eRISE 2013

Engineering RIsks and SEcurity Requirements

Federica Paci

April 23 2013

THE IDEA OF ERISE

□ Professional use “established” methods

✓ Invented maybe 10-15 years ago, they were proven to work but by keeping using them we might lose opportunities

□ Researchers “invent” new methods

✓ Design new methods to address emerging problems but they don’t really know if they really work

□ eRISE let research “meet” with practice

✓ Students & practitioners are exposed to research methods

✓ Researchers understand if their methods work in practice or not

WHY DO WE NEED YOU?

- □ **So what we need is your help as participants**
- ✓ Provide feedback as the method “work” or “does’t work”

- □ **Thanks to your feedback we will be able to tell:**
- ✓ *“it is not a method to find security recommendations..it helps us to represent the model but does not help in finding solution,” or*
- ✓ *“it helps to find out specific security requirement”*

- □ **We can speed up the road to innovation**

HONEST FEEDBACK IS IMPORTANT

□ Feedback by Participants

- ✓ "Need support or direction to know which security requirement is right. No automated way to give direction to the analysis"
- ✓ "No guidelines to estimate which part of the goal model is to be evaluated further."

□ Insights for Designers

- ✓ "I understood that we need a checklist, people need to do tick, tick, tick so they understand at what stage they are"
- ✓ "Without a guideline people don't know when to stop the analysis"

TRAINING

- □ Attend Lecture By Industrial Experts

Reference standards, best practices and real-life approaches for monitoring and control

- □ Attend Tutorials on the Methods by Designers

Context identification
Characterise target of analysis
What is the focus and scope of the analysis?
Identify and value assets
Asset-driven risk analysis process
Business oriented, e.g. availability of services generating revenue
Specify risk evaluation criteria
There will always be risks, but what losses can the client tolerate?
Similar to requirements in system development
SINTEF

- □ Attend Tutorials on the Case Studies by Customers

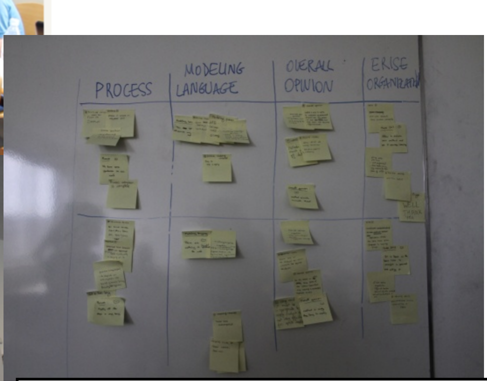
APPLICATION

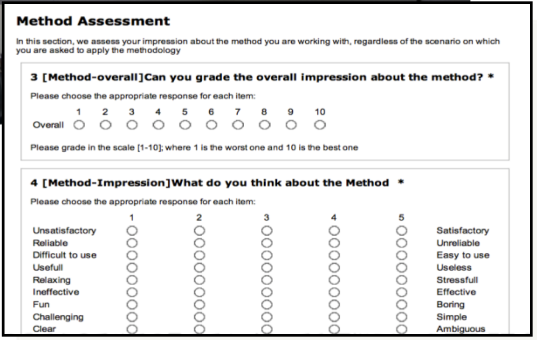
- ❑ **We divide you in groups (1 master student + 1 professional)**
- ❑ **We assign your group to a method and an industrial case**
- ❑ **You and your group mates apply the method to**
  - ✓ analyze threats of the case
  - ✓ identify security/privacy requirements that mitigate the threats
- ❑ **We audio-video record**
- ❑ **An observer will “watch you”**

EVALUATION

❑ You Evaluate the Methods

- ✓ Focus group interviews
  - We ask you questions about what works and what doesn’t
- ✓ Post –it notes sessions
  - You fill post-it notes with methods advantages and disadvantages
  - We ask you to order them by importance
- ✓ Post-Task Questionnaires
  - We ask you questions about usefulness, usability and intention to use the methods





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
Usefull	○	○	○	○	○	Useless
Relaxing	○	○	○	○	○	Stressfull
Ineffective	○	○	○	○	○	Effective
Fun	○	○	○	○	○	Boring
Challenging	○	○	○	○	○	Simple
Clear	○	○	○	○	○	Ambiguous

HOW YOU WILL BE EVALUATED?

❑ Method Designers and Customers Evaluate your "Final Products"

✓ **Presentation at end of the week in Trento**

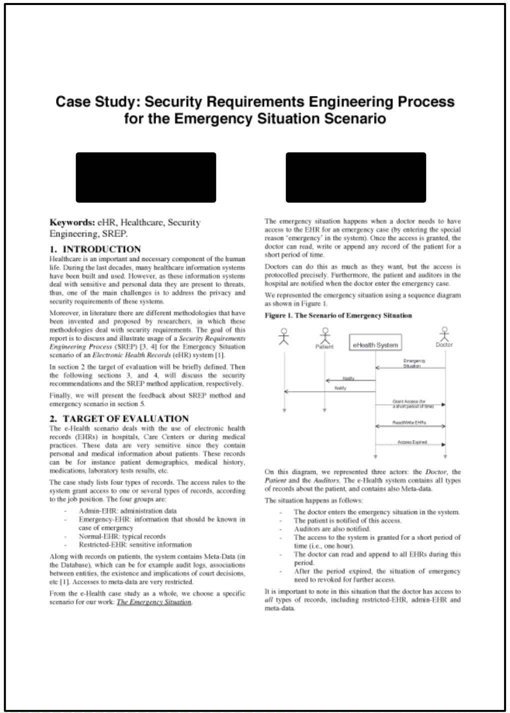
- What results do you have up to now e.g We have applied steps X and Y of method Z

✓ **Presentation at end of Paris' days**

- Summary of threats and security/privacy requirements identified with the method

✓ **Final 6 pages report**

- Target of Evaluation: Part of the case study analyzed with the method (1 page)
- Method Applications: Steps, Models, Diagrams, Tables etc (4 pages)
- Results: Threats and security/privacy requirements identified with the method (1 page)



Case Study: Security Requirements Engineering Process for the Emergency Situation Scenario

[redacted]

[redacted]

Keywords: eHR, Healthcare, Security Engineering, SREP.

1. INTRODUCTION

Healthcare is an important and necessary component of the human life. During the last decades, many healthcare information systems have been built and used. However, as these information systems deal with sensitive and personal data they are present to threats, thus, one of the main challenges is to address the privacy and security requirements of these systems.

Moreover, in literature there are different methodologies that have been invented and proposed by researchers, in which these methodologies deal with security requirements. The goal of this report is to discuss and illustrate usage of a *Security Requirements Engineering Process* (SREP) [3, 4] for the Emergency Situation scenario of an *Electronic Health Records* (eHR) system [1].

In section 2 the target of evaluation will be briefly defined. Then the following sections 3, and 4, will discuss the security recommendations and the SREP method application, respectively.

Finally, we will present the feedback about SREP method and emergency scenario in section 5.

2. TARGET OF EVALUATION

The e-Health scenario deals with the use of electronic health records (EHRs) in hospitals, Care Centers or during medical practices. These data are very sensitive since they contain personal and medical information about patients. These records can be for instance patient demographics, medical history, medications, laboratory tests results, etc.

The case study lists four types of records. The access rules to the system grant access to one or several types of records, according to the job position. The four groups are:

- Admin-EHR: administration data
- Emergency-EHR: information that should be known in case of emergency
- Normal-EHR: typical records
- Restricted-EHR: sensitive information

Along with records on patients, the system contains Meta-Data (in the Database), which can be for example audit logs, associations between entities, the existence and implications of court decisions, etc [1]. Accesses to meta-data are very restricted.

From the e-Health case study as a whole, we choose a specific scenario for our work: <u>*The Emergency Situation*</u>.

The emergency situation happens when a doctor needs to have access to the EHR for an emergency case (by entering the special reason 'emergency' in the system). Once the access is granted, the doctor can read, write or append any record of the patient for a short period of time.

Doctors can do this as much as they want, but the access is protocolled precisely. Furthermore, the patient and auditors in the hospital are notified when the doctor enter the emergency case.

We represented the emergency situation using a sequence diagram as shown in Figure 1.

Figure 1. The Scenario of Emergency Situation

On this diagram, we represented three actors: the *Doctor*, the *Patient* and the *Auditors*. The e-Health system contains all types of records about the patient, and contains also Meta-data.

The situation happens as follows:

- The doctor enters the emergency situation in the system.
- The patient is notified of this access.
- Auditors are also notified.
- The access to the system is granted for a short period of time (i.e., one hour).
- The doctor can read and append to all EHRs during this period.
- After the period expired, the situation of emergency need to revoked for further access.

It is important to note in this situation that the doctor has access to *all* types of records, including restricted-EHR, admin-EHR and meta-data.

ERISE 2013 ORGANIZATION

❑ Training Phase

- ✓ **May 13-15 2013** at the University of Trento, Italy

❑ Application Phases

- ✓ **May 16-17 2013** at the University of Trento, Italy
- ✓ **June 13-14 2013** at Dauphine University, Paris, France

❑ Evaluation Phase

- ✓ **June 14 2013** Focus Groups and Post-it notes sessions with participants, at Dauphine University, Paris, France
- ✓ **June 30 2013** Delivery of Group Final Reports
- ✓ **June 30-July 15 2013** Reports Assessment by method designers and customers

EVALUATED METHODS

- **CORAS:** Model- Driven Risk Analysis method by SINTEF

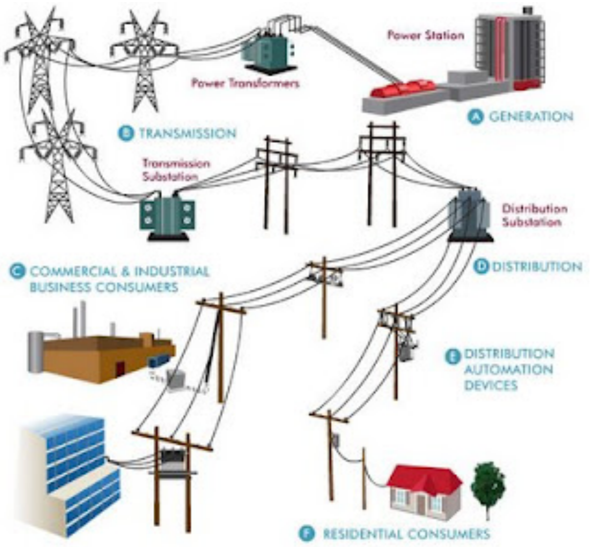
- **LINDDUN:** Method for Privacy Threats Analysis and Privacy Requirements Elicitation by KUL

- **Multilateral Privacy Requirements Analysis** by KUL

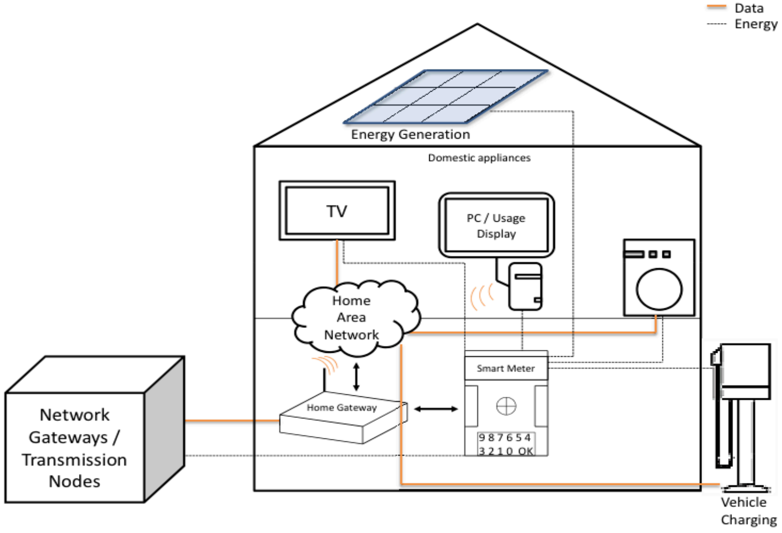
- **SREP:** Risk and Asset Driven Method for Security Requirements Elicitation by UCLM

SMART GRID – USE CASES

- □ Electricity Transmission Network (National Grid,UK)



- □ Smart Home (Siemens,DE)



WEEK IN TRENTO – MAY 13TH

- 9.00-11.00 - eRISE 2013 Organization and Group Assignment

- 11.00-12.00 Lecture on Business & ICT resilience: reference standards, best practices and real-life approaches for monitoring and control: Dr. A. Carone, KPMG (IT)

- 12.00-14.0 Lunch

- 14.00-15.00 “Manage Security Services". P. Sartori –CISSP – Informatica Trentina

- 15.00-16.00 Group Activity

WEEK IN TRENTO – MAY 14TH

- ❑ 9.00-10.00 CASE STUDY: Smart Grid: Dr. R. Ruprai, NATIONAL GRID (UK)

- ❑ 10.00-11.00 Lecture From Industrial Security Expert

- ❑ 11.00-12.00 Smart Grid Security Threats. Dr. R. Ruprai , NATIONAL GRID (UK)

- ❑ 12.00 – 14.00 Lunch

- ❑ 14.00-17.00 Tutorials in parallel
- ✓ **LINDDUNN**, K. Wuyts, R. Scandariato. Katholieke Univ. Leuven (BE)

- ✓ **MULTILATERAL PRIVACY REQUIREMENTS ANALYSIS**, Dr. S. Guerses, Katholieke Univ. Leuven (BE)

WEEK IN TRENTO – MAY 15TH

- ❑ 9.00-10.00 CASE STUDY: Smart-Grid: Dr. J. Stijohann – SIEMENS (DE)

- ❑ 10.00-13.00 Tutorials in Parallel

- ✓ **CORAS**. M. S. Tran, Univ. of Trento (IT)/SINTEF(NO)

- ✓ **SREP**. D. Mellado, Univ. Castilla La Mancha (ES)

- ❑ Afternoon is free for participants

WEEK IN TRENTO – MAY 16TH

- ❑ 9.00-9.30 Groups distribution to the Aulas
- ❑ 9.30-12.00 Teamwork on risks and security and privacy requirements – Method Application
- ❑ 12.00-14.0 Lunch
- ❑ 14.00-15.00 Teamwork on risks and security and privacy requirements – Method Application

WEEK IN TRENTO – MAY 17TH

- 9.00-12.00 Teamwork on risks and security and privacy requirements for each method – Presentation Preparation

- 12.00-14.00 Lunch

- 14.00-17.00 Group presentations (10 min each)

- 17.00-17.30 End of the first phase of the challenge

ERISE 2013 - SECOND PHASE

UNIVERSITY
OF TRENTO - Italy

TWO DAYS IN PARIS – JUNE 13TH

❑ **9.00-9.30** Objectives and expected outcomes

❑ **9.30-12.00** Teamwork on risks and security and privacy requirements for each method

❑ **12.00-13.00** Lunch

❑ **13.00-17.00** Teamwork on risks and security and privacy requirements for each method - Presentation Preparation

TWO DAYS IN PARIS – JUNE 14TH

□ **9.00-10.30** Post-it notes sessions

□ **10.30-11.00 Coffee Break**

□ **11.00-13.00** Focus Group Interviews

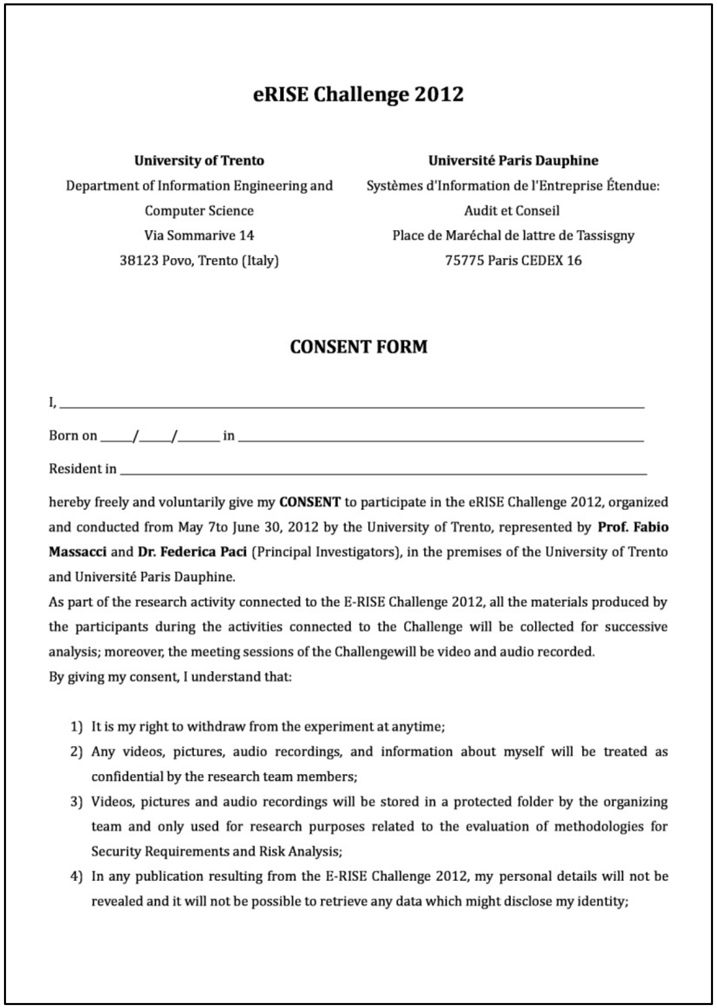
□ **13.00 -14.00** Lunch

□ **14.00 -17.00** Group presentations (10 min each)

□ **17.00-17.30** End of the challenge

YOUR RIGHTS AS PARTICIPANTS

- □ **We don't collect personal information**
  - ✓ Data are anonymized e.g we just use your initials
  - ✓ Recordings will not be shown to anyone, just tagged for analysis
    - how many hours Group1 spent discussing privacy?
- □ **Feel "too" observed?**
  - ✓ Just say so and we can stop recording
- □ **Think your drawings are too bad?**
  - ✓ No need to show them. Just say so.
- □ **Some feedback will be lost in this way, but so be it...**
- □ **The consent form tells your rights in complicated legal terms**



eRISE Challenge 2012

University of Trento
Department of Information Engineering and
Computer Science
Via Sommarive 14
38123 Povo, Trento (Italy)

Université Paris Dauphine
Systèmes d'Information de l'Entreprise Étendue:
Audit et Conseil
Place de Maréchal de lattre de Tassigny
75775 Paris CEDEX 16

CONSENT FORM

I, ____

Born on ____/____/_____ in ______________________________

Resident in ____

hereby freely and voluntarily give my **CONSENT** to participate in the eRISE Challenge 2012, organized and conducted from May 7to June 30, 2012 by the University of Trento, represented by **Prof. Fabio Massacci** and **Dr. Federica Paci** (Principal Investigators), in the premises of the University of Trento and Université Paris Dauphine.

As part of the research activity connected to the E-RISE Challenge 2012, all the materials produced by the participants during the activities connected to the Challenge will be collected for successive analysis; moreover, the meeting sessions of the Challengewill be video and audio recorded.

By giving my consent, I understand that:

1) It is my right to withdraw from the experiment at anytime;
2) Any videos, pictures, audio recordings, and information about myself will be treated as confidential by the research team members;
3) Videos, pictures and audio recordings will be stored in a protected folder by the organizing team and only used for research purposes related to the evaluation of methodologies for Security Requirements and Risk Analysis;
4) In any publication resulting from the E-RISE Challenge 2012, my personal details will not be revealed and it will not be possible to retrieve any data which might disclose my identity;

WHERE CAN YOU FIND INFORMATION ABOUT ERISE?

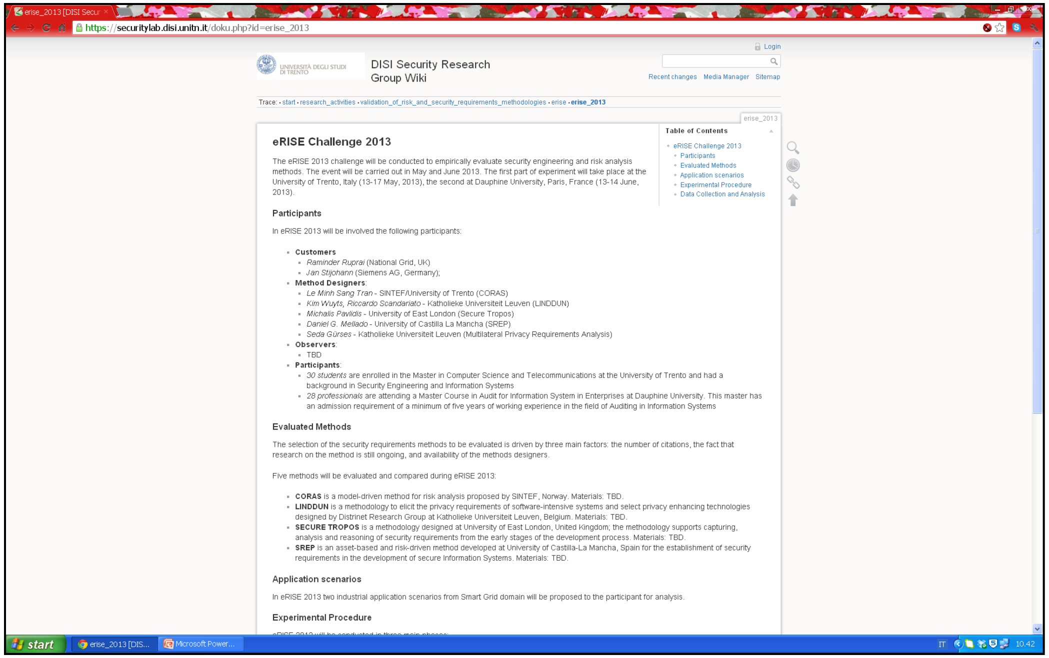
- ❑ https://securitylab.disi.unitn.it/doku.php?id=erise_2013
- ❑ You can find:

✓ Agendas

✓ Training Material
- Case Study Descriptions
- Tutorials on Methods

✓ Final Report Template

✓ Contact Information
- Organizers
- Method Designers
- Customers



DISI Security Research Group Wiki

Trace: · start · research_activities · validation_of_risk_and_security_requirements_methodologies · erise · **erise_2013**

eRISE Challenge 2013

The eRISE 2013 challenge will be conducted to empirically evaluate security engineering and risk analysis methods. The event will be carried out in May and June 2013. The first part of experiment will take place at the University of Trento, Italy (13-17 May, 2013), the second at Dauphine University, Paris, France (13-14 June, 2013).

Participants

In eRISE 2013 will be involved the following participants:

- **Customers**
  - *Raminder Ruprai* (National Grid, UK)
  - *Jan Stijohann* (Siemens AG, Germany);
- **Method Designers**:
  - *Le Minh Sang Tran* - SINTEF/University of Trento (CORAS)
  - *Kim Wuyts, Riccardo Scandariato* - Katholieke Universiteit Leuven (LINDDUN)
  - *Michalis Pavlidis* - University of East London (Secure Tropos)
  - *Daniel G. Mellado* - University of Castilla La Mancha (SREP)
  - *Seda Gürses* - Katholieke Universiteit Leuven (Multilateral Privacy Requirements Analysis)
- **Observers**:
  - TBD
- **Participants**:
  - *30 students* are enrolled in the Master in Computer Science and Telecommunications at the University of Trento and had a background in Security Engineering and Information Systems
  - *28 professionals* are attending a Master Course in Audit for Information System in Enterprises at Dauphine University. This master has an admission requirement of a minimum of five years of working experience in the field of Auditing in Information Systems

Evaluated Methods

The selection of the security requirements methods to be evaluated is driven by three main factors: the number of citations, the fact that research on the method is still ongoing, and availability of the methods designers.

Five methods will be evaluated and compared during eRISE 2013:

- **CORAS** is a model-driven method for risk analysis proposed by SINTEF, Norway. Materials: TBD.
- **LINDDUN** is a methodology to elicit the privacy requirements of software-intensive systems and select privacy enhancing technologies designed by Distrinet Research Group at Katholieke Universiteit Leuven, Belgium. Materials: TBD.
- **SECURE TROPOS** is a methodology designed at University of East London, United Kingdom; the methodology supports capturing, analysis and reasoning of security requirements from the early stages of the development process. Materials: TBD.
- **SREP** is an asset-based and risk-driven method developed at University of Castilla-La Mancha, Spain for the establishment of security requirements in the development of secure Information Systems. Materials: TBD.

Application scenarios

In eRISE 2013 two industrial application scenarios from Smart Grid domain will be proposed to the participant for analysis.

Experimental Procedure

eRISE 2013 will be conducted in three main phases:

ORGANIZING TEAM

❑ Organizers:

- Federica Paci → paci@disi.unitn.it
- Fabio Massacci → Fabio.Massacci@unitn.it

❑ Observers:

- Tong Li
- Katsiaryna Labunets
- Martina Degramatica
- Mattia Salnitri

WHAT PARTICIPANTS SAY ABOUT ERISE?

The Video is Available on YouTube at
http://www.youtube.com/watch?v=6pCwWfDvnHY

Any Question?