl(a_1) - Bel(a_1))$$

$$Pl(c) = 1 - (1 - Pl(a_1)) \cdot (1 - Pl(a_2)) + (1 - Pl(a_1)) \cdot (Pl(a_2) - Bel(a_2)) + (1 - Pl(a_2)) \cdot (Pl(a_1) - Bel(a_1))$$

Validation expe

- **30 students involved**
- **Repeated assessment**



Aggregation rule	Consistency of students' assessments		A ag	
	Confidence scale	*Decision scale*	*Confidence scale*	*Decision scale*
A-rule	1,03	0,64	1,04	0,80
NSC-rule	0,94	0,53	1,06	0,61
C-rule	0,84	0,88	0,91	0,66

Conclusion

- **Trust-IT provides for development, maintenance and sharing of trust cases for real life objects**
  - **A Personalized Information Platform for health and life Services**
    - **(6th EU FR Integrated Project PIPS)**
  - **A platform supporting WSN based health related applications**
    - **(6th EU FR STREP Project ANGEL)**
  - **TTA based dependable embedded systems**
    - **(6th EU FR Integrated Project DECOS)**
  - **Support for standards conformance (e.g. ISO 27001, ISO 14971:2000)**
  - **Trustworthiness of HON (Helth On the Ne) criteria**
- **Argument appraisal mechanism provides for third party assessment of trust cases**
- **Linguistic scales support communication of trust case contents between stakeholders**
- **More experiments are needed to calibrate and validate the appraisal mechanism**