HOW DO YOU KNOW THAT A SECURITY METHODOLOGY WORK?

AN EMPIRICAL APPROACH TO EVALUATE SECURITY DESIGN METHODS.

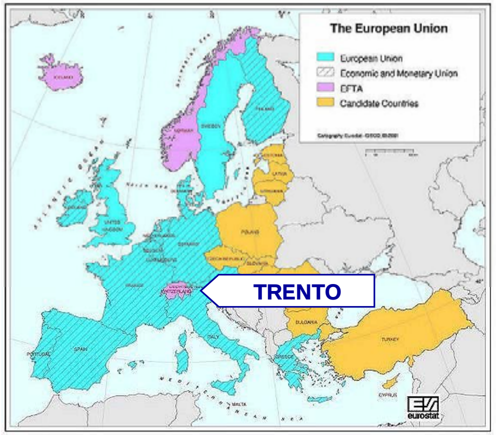
Joint work with
F. Paci, K. Labunet,
Y. Asnar, A.
Battocchi and
many others

Fabio Massacci
University of Trento – Italy
www.massacci.org

TALK'S ROADMAP

- □ Personal Introduction
- □ Motivations
- □ Research Questions
- □ An Experimental Protocol
- □ Running the Experiments
- □ Empirical Results or what really works
- □ Conclusions and Lessons Learned

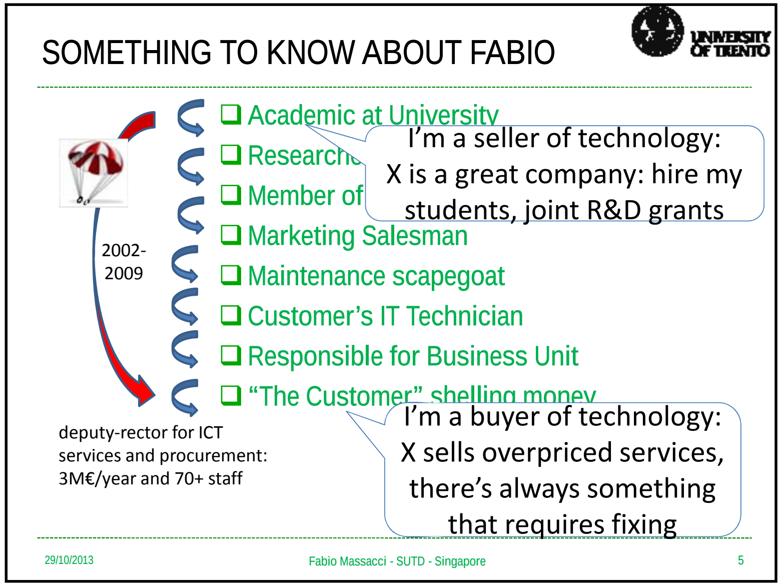
WHERE IS TRENTO, ITALY?



- □ 1962
- ✓ The Institute of Social Science is founded as locally funded Institution
- □ 1972
- ✓ The Institute becomes a private University
- □ 1982
- ✓ The University becomes a state University with special autonomy
- □ 2012
- ✓ Full provincial autonomy

SECURITY RESEARCH IN TRENTO

- □ Security research at the University of Trento (Italy)
- ✓ 3 professor + 1 senior researchers
- ✓ 5 post-doctoral researchers
- ✓ 10+ Phd students
- □ Coordinates many M€ European R&D Projects on
- ✓ Mobile Security and Security Engineering
- ✓ Cyber and Critical Infrastrctures Security Economics
- ✓ We work with:
  - UK/US National Grid, SAP, Symantec, Atos..
  - International Airports, Metropolitan Transport
- □ EIT Master in Security and Privacy
- □ More details at
- ✓ http://securitylab.disi.unitn.it



SOMETHING TO KNOW ABOUT FABIO

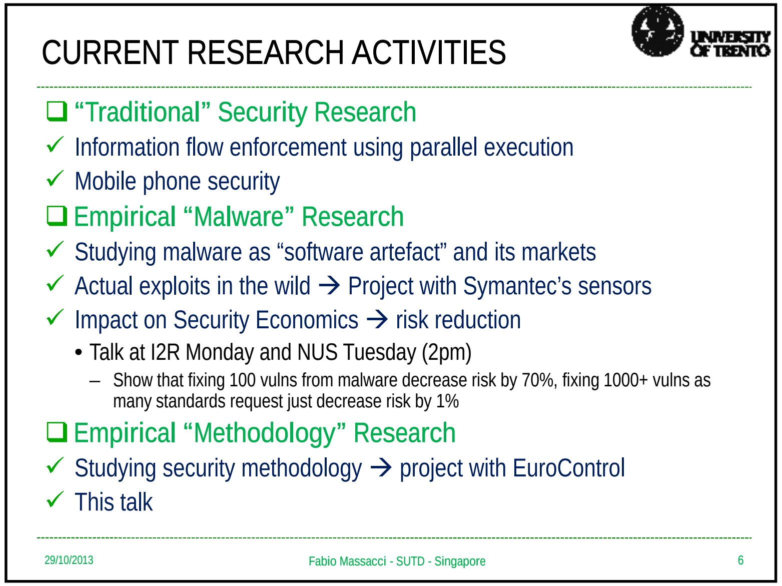
- ❑ Academic at University
- ❑ Researche
- ❑ Member of
- ❑ Marketing Salesman
- ❑ Maintenance scapegoat
- ❑ Customer's IT Technician
- ❑ Responsible for Business Unit
- ❑ "The Customer" shelling money

I'm a seller of technology: X is a great company: hire my students, joint R&D grants

2002-2009

deputy-rector for ICT services and procurement: 3M€/year and 70+ staff

I'm a buyer of technology: X sells overpriced services, there's always something that requires fixing



CURRENT RESEARCH ACTIVITIES

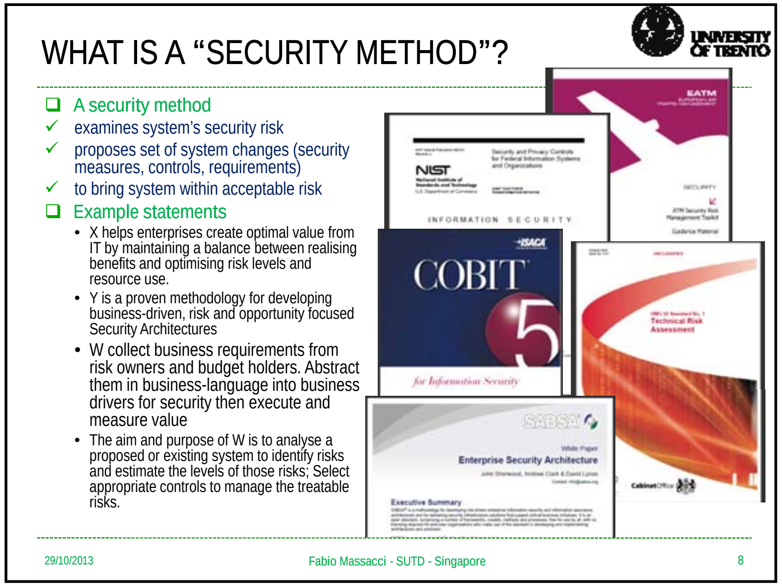
- ❑ "Traditional" Security Research
- ✓ Information flow enforcement using parallel execution
- ✓ Mobile phone security
- ❑ Empirical "Malware" Research
- ✓ Studying malware as "software artefact" and its markets
- ✓ Actual exploits in the wild → Project with Symantec's sensors
- ✓ Impact on Security Economics → risk reduction
  - Talk at I2R Monday and NUS Tuesday (2pm)
    - – Show that fixing 100 vulns from malware decrease risk by 70%, fixing 1000+ vulns as many standards request just decrease risk by 1%
- ❑ Empirical "Methodology" Research
- ✓ Studying security methodology → project with EuroControl
- ✓ This talk

ANIKETOS
NESSoS
SECONOMICS
TENACE

MOTIVATIONS

Motivations
Questions
Protocol
Experiments
Results
Conclusions

Why is important to know if a methodology works effectively



WHAT IS A "SECURITY METHOD"?

- ❑ A security method
- ✓ examines system's security risk
- ✓ proposes set of system changes (security measures, controls, requirements)
- ✓ to bring system within acceptable risk
- ❑ Example statements
  - X helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use.
  - Y is a proven methodology for developing business-driven, risk and opportunity focused Security Architectures
  - W collect business requirements from risk owners and budget holders. Abstract them in business-language into business drivers for security then execute and measure value
  - The aim and purpose of W is to analyse a proposed or existing system to identify risks and estimate the levels of those risks; Select appropriate controls to manage the treatable risks.

THE INDUSTRIAL PROBLEM

❑ "Poste Italiane" – large banking and mail delivery conglomerate

- ✓ 20B€ Revenues, 18M credit cards, 32M customers, 3M simcards
- ✓ 1033 IT Complex Services
  - Many Subject to EU Financial Directives, Privacy Directives, PCI DSS,etc
- ✓ 1857 requests for IT changes in 2012, 120 just for Jan/2013
  - Must identify security measures (if applicable) in short time

❑ How to Identify Security Measures?

- ✓ Use a standard?
  - ISO27002 lists measures → doesn't say which are applicable to you
  - PCI DSS list high level requirements → doesn't say which are in your scope
- ✓ Use a methodology, but which one?
  - ISACA's CoBIT, SABSA → focus on Business Goals
  - US NIST 800-53, UK's IAS → focus on Threats
- ✓ Solution → use "mine", proven to work... But what does it mean proven?

29/10/2013 Fabio Massacci - SUTD - Singapore 9

HOW TO SELECT A DRUG?

❑ FDA requires data from clinical trials (S. Thaul, CRS 2012)

- ✓ form
subj
- ✓ Trial
grou
safe

❑ Aca ... cal
trial

Safety

measured by toxicity testing to determine optimal dose of a drug needed to achieve the desired benefit and identify any potential adverse effects

Efficacy

Measured by a health benefit over a placebo or other intervention when tested in an ideal situation, such as a tightly controlled clinical trial.

Effectiveness

describes how the drug works in a real-world situation. May be lower than efficacy because of interactions with other real life conditions (other medications or health conditions of patient, slightly different duration or use, off-label untested condition)

29/10/2013 Fabio Massacci - SUTD - Singapore 10

LET'S SEE A TYPICAL SECURITY PAPER

❑ A typical paper (academia or industry)

Introduction
[optional: Industry Scenario]
Background on X
  Methodology, Modelling Language, Reasoning (if any) etc.
NewX with "Built-in" Security Constructs
  Always new methodological steps,
  Sometimes new modeling constructs,
  Rarely new reasoning features
Application of NewX to a (possibly industrial) scenario

❑ Validation i

❑ Survey of C

- ✓ 67% of Requ
- ✓ 13% have a
- ✓ My (old) papers are no exception (e.g. RE 05 most cited paper)

❑ Almost no tradition to empirically validate efficacy

- ✓ Opdahl et al.[Inf. Softw. Tech.2009] two controlled experiments: misuse cases vs attack trees
- ✓ More papers in IS Literature

29/10/2013 Fabio Massacci - SUTD - Singapore 11

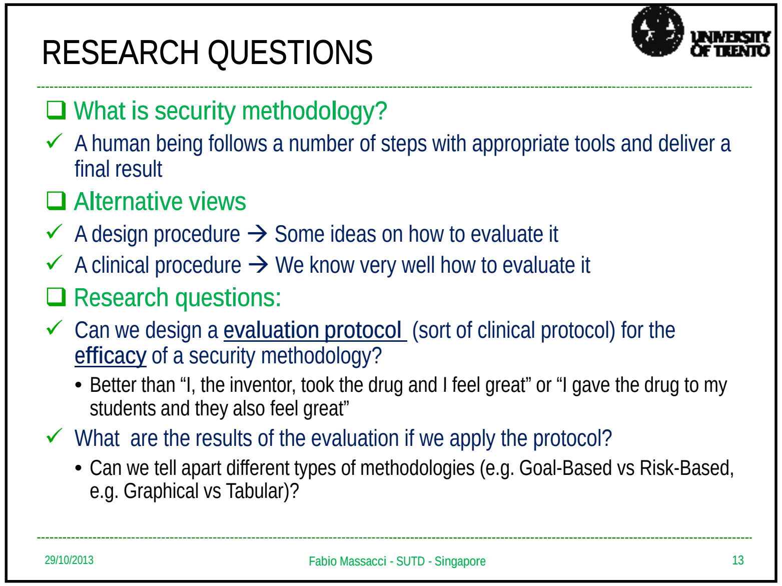
ANIKETOS
NESSoS
SECONOMICS
TENACE

RESEARCH QUESTIONS

✓Motivations
Questions
Protocol
Experiments
Results
Conclusions

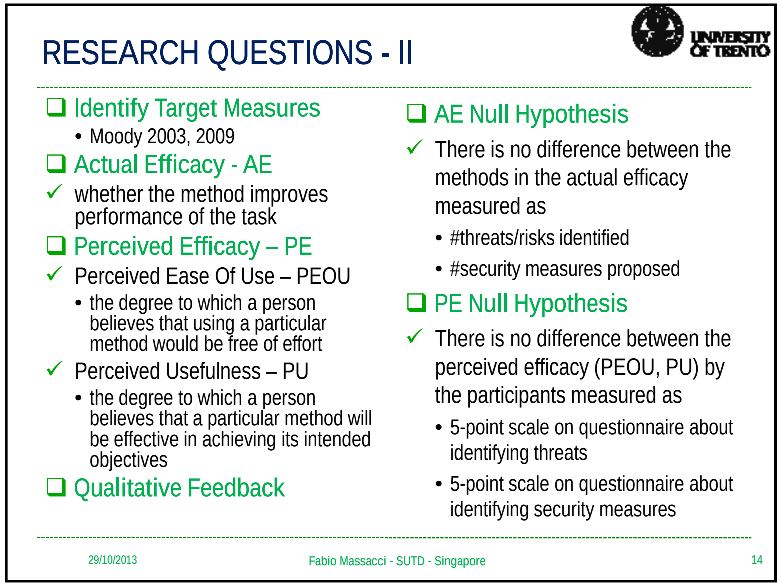
What we actually want to know when we plan to empirically evaluate a methodology?

29/10/2013 12



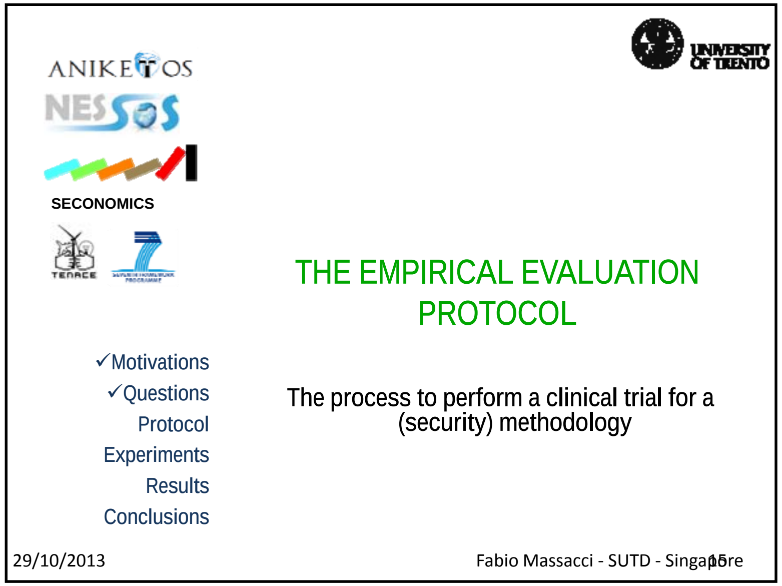
RESEARCH QUESTIONS

- ❑ What is security methodology?
  - ✓ A human being follows a number of steps with appropriate tools and deliver a final result
- ❑ Alternative views
  - ✓ A design procedure → Some ideas on how to evaluate it
  - ✓ A clinical procedure → We know very well how to evaluate it
- ❑ Research questions:
  - ✓ Can we design a evaluation protocol (sort of clinical protocol) for the efficacy of a security methodology?
    - Better than "I, the inventor, took the drug and I feel great" or "I gave the drug to my students and they also feel great"
  - ✓ What are the results of the evaluation if we apply the protocol?
    - Can we tell apart different types of methodologies (e.g. Goal-Based vs Risk-Based, e.g. Graphical vs Tabular)?



RESEARCH QUESTIONS - II

- ❑ Identify Target Measures
  - Moody 2003, 2009
- ❑ Actual Efficacy - AE
  - ✓ whether the method improves performance of the task
- ❑ Perceived Efficacy – PE
  - ✓ Perceived Ease Of Use – PEOU
    - the degree to which a person believes that using a particular method would be free of effort
  - ✓ Perceived Usefulness – PU
    - the degree to which a person believes that a particular method will be effective in achieving its intended objectives
- ❑ Qualitative Feedback
- ❑ AE Null Hypothesis
  - ✓ There is no difference between the methods in the actual efficacy measured as
    - #threats/risks identified
    - #security measures proposed
- ❑ PE Null Hypothesis
  - ✓ There is no difference between the perceived efficacy (PEOU, PU) by the participants measured as
    - 5-point scale on questionnaire about identifying threats
    - 5-point scale on questionnaire about identifying security measures



ANIKETOS

NESSoS

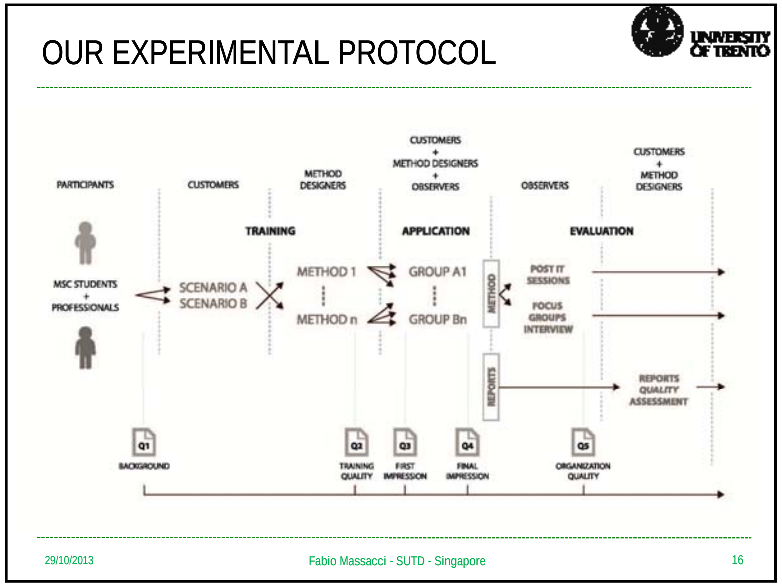
SECONOMICS

TENACE

THE EMPIRICAL EVALUATION PROTOCOL

The process to perform a clinical trial for a (security) methodology

✓Motivations
✓Questions
Protocol
Experiments
Results
Conclusions



OUR EXPERIMENTAL PROTOCOL

PROTOCOL STEPS

- ❑ Training of Participants
- ✓ Designers and customers train participants on methods and case studies
  →No learning bias due to previous knowledge
- ❑ Application of Methods
- ✓ Groups of participants apply methods to analyze the case study
  →Typical method applications are in groups (senior/junior consultants), reflect actual usage
  →Enough manpower to present significant results (to discriminate among methods)
- ❑ Evaluation
- ✓ Designers and customers evaluate correctness of application
  → Eliminate low quality output from evaluation (e.g "not motivated" participants)
- ✓ Participants evaluate the methods' effectiveness

29/10/2013 Fabio Massacci - SUTD - Singapore 17

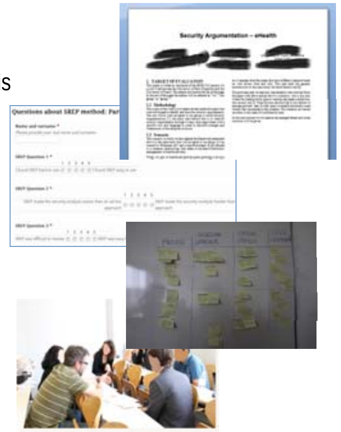
PROTOCOL ACTORS

- ❑ Participant
- ✓ Apply an security method to analyze a case study
  - Important to have both students (novices to the method but unbiased opinion) and practitioners (expert but may have prejudices on what it works).
  - Allows to understand gap between efficacy and effectiveness
- ❑ Designer
- ✓ The security requirements method inventor
  - Provide the best possible training for the method. No bias from the researcher in presenting better his own method
- ❑ Customer
- ✓ The owner of a case study on which the methods are applied
  - Indipende validation of the quality of the results (irrespective of method!). Any method can produce "enough" security requirements if the quality doesn't matter
- ❑ Observer
- ✓ Collect data and Audio-video record Participants
  - Many information requires interaction

29/10/2013 Fabio Massacci - SUTD - Singapore 18

PROTOCOL MEASUREMENTS

- ❑ Actual Efficacy
- ✓ Participants Reports
  - Quantitative, Qualitative Content Analysis
- ✓ Audio-Video Recording
  - Coding, qualitative, quantitative analysis
- ❑ Perceived Efficacy
- ✓ Questionnaires
  - Statistical Analysis (Rank-Sum test)
- ❑ Qualitative analysis
- ✓ Post-it notes
  - Affinity Analysis
- ✓ Focus Groups Interviews
  - Coding, qualitative analysis



Security Argumentation – eHealth

[redacted]

1. TARGET OF EVALUATION

1.1 Methodology

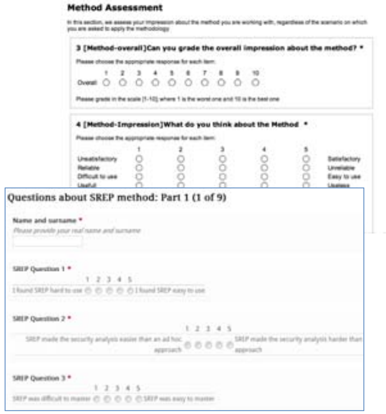
1.2 Scenario

Questions about SREP method: Part

29/10/2013 Fabio Massacci - SUTD - Singapore 19

QUESTIONNAIRES FOR STATISTICS

- ❑ Collect Information about:
- ✓ Participants' background
- ✓ Methods' Effectiveness
- ✓ Comparison with other methods
- ❑ Administered at different stages:
- ✓ Beginning (Q1)
  → Establish baselines and demographics
- ✓ Post Training (Q2)
- ✓ Beginning of Application (Q3)
  → How things looks like initially, may be affected by bias in the training
- ✓ Post Application (Q4)
  → Your final opinion after you have really used the methodology



Method Assessment

In this section, we assess your impression about the method you are working with, regardless of the scenario on which you are asked to apply the methodology

3 [Method-overall]Can you grade the overall impression about the method? *

Please choose the appropriate response for each item:

	1	2	3	4	5	6	7	8	9	10
Overall	○	○	○	○	○	○	○	○	○	○

Please grade in the scale [1-10] where 1 is the worst one and 10 is the best one

4 [Method-Impression]What do you think about the Method *

Please choose the appropriate response for each item:

	1	2	3	4	5	
Unsatisfactory	○	○	○	○	○	Satisfactory
Reliable	○	○	○	○	○	Unreliable
Difficult to use	○	○	○	○	○	Easy to use
Useful	○	○	○	○	○	Useless

Questions about SREP method: Part 1 (1 of 9)

Name and surname *
Please provide your real name and surname

SREP Question 1 *

	1	2	3	4	5	
I found SREP hard to use	○	○	○	○	○	I found SREP easy to use

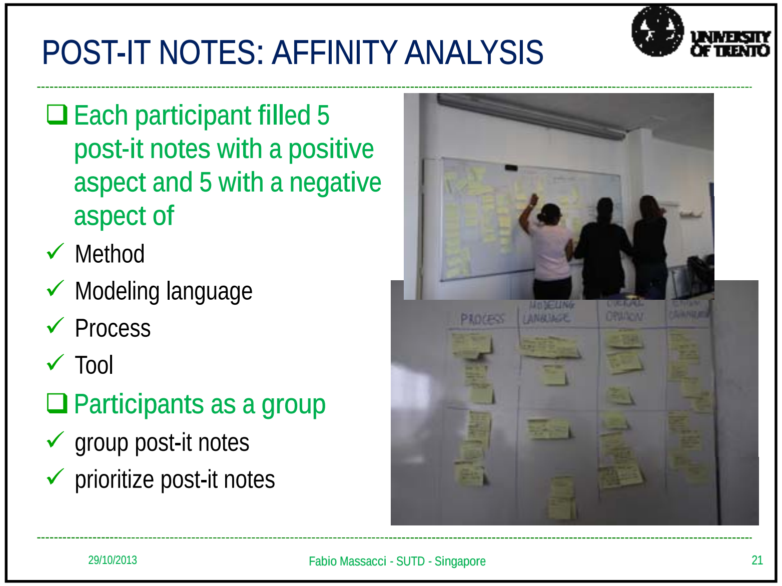
SREP Question 2 *

	1	2	3	4	5	
SREP made the security analysis easier than an ad hoc approach	○	○	○	○	○	SREP made the security analysis harder than approach

SREP Question 3 *

	1	2	3	4	5	
SREP was difficult to master	○	○	○	○	○	SREP was easy to master

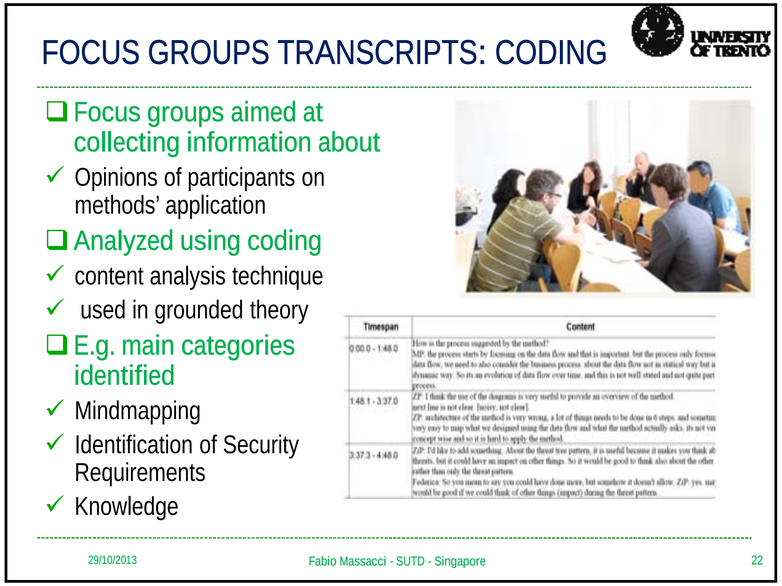
29/10/2013 Fabio Massacci - SUTD - Singapore 20



POST-IT NOTES: AFFINITY ANALYSIS

- ❑ Each participant filled 5 post-it notes with a positive aspect and 5 with a negative aspect of
  - ✓ Method
  - ✓ Modeling language
  - ✓ Process
  - ✓ Tool
- ❑ Participants as a group
  - ✓ group post-it notes
  - ✓ prioritize post-it notes

29/10/2013 Fabio Massacci - SUTD - Singapore 21



FOCUS GROUPS TRANSCRIPTS: CODING

- ❑ Focus groups aimed at collecting information about
  - ✓ Opinions of participants on methods' application
- ❑ Analyzed using coding
  - ✓ content analysis technique
  - ✓ used in grounded theory
- ❑ E.g. main categories identified
  - ✓ Mindmapping
  - ✓ Identification of Security Requirements
  - ✓ Knowledge

Timespan	Content
0:00.0 - 1:48.0	How is the process suggested by the method? MP: the process starts by focusing on the data flow and that is important, but the process only focuse data flow, we need to also consider the business process. about the data flow not in statical way but i dynamic way. So its an evolution of data flow over time, and this is not well stated and not quite part process.
1:48.1 - 3:37.0	ZP: I think the use of the diagrams is very useful to provide an overview of the method. next line is not clear. [noisy, not clear]. ZP: architecture of the method is very wrong, a lot of things needs to be done in 6 steps. and sometin very easy to map what we designed using the data flow and what the method actually asks. its not ve concept wise and so it is hard to apply the method.
3:37.3 - 4:48.0	ZiP: I'd like to add something. About the threat tree pattern, it is useful because it makes you think ab threats, but it could have an impact on other things. So it would be good to think also about the other rather than only the threat pattern. Federica: So you mean to say you could have done more, but somehow it doesn't allow. ZiP: yes. ma would be good if we could think of other things (impact) during the threat pattern.

29/10/2013 Fabio Massacci - SUTD - Singapore 22

ANIKETOS

NESSoS

SECONOMICS

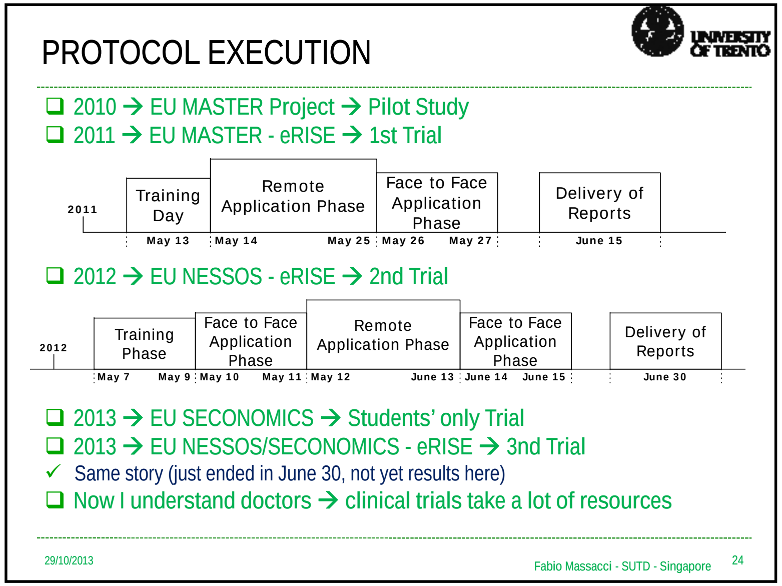
TENACE

RUNNING THE EXPERIMENTS

- ✓Motivations
- ✓Questions
- ✓Protocol
- Experiments
- Results
- Conclusions

Executing the clinical trials

29/10/2013 Fabio Massacci - SUTD - Singapore 23



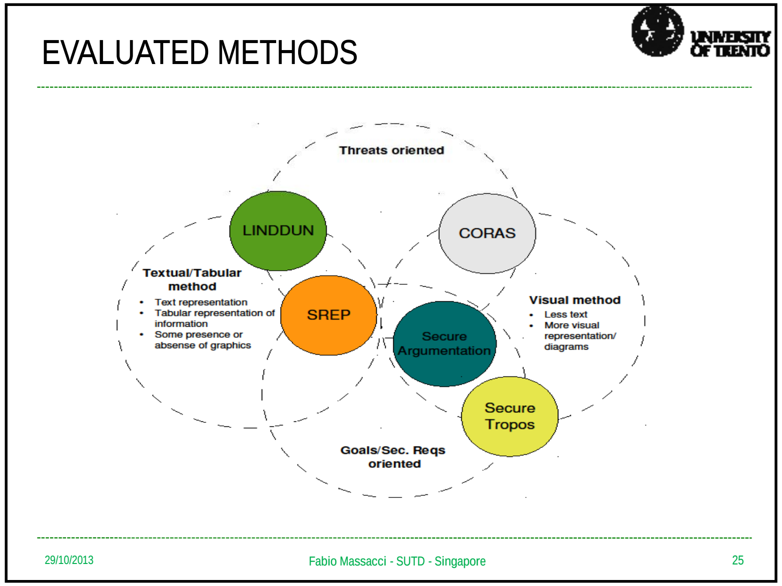
PROTOCOL EXECUTION

- ❑ 2010 → EU MASTER Project → Pilot Study
- ❑ 2011 → EU MASTER - eRISE → 1st Trial

- ❑ 2012 → EU NESSOS - eRISE → 2nd Trial

- ❑ 2013 → EU SECONOMICS → Students' only Trial
- ❑ 2013 → EU NESSOS/SECONOMICS - eRISE → 3nd Trial
  - ✓ Same story (just ended in June 30, not yet results here)
- ❑ Now I understand doctors → clinical trials take a lot of resources

29/10/2013 Fabio Massacci - SUTD - Singapore 24



EVALUATED METHODS

UNIVERSITY OF TRENTO

Threats oriented

LINDDUN

CORAS

Textual/Tabular method

- Text representation
- Tabular representation of information
- Some presence or absense of graphics

SREP

Secure Argumentation

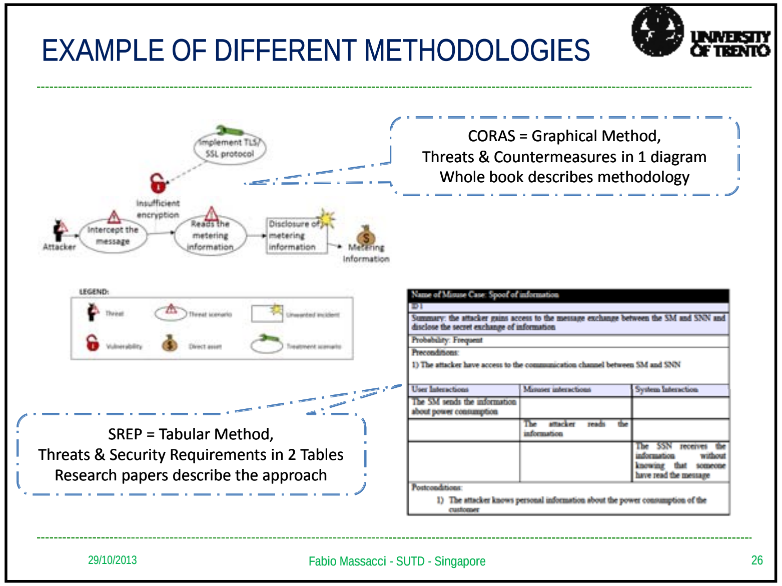
Visual method

- Less text
- More visual representation/ diagrams

Secure Tropos

Goals/Sec. Reqs oriented

29/10/2013 Fabio Massacci - SUTD - Singapore 25



EXAMPLE OF DIFFERENT METHODOLOGIES

UNIVERSITY OF TRENTO

Implement TLS/ SSL protocol

Insufficient encryption

Attacker

Intercept the message

Reads the metering information

Disclosure of metering information

Metering Information

LEGEND:

Threat

Threat scenario

Unwanted incident

Vulnerability

Direct asset

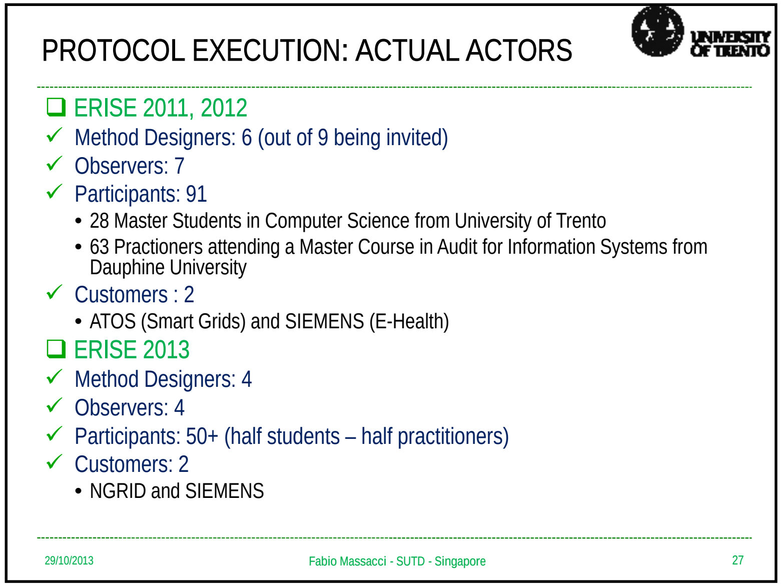
Treatment scenario

CORAS = Graphical Method,
Threats & Countermeasures in 1 diagram
Whole book describes methodology

Name of Misuse Case: Spoof of information		
ID 1		
Summary: the attacker gains access to the message exchange between the SM and SNN and disclose the secret exchange of information		
Probability: Frequent		
Preconditions: 1) The attacker have access to the communication channel between SM and SNN		
User Interactions	Misuser interactions	System Interaction
The SM sends the information about power consumption		
	The attacker reads the information	
		The SSN receives the information without knowing that someone have read the message
Postconditions: 1) The attacker knows personal information about the power consumption of the customer		

SREP = Tabular Method,
Threats & Security Requirements in 2 Tables
Research papers describe the approach

29/10/2013 Fabio Massacci - SUTD - Singapore 26



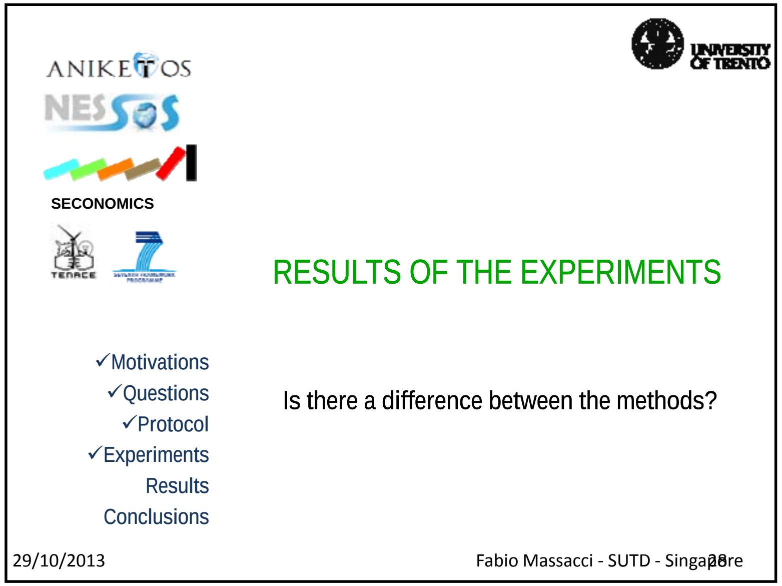
PROTOCOL EXECUTION: ACTUAL ACTORS

UNIVERSITY OF TRENTO

❑ ERISE 2011, 2012
- ✓ Method Designers: 6 (out of 9 being invited)
- ✓ Observers: 7
- ✓ Participants: 91
  - 28 Master Students in Computer Science from University of Trento
  - 63 Practioners attending a Master Course in Audit for Information Systems from Dauphine University
- ✓ Customers : 2
  - ATOS (Smart Grids) and SIEMENS (E-Health)

❑ ERISE 2013
- ✓ Method Designers: 4
- ✓ Observers: 4
- ✓ Participants: 50+ (half students – half practitioners)
- ✓ Customers: 2
  - NGRID and SIEMENS

29/10/2013 Fabio Massacci - SUTD - Singapore 27



ANIKETOS

NESSoS

SECONOMICS

TENACE

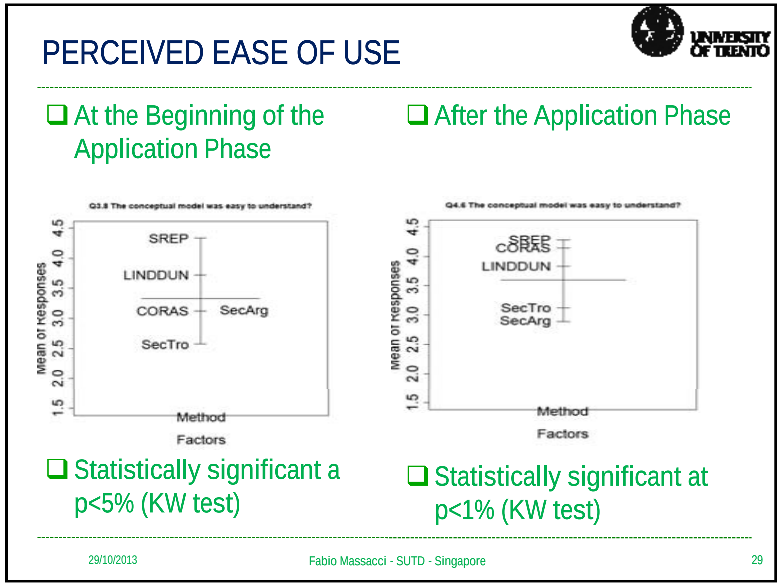
UNIVERSITY OF TRENTO

RESULTS OF THE EXPERIMENTS

✓Motivations
✓Questions
✓Protocol
✓Experiments
Results
Conclusions

Is there a difference between the methods?

29/10/2013 Fabio Massacci - SUTD - Singapore 28

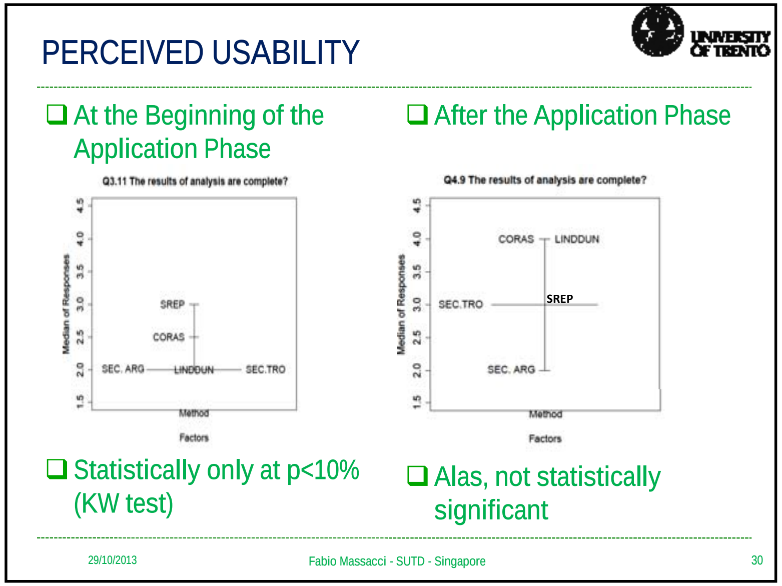


PERCEIVED EASE OF USE

- ❑ At the Beginning of the Application Phase
- ❑ After the Application Phase

- ❑ Statistically significant a p<5% (KW test)
- ❑ Statistically significant at p<1% (KW test)

29/10/2013 Fabio Massacci - SUTD - Singapore 29

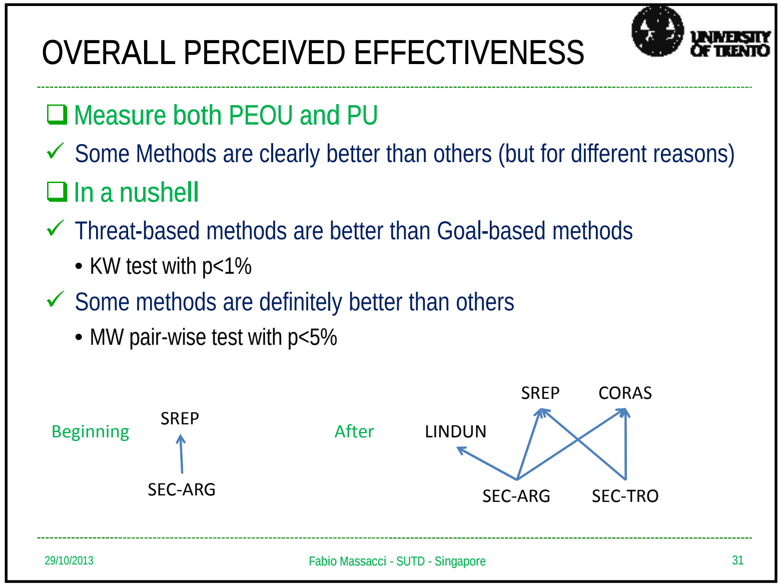


PERCEIVED USABILITY

- ❑ At the Beginning of the Application Phase
- ❑ After the Application Phase

- ❑ Statistically only at p<10% (KW test)
- ❑ Alas, not statistically significant

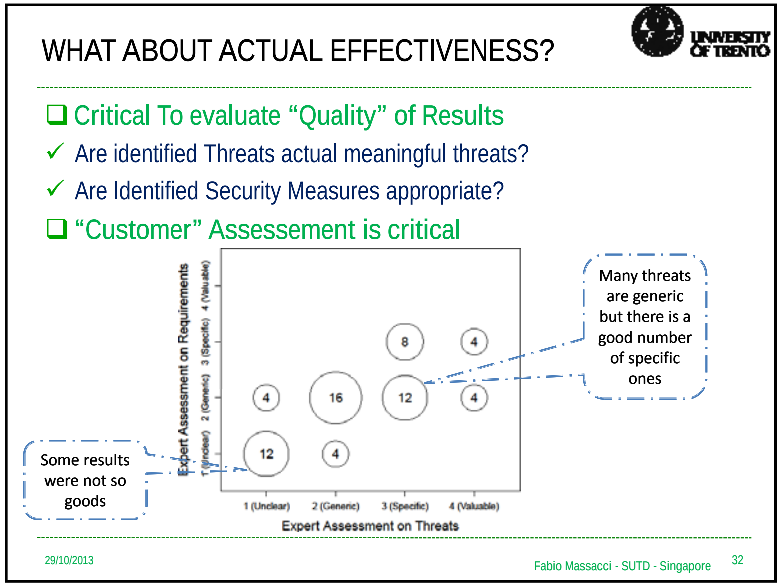
29/10/2013 Fabio Massacci - SUTD - Singapore 30



OVERALL PERCEIVED EFFECTIVENESS

- ❑ Measure both PEOU and PU
- ✓ Some Methods are clearly better than others (but for different reasons)
- ❑ In a nushell
- ✓ Threat-based methods are better than Goal-based methods
  - KW test with p<1%
- ✓ Some methods are definitely better than others
  - MW pair-wise test with p<5%

29/10/2013 Fabio Massacci - SUTD - Singapore 31



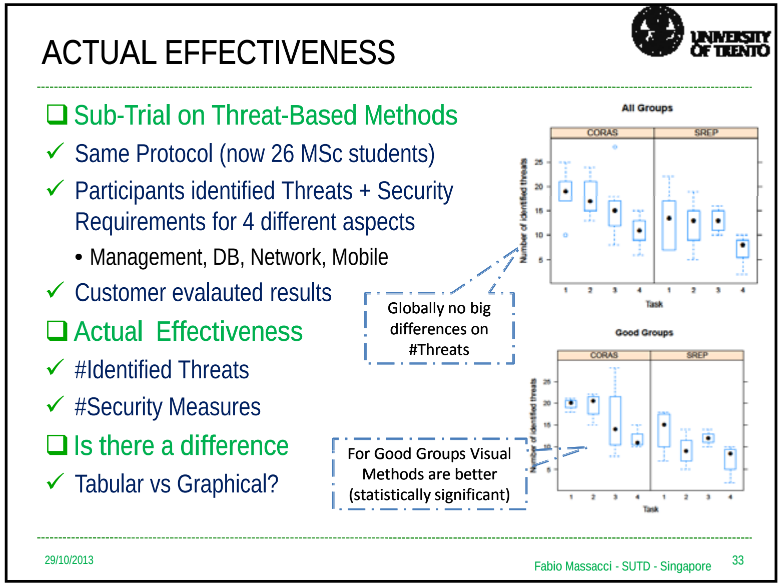
WHAT ABOUT ACTUAL EFFECTIVENESS?

- ❑ Critical To evaluate “Quality” of Results
- ✓ Are identified Threats actual meaningful threats?
- ✓ Are Identified Security Measures appropriate?
- ❑ “Customer” Assessement is critical

Many threats are generic but there is a good number of specific ones

Some results were not so goods

29/10/2013 Fabio Massacci - SUTD - Singapore 32



ACTUAL EFFECTIVENESS

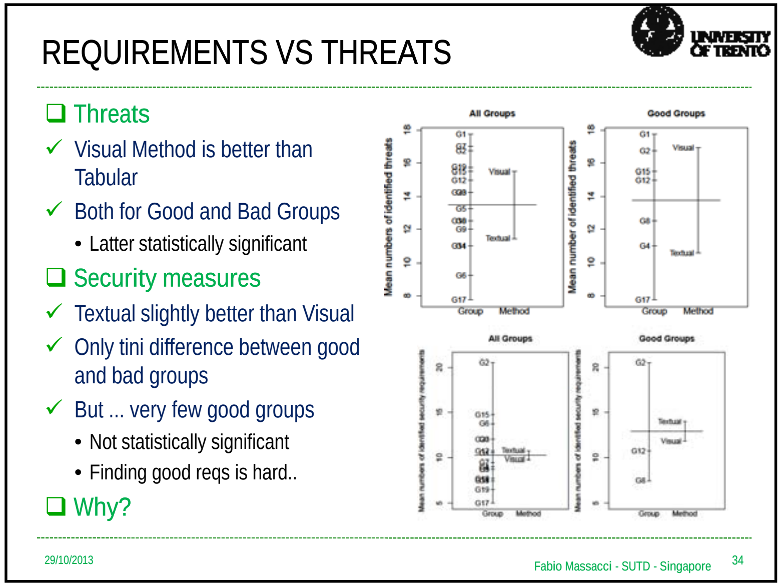
UNIVERSITY OF TRENTO

- ❑ Sub-Trial on Threat-Based Methods
- ✓ Same Protocol (now 26 MSc students)
- ✓ Participants identified Threats + Security Requirements for 4 different aspects
  - Management, DB, Network, Mobile
- ✓ Customer evaluated results
- ❑ Actual Effectiveness
- ✓ #Identified Threats
- ✓ #Security Measures
- ❑ Is there a difference
- ✓ Tabular vs Graphical?

Globally no big differences on #Threats

For Good Groups Visual Methods are better (statistically significant)

29/10/2013 Fabio Massacci - SUTD - Singapore 33

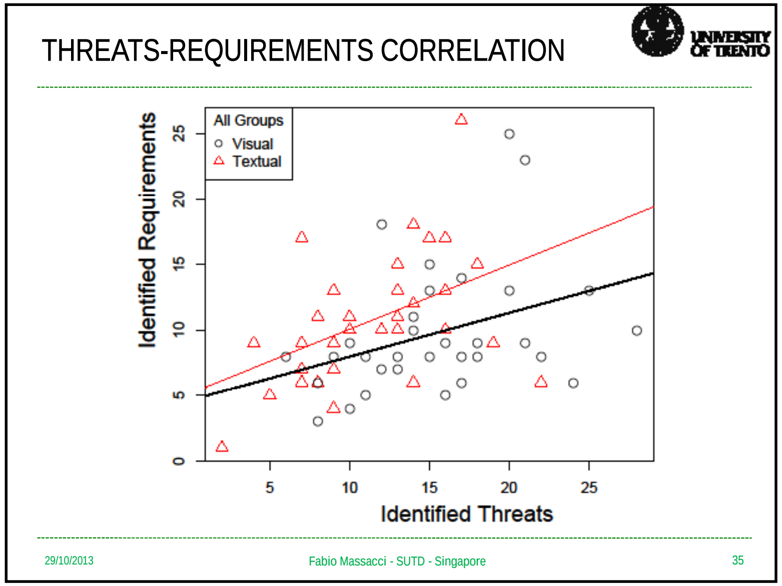


REQUIREMENTS VS THREATS

UNIVERSITY OF TRENTO

- ❑ Threats
- ✓ Visual Method is better than Tabular
- ✓ Both for Good and Bad Groups
  - Latter statistically significant
- ❑ Security measures
- ✓ Textual slightly better than Visual
- ✓ Only tini difference between good and bad groups
- ✓ But ... very few good groups
  - Not statistically significant
  - Finding good reqs is hard..
- ❑ Why?

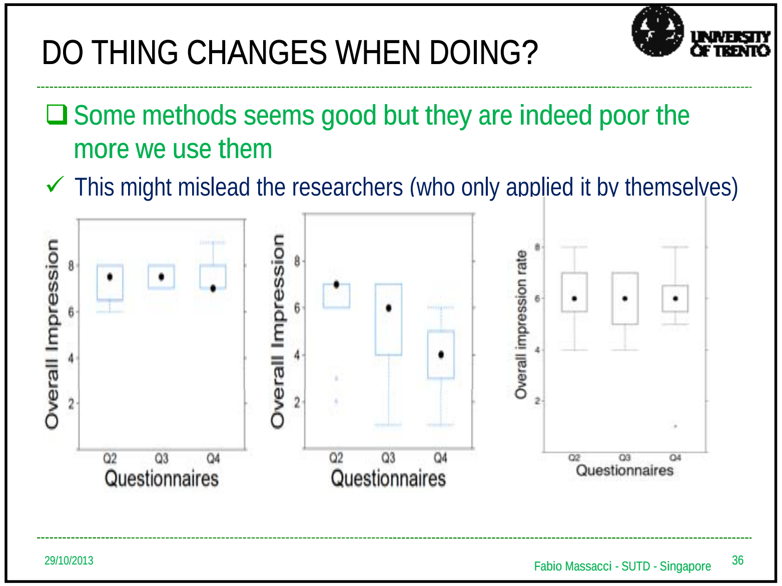
29/10/2013 Fabio Massacci - SUTD - Singapore 34



THREATS-REQUIREMENTS CORRELATION

UNIVERSITY OF TRENTO

29/10/2013 Fabio Massacci - SUTD - Singapore 35

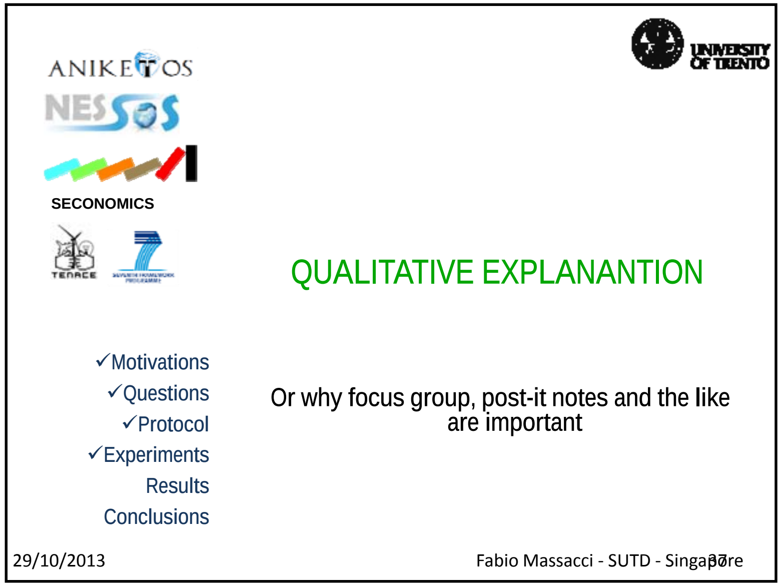


DO THING CHANGES WHEN DOING?

UNIVERSITY OF TRENTO

- ❑ Some methods seems good but they are indeed poor the more we use them
- ✓ This might mislead the researchers (who only applied it by themselves)

29/10/2013 Fabio Massacci - SUTD - Singapore 36



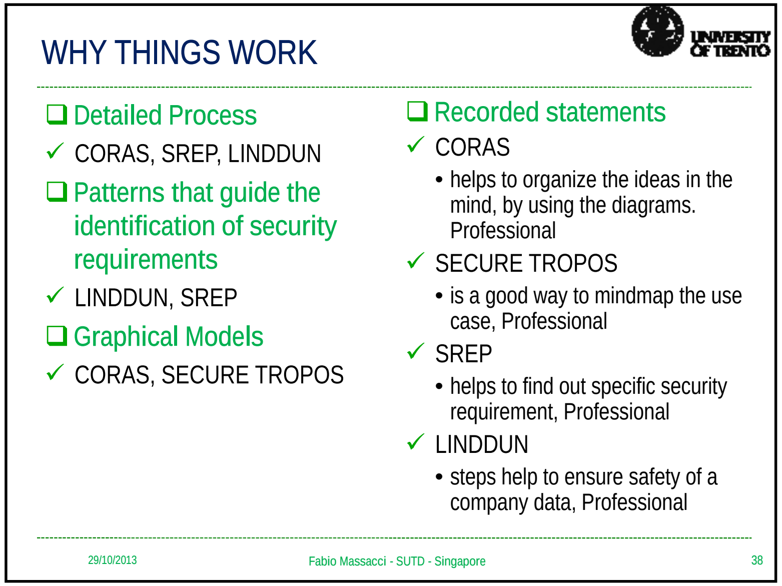
ANIKETOS
NESSoS
SECONOMICS
TENACE
UNIVERSITY OF TRENTO

QUALITATIVE EXPLANANTION

Or why focus group, post-it notes and the like are important

✓Motivations
✓Questions
✓Protocol
✓Experiments
Results
Conclusions

29/10/2013 Fabio Massacci - SUTD - Singapore 37

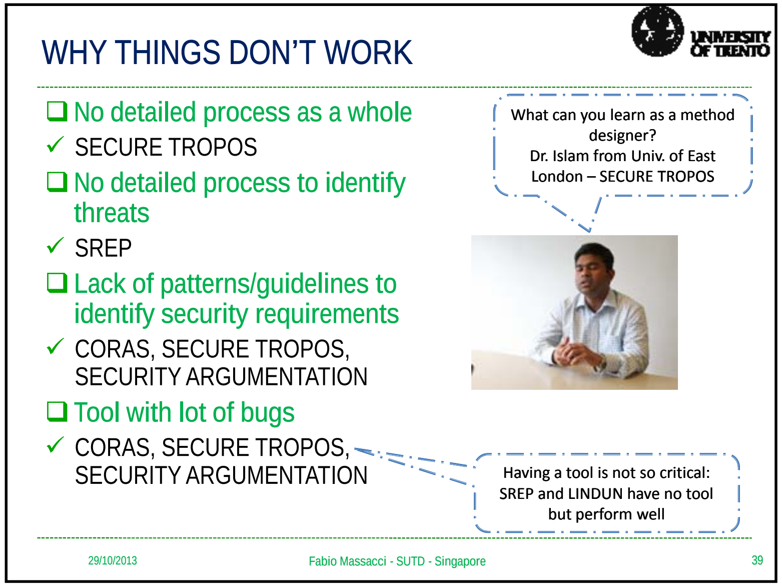


WHY THINGS WORK

- ❑ Detailed Process
- ✓ CORAS, SREP, LINDDUN
- ❑ Patterns that guide the identification of security requirements
- ✓ LINDDUN, SREP
- ❑ Graphical Models
- ✓ CORAS, SECURE TROPOS

- ❑ Recorded statements
- ✓ CORAS
  - helps to organize the ideas in the mind, by using the diagrams. Professional
- ✓ SECURE TROPOS
  - is a good way to mindmap the use case, Professional
- ✓ SREP
  - helps to find out specific security requirement, Professional
- ✓ LINDDUN
  - steps help to ensure safety of a company data, Professional

29/10/2013 Fabio Massacci - SUTD - Singapore 38



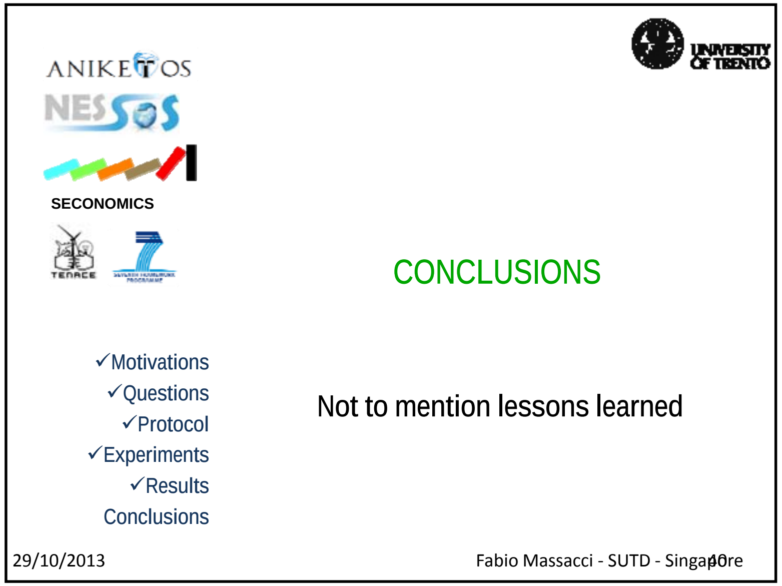
WHY THINGS DON'T WORK

- ❑ No detailed process as a whole
- ✓ SECURE TROPOS
- ❑ No detailed process to identify threats
- ✓ SREP
- ❑ Lack of patterns/guidelines to identify security requirements
- ✓ CORAS, SECURE TROPOS, SECURITY ARGUMENTATION
- ❑ Tool with lot of bugs
- ✓ CORAS, SECURE TROPOS, SECURITY ARGUMENTATION

What can you learn as a method designer?
Dr. Islam from Univ. of East London – SECURE TROPOS

Having a tool is not so critical: SREP and LINDUN have no tool but perform well

29/10/2013 Fabio Massacci - SUTD - Singapore 39



ANIKETOS
NESSoS
SECONOMICS
TENACE
UNIVERSITY OF TRENTO

CONCLUSIONS

Not to mention lessons learned

✓Motivations
✓Questions
✓Protocol
✓Experiments
✓Results
Conclusions

29/10/2013 Fabio Massacci - SUTD - Singapore 40

SUMMARY OF EXPERIMENT

❑ When does a methodology work?

- ✓ Clear Process is essential → Threat based methods all have it
- ✓ Visual Diagrams alone don't help
  - LINDUN,SREP > SEC-TROPOS, SEC-ARG
- ✓ Visual Diagrams helps when brainstorming is key → e.g. threats
- ✓ Tool support doesn't seem to matter → only negative if tool isn't good

❑ Open Issues

- ✓ Threat-based better than goal-based?
  - CORAS > SEC-TRO but for a different reasons (i.e. process), we need a Goal-based method with a clear,well defined process
- ✓ What about scaling to large assessment?

29/10/2013 Fabio Massacci - SUTD - Singapore 41

THREATS TO VALIDITY

❑ Internal Validity

- ✓ Participants' knowledge of other methods
  - Cannot be eliminated
- ✓ Training Time too short

❑ External Validity

- ✓ Generalization of our results
  - SREP and CORAS are pretty different but both beat goal/problem models

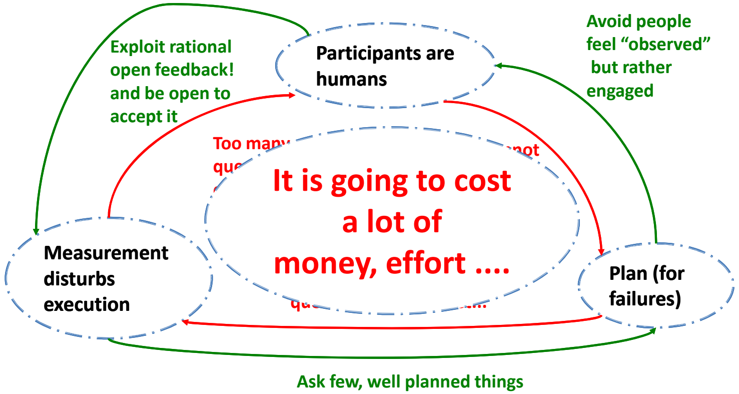
❑ Conclusion Validity

- ✓ Statistical significance → addressed
- ✓ Correctness of requirements identified

29/10/2013 Fabio Massacci - SUTD - Singapore 42

LEASSONS LEARNED

❑ It seems easy now but...



Exploit rational open feedback! and be open to accept it

Participants are humans

Avoid people feel "observed" but rather engaged

It is going to cost a lot of money, effort ....

Measurement disturbs execution

Plan (for failures)

Ask few, well planned things

29/10/2013 Fabio Massacci - SUTD - Singapore 43

CONCLUSIONS

❑ Empirical Evaluation of Efficacy of Design is difficult

- ✓ 4 qualitative studies over 4 years, 10 designers, 100+ participants, 6 customers, 10 observers
- ✓ Evaluation based on an application scenario is a lot easier !!!

❑ Some high-level results

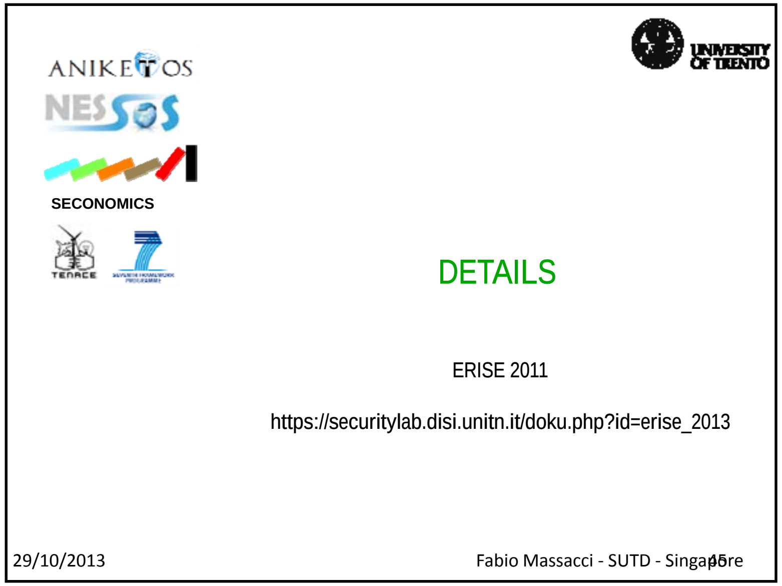
- ✓ Threat based better than goal-based and problem-based
- ✓ Graphics better for tasks involving brainstorming
  - less effective when systematic search is important

❑ Want to join the effort?

- ✓ Sending participants?
- ✓ Local "Experiment" course?

❑ More Info? → http://securitylab.disi.unitn.it

29/10/2013 Fabio Massacci - SUTD - Singapore 44



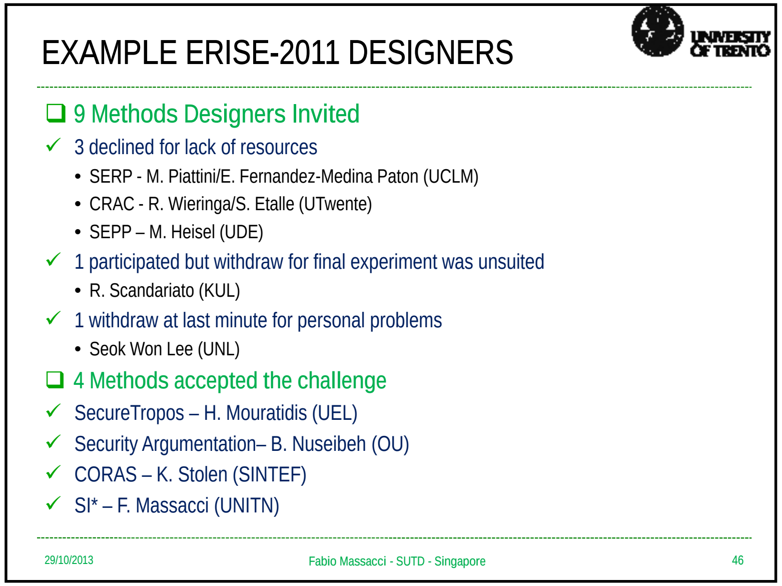
SECONOMICS

DETAILS

ERISE 2011

https://securitylab.disi.unitn.it/doku.php?id=erise_2013

29/10/2013 Fabio Massacci - SUTD - Singapore 45



EXAMPLE ERISE-2011 DESIGNERS

❑ 9 Methods Designers Invited

✓ 3 declined for lack of resources
- SERP - M. Piattini/E. Fernandez-Medina Paton (UCLM)
- CRAC - R. Wieringa/S. Etalle (UTwente)
- SEPP – M. Heisel (UDE)

✓ 1 participated but withdraw for final experiment was unsuited
- R. Scandariato (KUL)

✓ 1 withdraw at last minute for personal problems
- Seok Won Lee (UNL)

❑ 4 Methods accepted the challenge

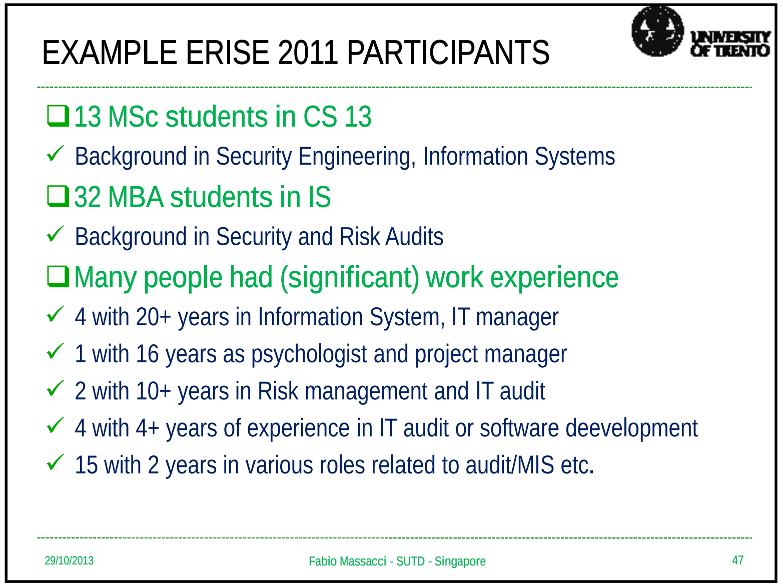
✓ SecureTropos – H. Mouratidis (UEL)

✓ Security Argumentation– B. Nuseibeh (OU)

✓ CORAS – K. Stolen (SINTEF)

✓ SI* – F. Massacci (UNITN)

29/10/2013 Fabio Massacci - SUTD - Singapore 46



EXAMPLE ERISE 2011 PARTICIPANTS

❑ 13 MSc students in CS 13

✓ Background in Security Engineering, Information Systems

❑ 32 MBA students in IS

✓ Background in Security and Risk Audits

❑ Many people had (significant) work experience

✓ 4 with 20+ years in Information System, IT manager

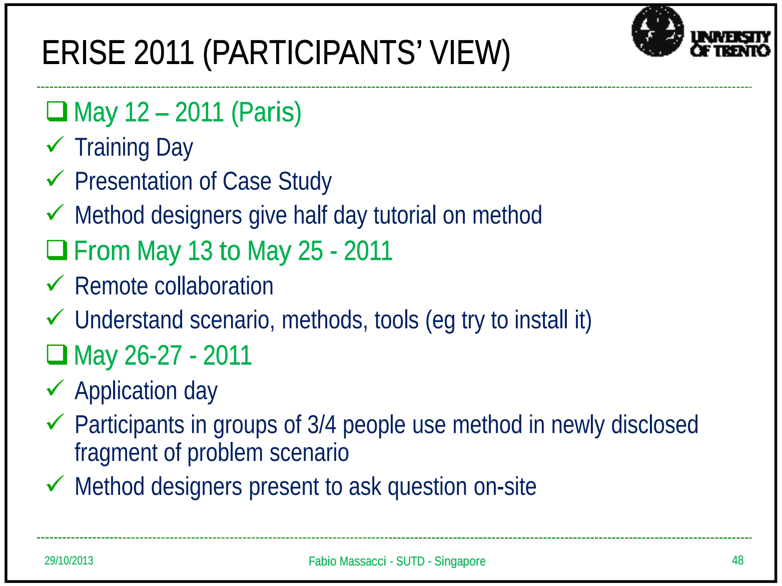
✓ 1 with 16 years as psychologist and project manager

✓ 2 with 10+ years in Risk management and IT audit

✓ 4 with 4+ years of experience in IT audit or software deevelopment

✓ 15 with 2 years in various roles related to audit/MIS etc.

29/10/2013 Fabio Massacci - SUTD - Singapore 47



ERISE 2011 (PARTICIPANTS' VIEW)

❑ May 12 – 2011 (Paris)

✓ Training Day

✓ Presentation of Case Study

✓ Method designers give half day tutorial on method

❑ From May 13 to May 25 - 2011

✓ Remote collaboration

✓ Understand scenario, methods, tools (eg try to install it)

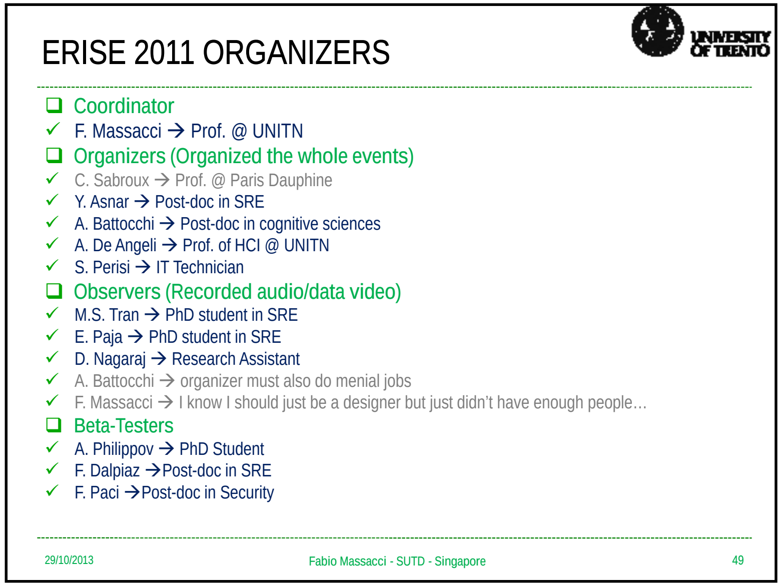
❑ May 26-27 - 2011

✓ Application day

✓ Participants in groups of 3/4 people use method in newly disclosed fragment of problem scenario

✓ Method designers present to ask question on-site

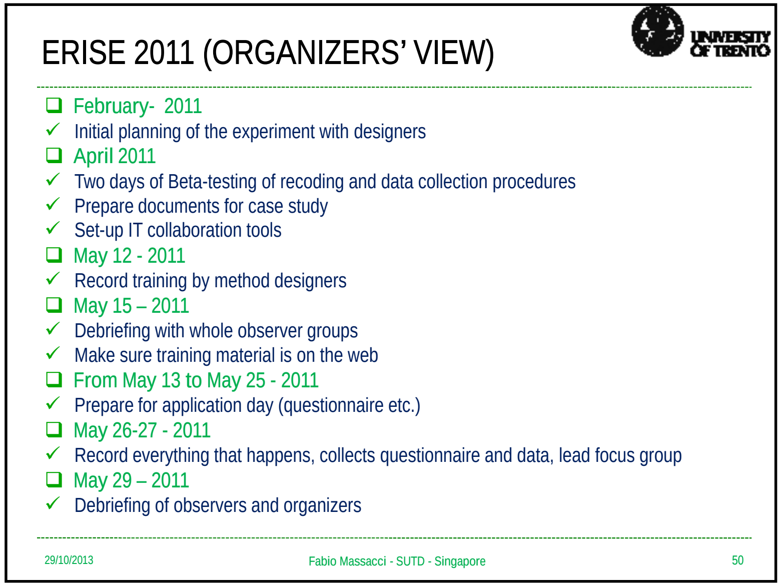
29/10/2013 Fabio Massacci - SUTD - Singapore 48



ERISE 2011 ORGANIZERS

- ❑ Coordinator
- ✓ F. Massacci → Prof. @ UNITN
- ❑ Organizers (Organized the whole events)
- ✓ C. Sabroux → Prof. @ Paris Dauphine
- ✓ Y. Asnar → Post-doc in SRE
- ✓ A. Battocchi → Post-doc in cognitive sciences
- ✓ A. De Angeli → Prof. of HCI @ UNITN
- ✓ S. Perisi → IT Technician
- ❑ Observers (Recorded audio/data video)
- ✓ M.S. Tran → PhD student in SRE
- ✓ E. Paja → PhD student in SRE
- ✓ D. Nagaraj → Research Assistant
- ✓ A. Battocchi → organizer must also do menial jobs
- ✓ F. Massacci → I know I should just be a designer but just didn't have enough people…
- ❑ Beta-Testers
- ✓ A. Philippov → PhD Student
- ✓ F. Dalpiaz →Post-doc in SRE
- ✓ F. Paci →Post-doc in Security

29/10/2013 Fabio Massacci - SUTD - Singapore 49



ERISE 2011 (ORGANIZERS' VIEW)

- ❑ February- 2011
- ✓ Initial planning of the experiment with designers
- ❑ April 2011
- ✓ Two days of Beta-testing of recoding and data collection procedures
- ✓ Prepare documents for case study
- ✓ Set-up IT collaboration tools
- ❑ May 12 - 2011
- ✓ Record training by method designers
- ❑ May 15 – 2011
- ✓ Debriefing with whole observer groups
- ✓ Make sure training material is on the web
- ❑ From May 13 to May 25 - 2011
- ✓ Prepare for application day (questionnaire etc.)
- ❑ May 26-27 - 2011
- ✓ Record everything that happens, collects questionnaire and data, lead focus group
- ❑ May 29 – 2011
- ✓ Debriefing of observers and organizers

29/10/2013 Fabio Massacci - SUTD - Singapore 50