



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



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



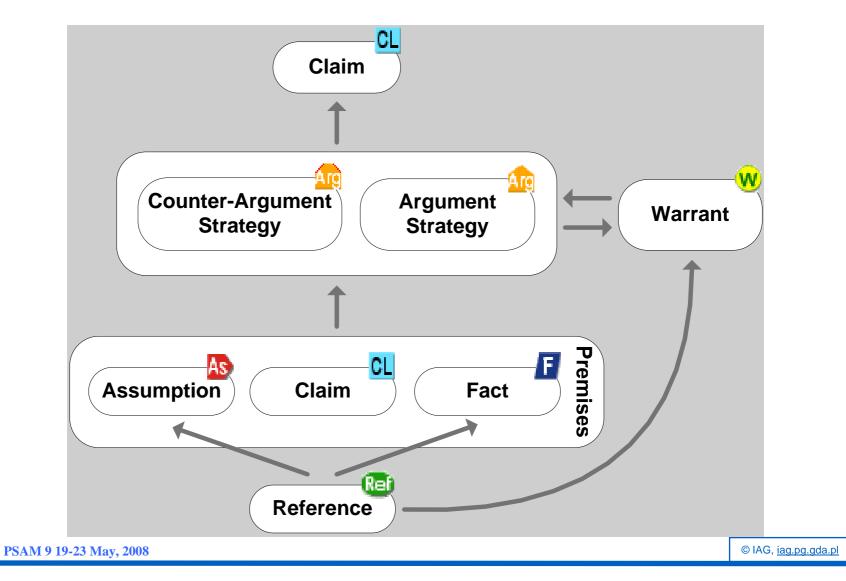
Trust Case

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



(F)

E.

Trust Case example

- CL Safety of ANGEL user
 - 🖻 Argument by considering protection against safety hazards
 - W WARRANT: All unacceptable identified safety hazards are dealt with
 - CL Correctness of alarms
 - CL Exercise status information and exercise improving comments
 - CL Correctness of user's data
 - 🖻 🎰 Argument by describing system features
 - W WARRANT: Features are located in two layers platform and application
 - CL Support from ANGEL platform to correctness of data
 - 🗄 🎰 Argument by describing supporting functionalities and properties
 - WARRANT: Platform maintains reliablity of data
 - CH Reliability of ANGEL data
 - E CL Reliability of data storage and processing of ANGEL application
 - 🔚 🚼 Correct exercise support from ANGEL application
 - 🗄 🛄 ANGEL system instalation, configuration and maintanance
 - E CL Accidental damage of sensors e.g. due to Patient's physical activity
 - 📸 Argument by reference to platform component property
 - W WARRANT: Sensor design protects them sufficiently from accidental damage Sensor node resilience

- 6 -

Edycja <u>W</u> idok <u>H</u> istoria <u>Z</u> akładki <u>N</u> arzędzia Pomo <u>c</u>			
• 🗼 • 🥑 💿 🏠 TCT http://localhost/TCT/ANGEL		*	Google
Project Edit View A	ccount Help L	.og out	Project: ANGEL Final Demonstrat Version: Final demonstrator trust Role: Administrator
Hazard analysis employed a Analysis of safety hazards for a saf	tion of essential aspects against safety hazards ified safety hazards are dealt with		tor scope
scription Notes Chang A Move Up LINK & Move Down & Cut & Copy So to link target & 1			Hide abel: Include in report
me: Hazard identification for Scenario 1		abel: tate:	Initial
czono	Apply Cancel		

<u>E</u> dycja <u>W</u> idok <u>H</u> istoria <u>Z</u> akładki <u>N</u> arzędzia Pomo <u>c</u>									
- 🛸 - (🔹 🗣 🕑 🚱 🏠 TCT http://localhost/TCT/ANGEL 🔹 🕨 💽 🖬 Google								
Project Edit View Account Help Log out Project: ANGEL Final Demo Version: Final demonstrat Role: Administrator									
Trust cas	se for ANGEL final demo	n ctu-	ton						
CL ANGE	L ANGEL system trustworthines 💌 Microsoft Excel - GUT_IR_ANGEL_HAZOP_scen1_01-3.xls								
🗄 🎰 Arg	jument by analysing tru	:2)	<u>P</u> lik <u>E</u> dycj	ia <u>W</u> idok W <u>s</u> taw <u>F</u> ormat <u>N</u> arzędzia <u>D</u> ane <u>O</u> kno Pomo <u>c</u> Ado <u>b</u> e PDF	Wpis				
···• •• ••	WARRANT: Argument fr			δ 🚔 🚔 🛍 🛍 + 🗉 → 😒 Σ + δ ↓ Χ ↓ 🛄 @ 📮 i Arial	• 11 • B ≣ ≣ ≣				
	Safety of ANGEL user								
	ो Argument by conside → ₩ WARRANT: All una								
	🗄 🎪 Argument by re		B20	✓ f Air Humidification System					
	W WARRANT: S	1	A	B Functionality					
	🕀 📕 Hazard analy		0001	Remote house live monitoring from mobile phone	House monitoring data are				
	🖃 🖪 Analysis of s	3		Remote house live monitoring from Pc	House monitoring data are				
	🖓 ANGEL Pla			Indoor house live monitoring from mobile phone	House monitoring data are				
				Indoor house live monitoring from Pc	House monitoring data are				
	- 🦙 Hazard ide - 🖙 System sa			House live monitoring response time					
	⊕ 🗗 Hazard analy			House sensors status	No information on sensor s				
-	Correctness of ala	8		Automatic filter cleaning	Filter is not cleaned				
crintian	Notes Change history	9		User Notification about dirty filters condition	User is not notified on dirty				
scription	Notes Change history	10		Query about conditioner filters status	No information on filter stat				
LINK		11		Temperature and Humidity monitoring	Temperature or humidity				
		12		Temperature and Humidity notification	No notification of danger				
Go to link ta	arnet	13	0012	Dangers notification using third parties WSNs	No notification of dangerous				
	arget	14	0013	Delayed air analysis	No periodical air analysi				
REFERENC	CE	15	0014	Plant Monitor	Plants are not monitored				
	F 16 0015 Plant Humidification System								
me:	Humidification constrain								
		18	0017	Plant Condition Notification	No notification of incorrect				
	Air humidification is not co								
		20	0019	Air Humidification System	Air humidification is not				
C70D0		21	0020	Bad humidity level notification	User is not notified on bad				
czono		22							



Language for **Scenarios for** representing using trust cases trust cases Trust case Trust Templates processes case Patterns 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

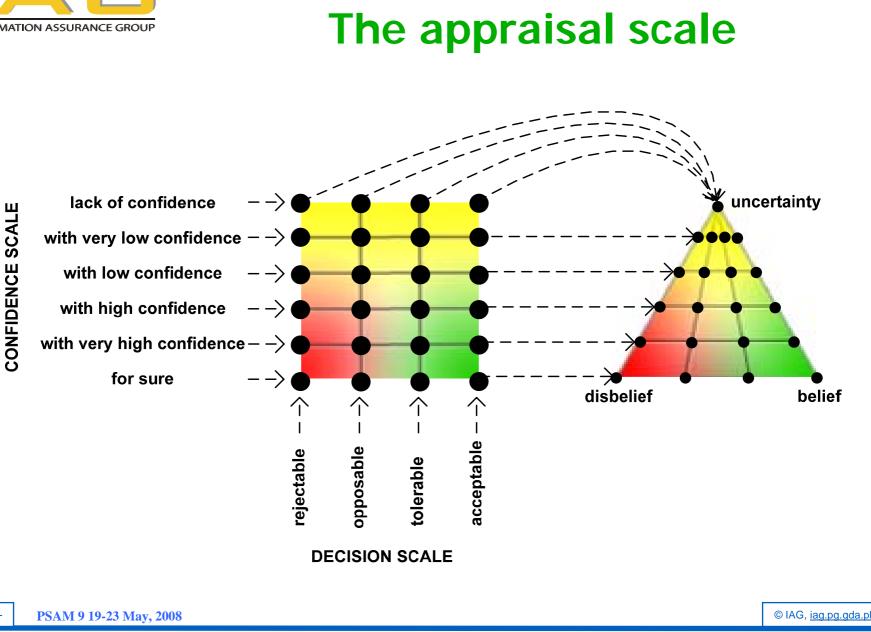
Provide an argumentation appraisal mechanism which starts from assessments of the facts and inferences in the argument and aggregates them to an assessment of the topmost claim



Trust Case example

Safety of ANGEL user Argument by considering protection against safety hazards WARRANT: All unacceptable identified safety hazards are dealt with **Correctness of alarms** Exercise status information and exercise improving comments + Correctness of user's data Argument by describing system features WARRANT: Features are located in two layers - platform and application Support from ANGEL platform to correctness of data Argument by describing supporting functionalities and properties E. WARRANT: Platform maintains reliablity of data Reliability of ANGEL data Reliability of data storage and processing of ANGEL application **I** Gorrect exercise support from ANGEL application ANGEL system instalation, configuration and maintanance Accidental damage of sensors e.g. due to Patient's physical activity Argument by reference to platform component property WARRANT: Sensor design protects them sufficiently from accidental damage Sensor node resilience







Appraisal example

<u>E</u> dycja <u>W</u> idok	<u>H</u> istoria <u>Z</u> akładki <u>N</u> arzędzia Pomo <u>c</u>				
• 🔶 • 🥑 (CT http://localhost/TCT/ANGEL			•	Google
	Project Edit View Ad	ccount Help		Log out	Project: ANGEL Final Demonstrat Version: Final demonstrator trust Role: Administrator
CL ANGEL sys	ANGEL final demonstrator tem trustworthiness nt by analysing trustworthiness as RANT: Argument from the constitut y of ANGEL user gument by considering protection a WARRANT: All unacceptable identi Argument by referring to compl WARRANT: Safety hazard an Hazard analysis employed a F Analysis of safety hazards fo Hazard analysis covers the s ANGEL Platform Definition Correctness of alarms	ion of essential as against safety haza ified safety hazards eteness of system alysis process iden well-defined proce or Angel application cope of Final Demo	rds 5 are dealt with hazard analysis tified major hazards within ss derived from standards scope identified major accionstrator		r scope
scription Note		Trust evaluation			Hide
elief: isbelief: ncertainty:	Confidence level: for sure Decision:				
Â,	acceptable Delete assessment				
		Apply	/ Cancel		
C70D0					

<u>E</u> dycja <u>W</u> idok	<u>H</u> istoria <u>Z</u> akładki <u>N</u> arzędzia Pomo <u>c</u>			
• 🔶 • 🕑	CT http://localhost/TCT/ANGEL		•	Google
<u> 1</u>	Project Edit View Ad	count Help	Log out	Project: ANGEL Final Demonstrate Version: Final demonstrator trust Role: Administrator
₩ WAR CL Safet 	RANT: Argument from the constitut y of ANGEL user gument by considering protection a WARRANT: All unacceptable identi Argument by referring to compl WARRANT: Safety hazard an Hazard analysis employed a F Analysis of safety hazards fo ANGEL Platform Definition ANGEL Platform Definition Hazard identification for S Kara Hazard identification for S System safety hazards ass Hazard analysis covers the s	ion of essential aspects gainst safety hazards fied safety hazards are dealt wit eteness of system hazard analys alysis process identified major ha well-defined process derived fro r Angel application scope identifi - description of application scop cenario 1 cenario 2 & 3 sesment report	is azards within the demonstrat m standards <mark>ed major accidents</mark>	tor scope
scription Note	s Change history Links to node	Trust evaluation		Hide
Assessor mode	e 🔿 Viewer mode			
elief: sbelief: ncertainty:	Confidence level: with very high confider Decision: tolerable			
	·	Apply Cancel		
czono				

<u>E</u> dycja <u>W</u> idok i	<u>H</u> istoria <u>Z</u> akładki <u>N</u> arz	ędzia Pomo <u>c</u>						
• 🔶 • 🥑 (🔀 🚮 TCT http://lo	alhost/TCT/ANGEL				•		ogle
	Project Edit	View Ac	count Help		Log out		/ersion: F	ANGEL Final Demonstrat Final demonstrator trust Administrator
W WARI ⇒ CL Safet ⇒ ân Ari ⇒ W ⇒ CL ⊕ CL	⊟ <mark>F Hazard analys</mark> 	m the constituti ng protection a ceptable identif erring to comple fety hazard and is employed a v privacy risk ass fety hazards for is covers the so ms rmation and exe	ion of essential a gainst safety ha fied safety hazar eteness of syste alysis process id well-defined pro sesment process r Angel applicati cope of Final Der	zards ds are dealt with m hazard analysis entified major ha cess derived from description on scope identifie nonstrator	zards within the demor	nstrator	scope	
scription Note	S Change history	Links to node	Trust evaluation					Hide
Assessor mode	e 🔍 Viewer mode							
elief: sbelief: ncertainty:	Decision:	nigh confiden						
			Ар	ply Cancel)			
czono								

<u>E</u> dycja <u>W</u> idok	<u>H</u> istoria <u>Z</u> akładki <u>N</u> arzędzia Pomo <u>c</u>					
• 🔿 • 🥑 (CT http://localhost/TCT/ANGEL			•	G Google	
<u> 1</u>	Project Edit View Ad	count Help		Log out	Project: ANGEL Fina Version: Final demo Role: Administra	nstrator trust
₩ WAR CL Safet 	RANT: Argument from the constitut gument by considering protection a WARRANT: All unacceptable identi Argument by referring to comple WARRANT: Well-defined safe F Hazard analysis employed a F Hazard analysis covers the se Correctness of alarms Exercise status information and ex ANGEL system instalation, configure	ion of essential asy fied safety hazards eteness of system ety hazard analysis well-defined proce r Angel application cope of Final Demo ercise improving c	rds are dealt with hazard analysis process identifies all ma ss derived from standard scope identified major ad nstrator omments	s		
scription Note	s Change history Links to node	Trust evaluation				Hide
Assessor mode	e 🔿 Viewer mode					
elief: sbelief: ncertainty:	Confidence level: with very high confider Decision: acceptable					
		Apply	Cancel			
czono						

<u>E</u> dycja <u>W</u> idok	<u>H</u> istoria <u>Z</u> akładki <u>N</u> arzędzia Pomo <u>c</u>					
• 🗼 • 🕑	C 🏠 TCT http://localhost/TCT/ANGE	-		Ŧ	► G•G	oogle
	Project Edit View a	Account Help		Log out	Version:	ANGEL Final Demonstrate Final demonstrator trust Administrator
	RANT: Argument from the constitu- ty of ANGEL user gument by considering protection WARRANT: All unacceptable iden Argument by referring to com WARRANT: Well-defined sa WWARRANT: Well-defined sa Hazard analysis employed a F Hazard analysis covers the Correctness of safety hazards f Exercise status information and a Correctness of alarms	ution of essential asp against safety hazar tified safety hazards oleteness of system f fety hazard analysis a well-defined proces for Angel application scope of Final Demos exercise improving co	ds are dealt with <mark>azard analysis</mark> process identifies all majo s derived from standards scope identified major acc nstrator			
scription Note	es Change history Links to node	Trust evaluation				Hide
Assessor mode	e 🔯 Viewer mode					
elief: isbelief: ncertainty:	Confidence level: with very high confide Decision: tolerable	ence				
		Apply	Cancel			

<u>E</u> dycja <u>W</u> idok <u>F</u>	<u> H</u> istoria <u>Z</u> akładki <u>N</u> arzędzia Pomo <u>c</u>						
• 🔿 • 🥑 (CT http://localhost/TCT/ANGEL				• 🕨 🖸	- Google	
	Project Edit View A	ccount Help		Log out	Versio	t: ANGEL Final Den n: Final demonstra le: Administrator	
₩ WARF CL Safet Ang Arg 	IL DY ANALYSING CRUSTWORTHINESS AS RANT: Argument from the constitu- y of ANGEL user gument by considering protection WARRANT: All unacceptable ident WARRANT: All unacceptable ident WARRANT: Well-defined saf G Hazard analysis employed a G F Hazard analysis employed a G F Hazard analysis covers the s MAGEL Platform Definition Correctness of alarms Exercise status information and es Correctness of user's data	tion of essential asp against safety hazar ified safety hazards leteness of system l ety hazard analysis well-defined proces or Angel application scope of Final Demo n - description of ap	rds are dealt with hazard analysis process identifi ss derived from scope identified instrator oplication scope	standards			
scription Note	s Change history Links to node	Trust evaluation					Hide
Assessor mode	• • Viewer mode						
elief: isbelief: ncertainty:	Confidence level: with low confidence Decision: tolerable	<u>}</u>					
	User name TCT administrator	Con	fidence level	with low confidence		Decision tolerable	
		Apply	/ Cancel				
CZODO							

<u>E</u> dycja <u>W</u> idok <u>I</u>	<u>H</u> istoria <u>Z</u> akładki <u>N</u> arz	ędzia Pomo <u>c</u>					
• 🔶 • 🥑 (🔀 🚮 TCT http://lo	calhost/TCT/ANGEL				• 🕨 💽 •	Google
	Project Edit	View Ac	count Help		Log out	Version:	ANGEL Final Demonstrate Final demonstrator trust Administrator
WWARI ⇒.CL Safet ⇒	₩ WARRANT: W Hazard analys F Analysis of sa Hazard analys	m the constituti ing protection a ceptable identif erring to comple ell-defined safe is employed a s fety hazards for is covers the so form Definition ms rmation and ex	ion of essential asp igainst safety haza fied safety hazards eteness of system ety hazard analysis well-defined proce r Angel application cope of Final Demo - description of ap	rds are dealt with nazard analysis process identifies a ss derived from stan scope identified ma nstrator plication scope	ndards		
scription Note	s Change history	Links to node	Trust evaluation				Hide
Assessor mode							
elief: isbelief: ncertainty:	Decision:	v confidence Ierable					
			Apply	Cancel			
c70D0							



The aggregation mechanism



Different argument types depending on how the premises contribute to the conclusion

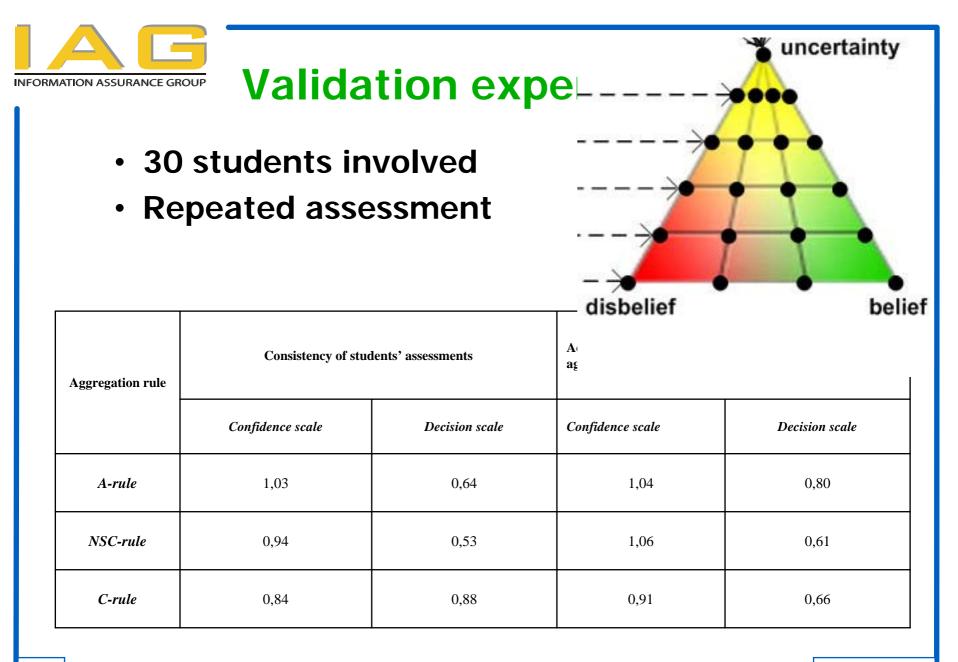
- Different aggregation rule for each argument type
- Mapping of the linguistic values on Dempster-Shaffer belief and plausability functions

A-argument rule

Yager's modification of Dempster's rule of combination

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

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





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