An Experiment on Comparing Textual vs. Visual Industrial Methods for Security Risk Assessment

Katsyarina Labunets, Federica Paci, Fabio Massacci
University of Trento
August 25th 2014

Outline

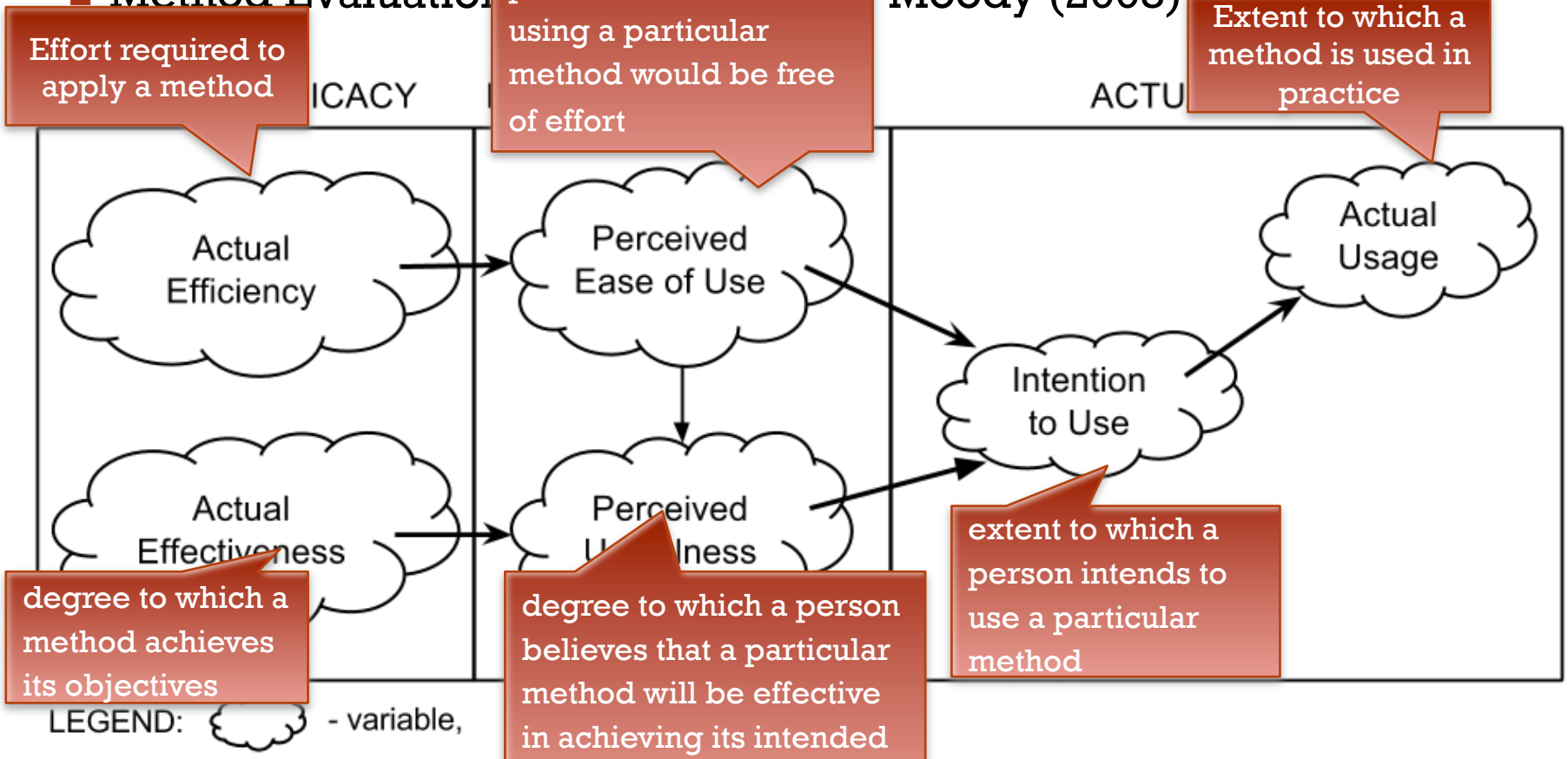
- Motivation
- Research Questions
- Design and Execution
- Analysis and Results
- Conclusions

Motivation

- Many methods for identifying security concerns early in the software development lifecycle
  - They should avoid costly re-design of the system
- *What if these methods do not work in practice?*
  - No critical vulnerabilities are identified
  - You spend money to fix the system later

How to Evaluate Method Success?

- Method Evaluation … Moody (2003)

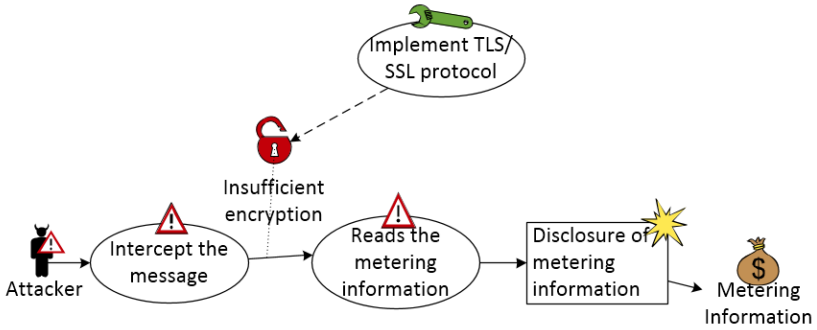


Research Questions

- **Actual Effectiveness**
  - *Is there a difference in visual and textual methods' actual effectiveness?*
- **Method's Perception**
  - *Is there a difference in visual and textual methods' **perceived easy of use (PEOU)**?*
  - *Is there a difference in visual and textual methods' **perceived usefulness (PU)**?*
  - *Is there a difference in visual and textual participants' **intention to use (ITU)** the methods?*
- **Qualitative Explanations**
  - *Is there a qualitative driver that explains why a method is more successful than an another?*

Design & Execution: Methods

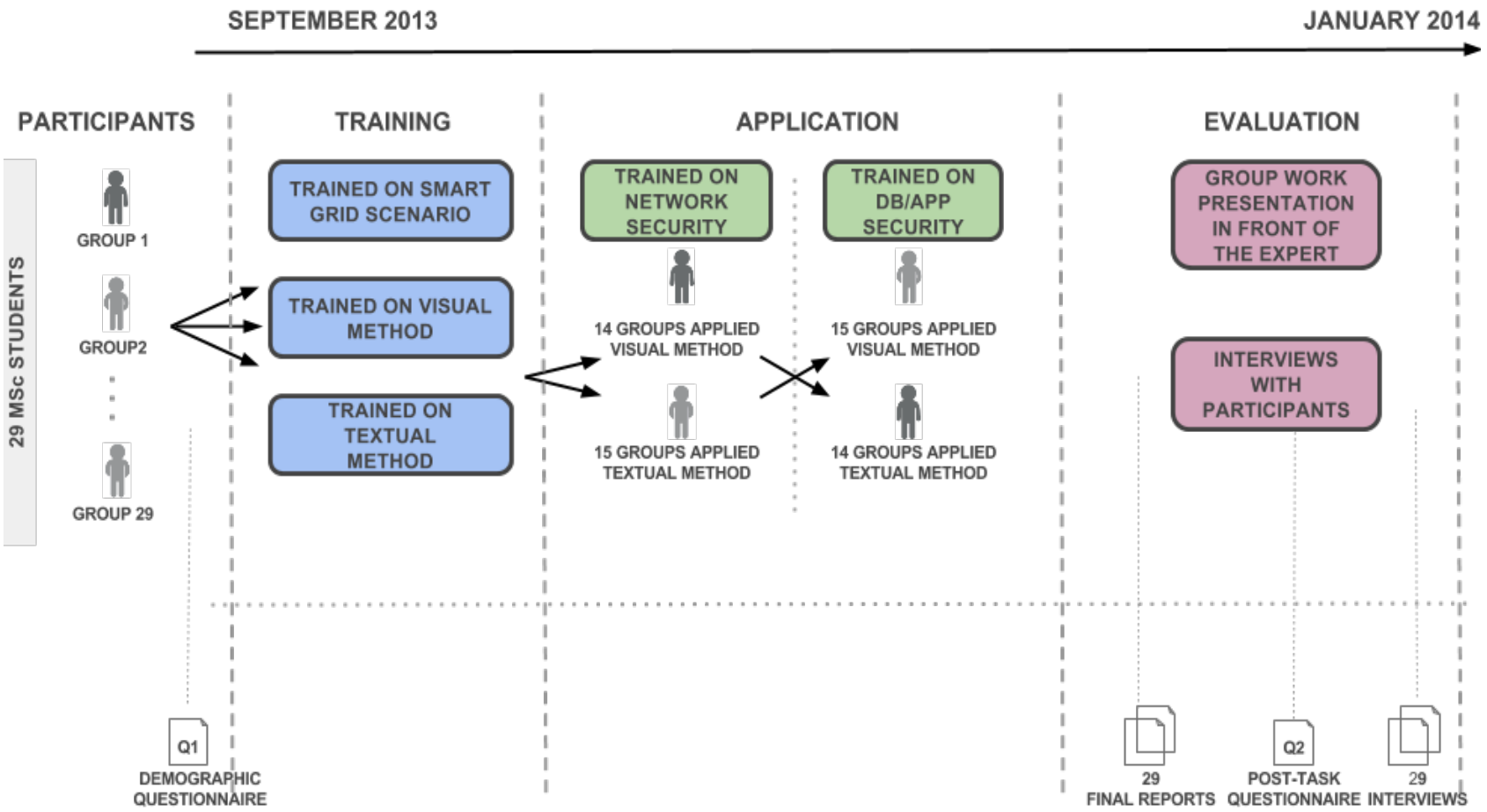
- **CORAS**
  - Model-driven method for risk analysis developed by SINTEF
  - Provides a language for risk modeling, a tool and method for risk analysis
  - Compliant with ISO 31000



- **EUROCONTROL ATM Security Risk Management Toolkit**
  - Method to identify, assess, document and manage security risks
  - Facilitate security risk management in a project development life cycle
  - Compliant with ISO 31000

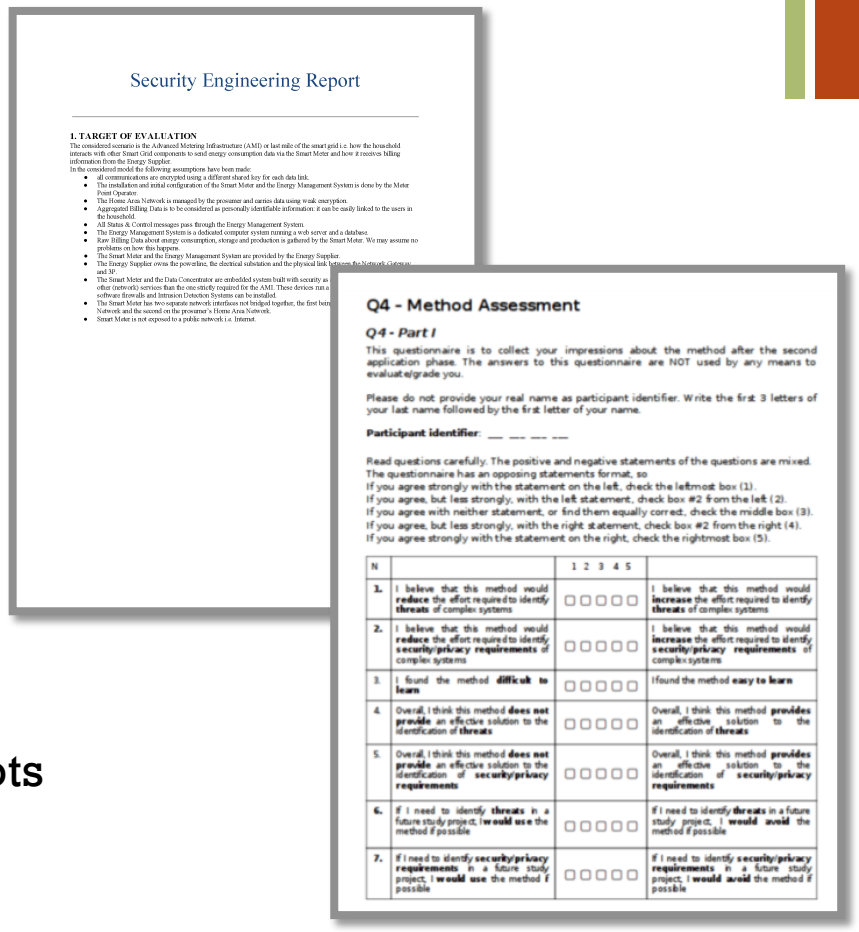
Threat Agent	Asset Attacked	Attack Likelihood	Justification
Compromised MPO	SM, EMS	Probable	Can use message replay attack and access customer data
Malicious attacker	EMS, HAN, SA, S&C	Probable	By Eavesdropping and Sniffing on the HAN, can use DOS attack to deny availability of HAN, Hacking the EMS and tampering the S&C and accessing the SA

Design & Execution: Procedure



Design & Execution: Measurements

- **Actual Effectiveness**
  - Participants Reports
    - Statistical Analysis
- **Perception**
  - Post-Task Questionnaire
    - Statistical Analysis
- **Qualitative Drivers**
  - Individual Interviews' Transcripts
    - Coding (Grounded Theory)



Security Engineering Report

1. TARGET OF EVALUATION

The considered scenario is the Advanced Metering Infrastructure (AMI) or last mile of the smart grid i.e. how the household interacts with other Smart Grid components to send energy consumption data via the Smart Meter and how it receives billing information from the Energy Supplier.
In the considered model the following assumptions have been made:

- All communications are encrypted using a different shared key for each data link.
- The installation and initial configuration of the Smart Meter and the Energy Management System is done by the Meter Point Operator.
- The Home Area Network is managed by the prosumer and carries data using weak encryption.
- Aggregated Billing Data is to be considered as personally identifiable information: it can be easily linked to the users in the household.
- All Status & Control messages pass through the Energy Management System.
- The Energy Management System is a dedicated computer system running a web server and a database.
- Raw Billing Data about energy consumption, storage and production is gathered by the Smart Meter. We may assume no problems on how this happens.
- The Smart Meter and the Energy Management System are provided by the Energy Supplier.
- The Energy Supplier owns the powerline, the electrical substation and the physical link between the Network Gateway and SP.
- The Smart Meter and the Data Concentrator are embedded system built with security as other (network) services than the one strictly required for the AMI. These devices run a software firewalls and Intrusion Detection Systems can be installed.
- The Smart Meter has two separate network interfaces not bridged together, the first being Network and the second on the prosumer's Home Area Network.
- Smart Meter is not exposed to a public network i.e. Internet.

Q4 - Method Assessment

Q4 - Part I

This questionnaire is to collect your impressions about the method after the second application phase. The answers to this questionnaire are NOT used by any means to evaluate/grade you.

Please do not provide your real name as participant identifier. Write the first 3 letters of your last name followed by the first letter of your name.

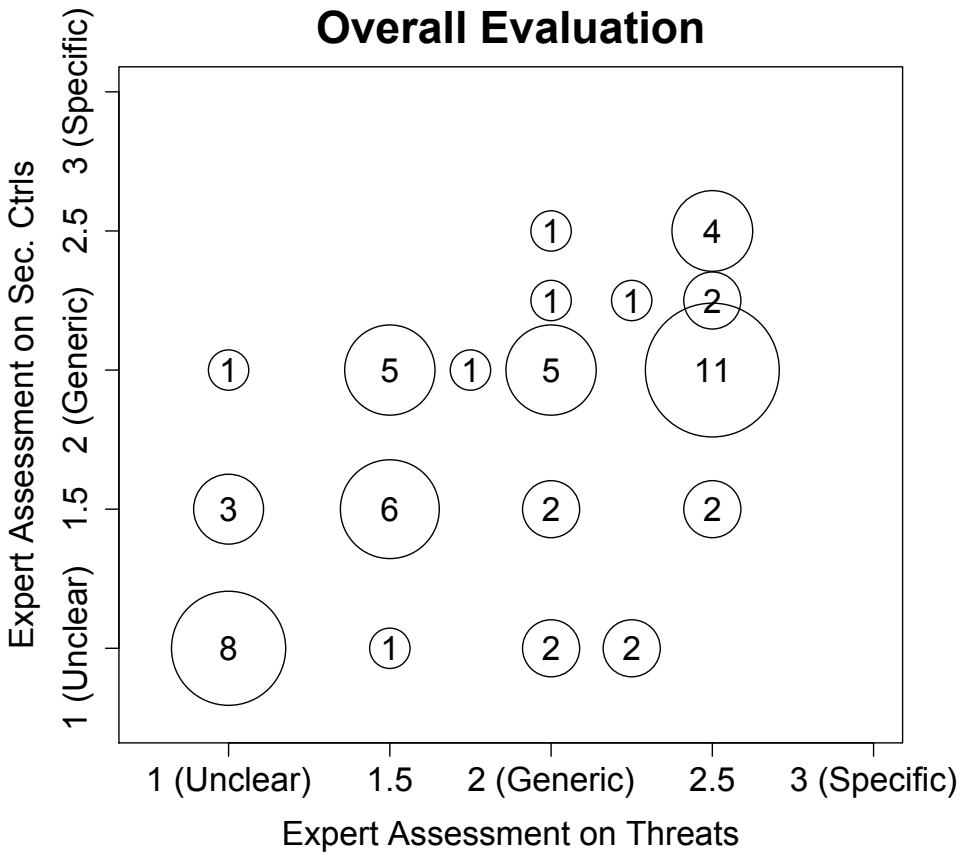
Participant identifier: __ __ __ __

Read questions carefully. The positive and negative statements of the questions are mixed.
The questionnaire has an opposing statements format, so
If you agree strongly with the statement on the left, check the leftmost box (1).
If you agree, but less strongly, with the left statement, check box #2 from the left (2).
If you agree with neither statement, or find them equally correct, check the middle box (3).
If you agree, but less strongly, with the right statement, check box #2 from the right (4).
If you agree strongly with the statement on the right, check the rightmost box (5).

N		1 2 3 4 5	
1.	I believe that this method would **reduce** the effort required to identify **threats** of complex systems	☐☐☐☐☐	I believe that this method would **increase** the effort required to identify **threats** of complex systems
2.	I believe that this method would **reduce** the effort required to identify **security/privacy requirements** of complex systems	☐☐☐☐☐	I believe that this method would **increase** the effort required to identify **security/privacy requirements** of complex systems
3.	I found the method **difficult to learn**	☐☐☐☐☐	I found the method **easy to learn**
4.	Overall, I think this method **does not provide** an effective solution to the identification of **threats**	☐☐☐☐☐	Overall, I think this method **provides** an effective solution to the identification of **threats**
5.	Overall, I think this method **does not provide** an effective solution to the identification of **security/privacy requirements**	☐☐☐☐☐	Overall, I think this method **provides** an effective solution to the identification of **security/privacy requirements**
6.	If I need to identify **threats** in a future study project, I **would use** the method if possible	☐☐☐☐☐	If I need to identify **threats** in a future study project, I **would avoid** the method if possible
7.	If I need to identify **security/privacy requirements** in a future study project, I **would use** the method if possible	☐☐☐☐☐	If I need to identify **security/privacy requirements** in a future study project, I **would avoid** the method if possible

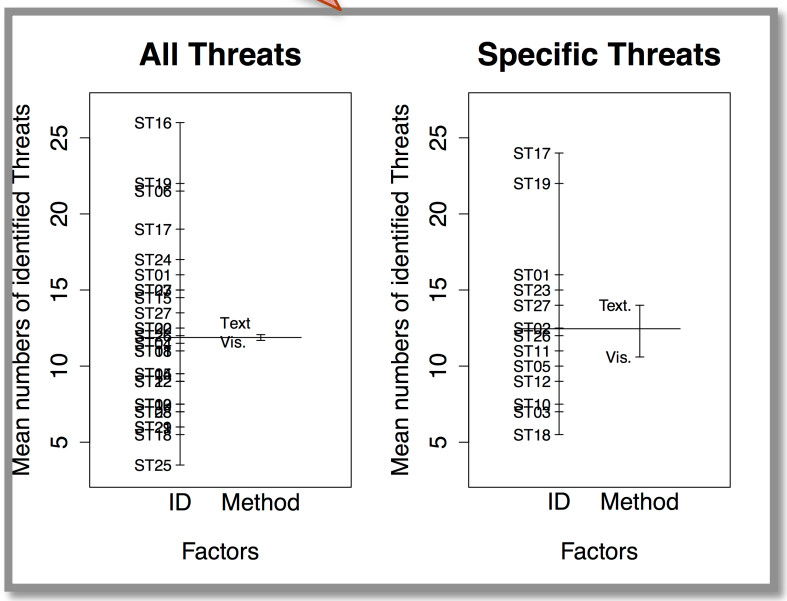
Analysis and Results: Actual Effectiveness (1)

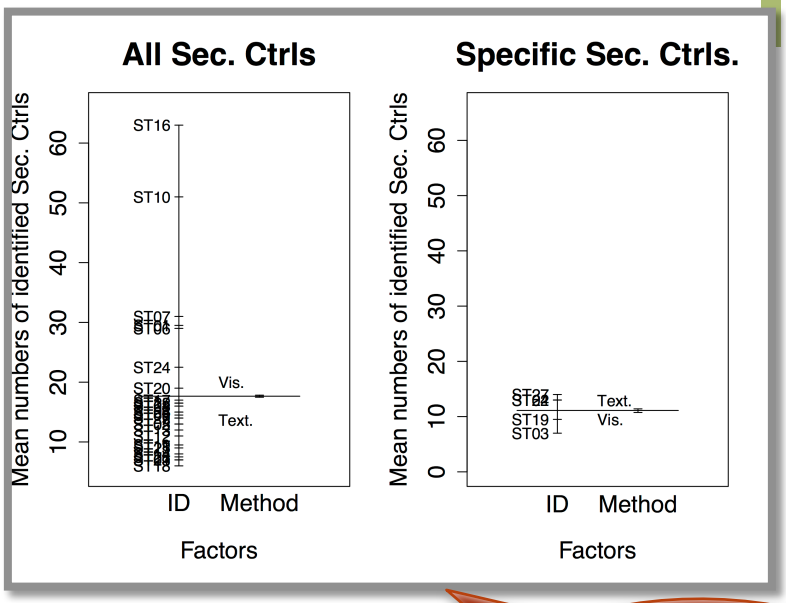
- A method is **effective** when it produces "good" threats and controls for the **target of analysis**
- Domain experts evaluate quality of threats and security controls
- Good threats/controls
  - Evaluation > 2
  - 24 out 58 method's application produced some good threats/ controls



& Results: Actual veness (2)

Not statistically significant

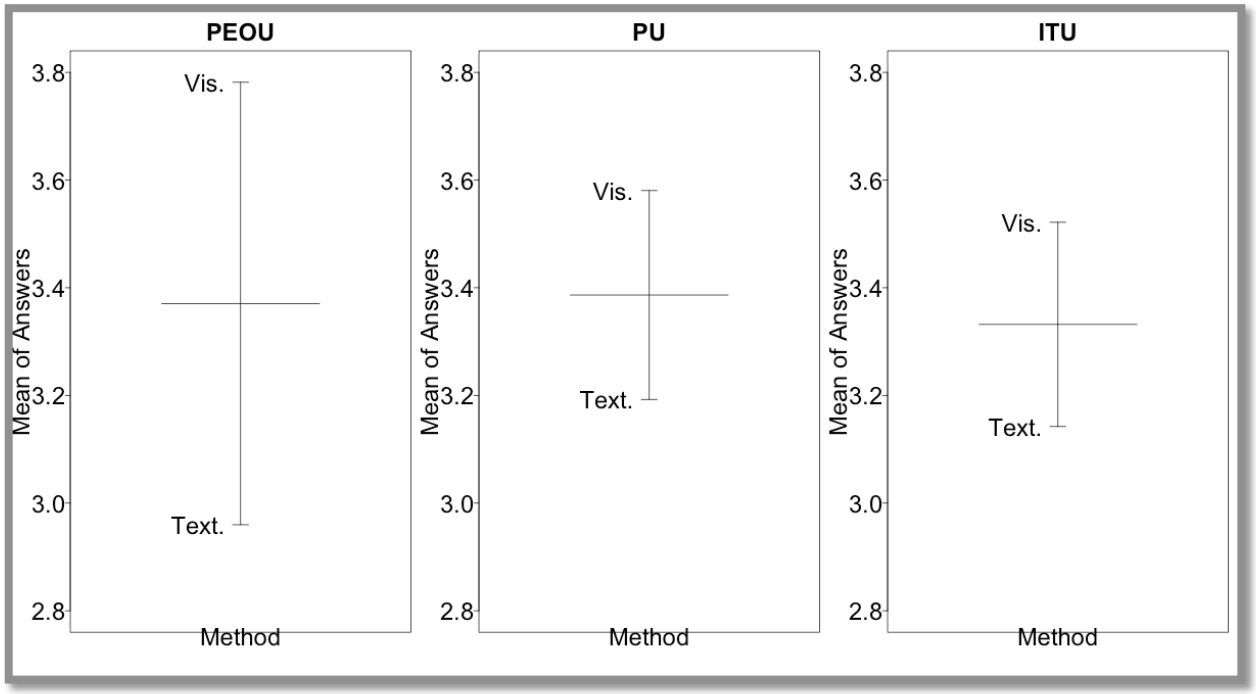




Not statistically significant

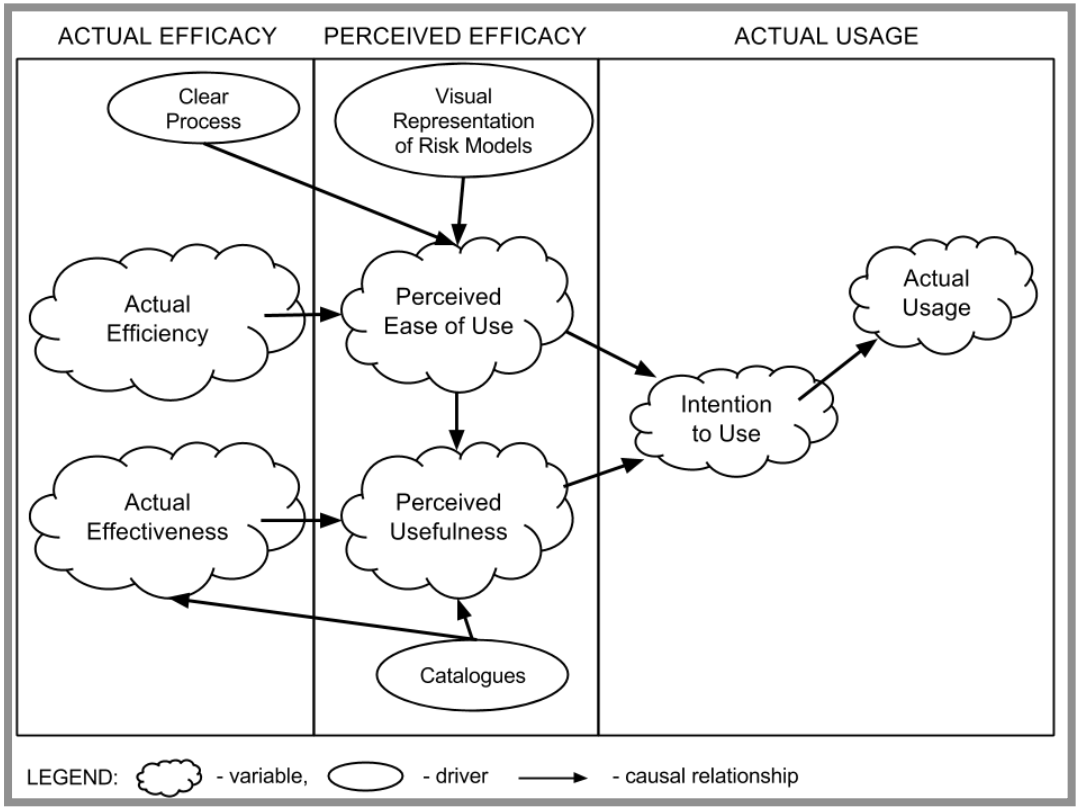
- **Reports Analysis**
  - **Threats**
    - **Textual method performs better (good threats)**
  - **Security Controls**
    - No difference between the methods (both)

Analysis & Results: Perception



- **Questionnaires Analysis**
  - Perceived easy of use, perceived usefulness, and intention to use is **higher for visual method**
  - Results are statistically significant
    - Mann-Whitney test reports p-value < 0.05

Analysis & Results: Qualitative Drivers



- **Interview Analysis**
  - 15 codes
- **Reported Statements**
  - **Clear Process**
    - *The steps are very well defined*
  - **Visual Representation**
    - *The advantage is the visualization*
  - **Catalogues**
    - *If you have a catalogues it's easier to decide what to do*

Conclusions

- No difference in actual effectiveness of visual and textual methods for security risk assessment
- Visual methods for security risk assessment are better perceived by participants
- What works
  - Clear Process → Perceived Easy of Use
  - Visual Representation → Perceived Easy of Use
  - Catalogues → Perceived Usefulness
- Next Steps
  - Compare results with the replication with professionals
  - Comprehensibility of visual and textual representation

Any Question?

Experiment(s) Context