ENGINEERING PRIVACY REQUIREMENTS: VALUABLE LESSONS FROM ANOTHER REALM

Yod Samuel Martín García
Dpt. Ingeniería de Sistemas Telemáticos
Universidad Politécnica De Madrid

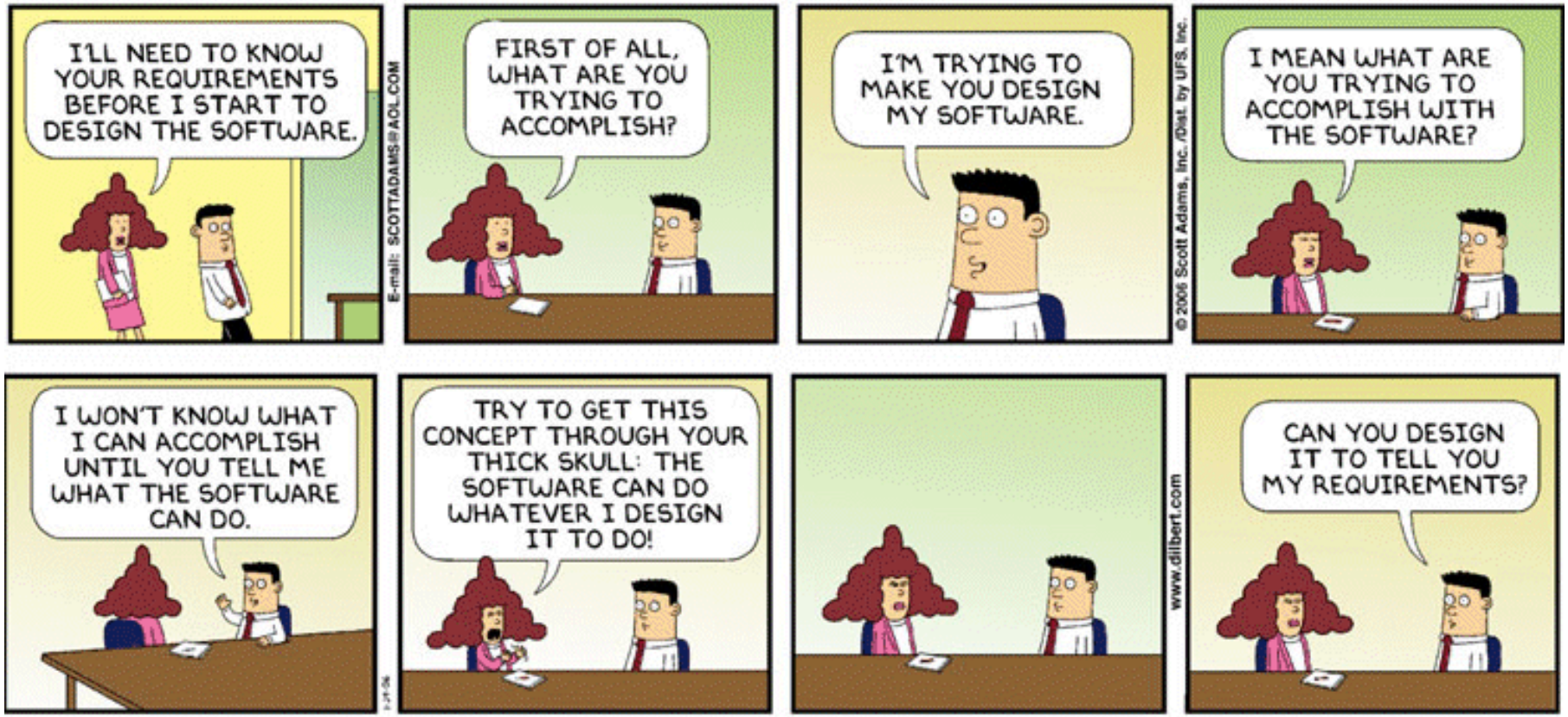
ESPRE 2014
Karlskrona, Aug 28 2014

What am I talking about?

- A category of NFRs
- A quality attribute
- A factor of user experience
- Best if built in since inception
- Interdisciplinary
- Often legally mandated
- Often overlooked
- A Digital Human Right
- A component of CSR
- There is a workshop at RE'14

~~**PRIVACY?**~~

Privacy reqs? Which requirements?



What am I talking about?

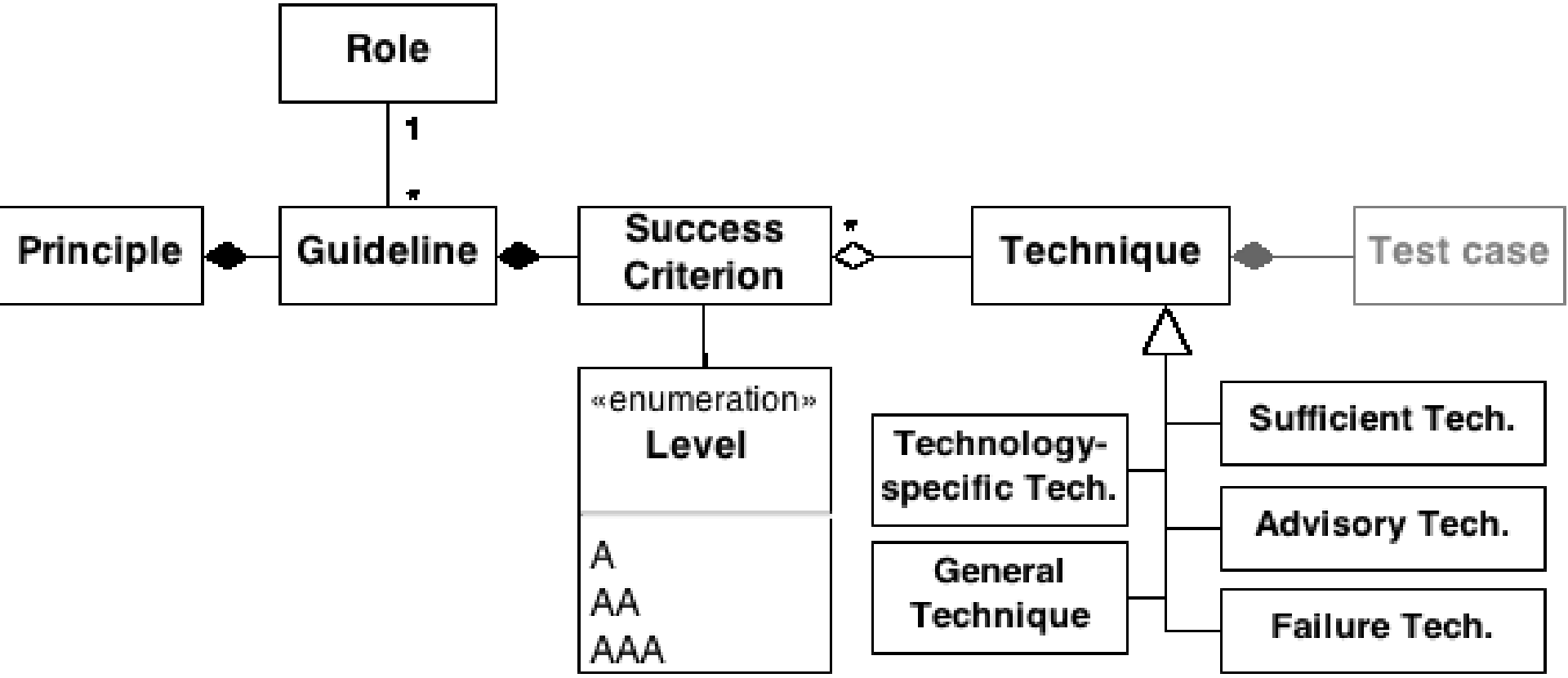
- A category of NFRs
- A quality attribute
- A factor of user experience
- Best if built in since inception
- Interdisciplinary
- Often legally mandated
- Often overlooked
- A Digital Human Right
- A component of CSR
- There is a workshop at RE'14

~~PRIVACY?~~

- Expressed a set of universal requirements
  - Product- and service-independent
  - Stakeholder-neutral
  - Structured and hierarchized
  - Prioritized
  - Standardized catalogue

ACCESSIBILITY

A Proposal to Structure Privacy Requirements

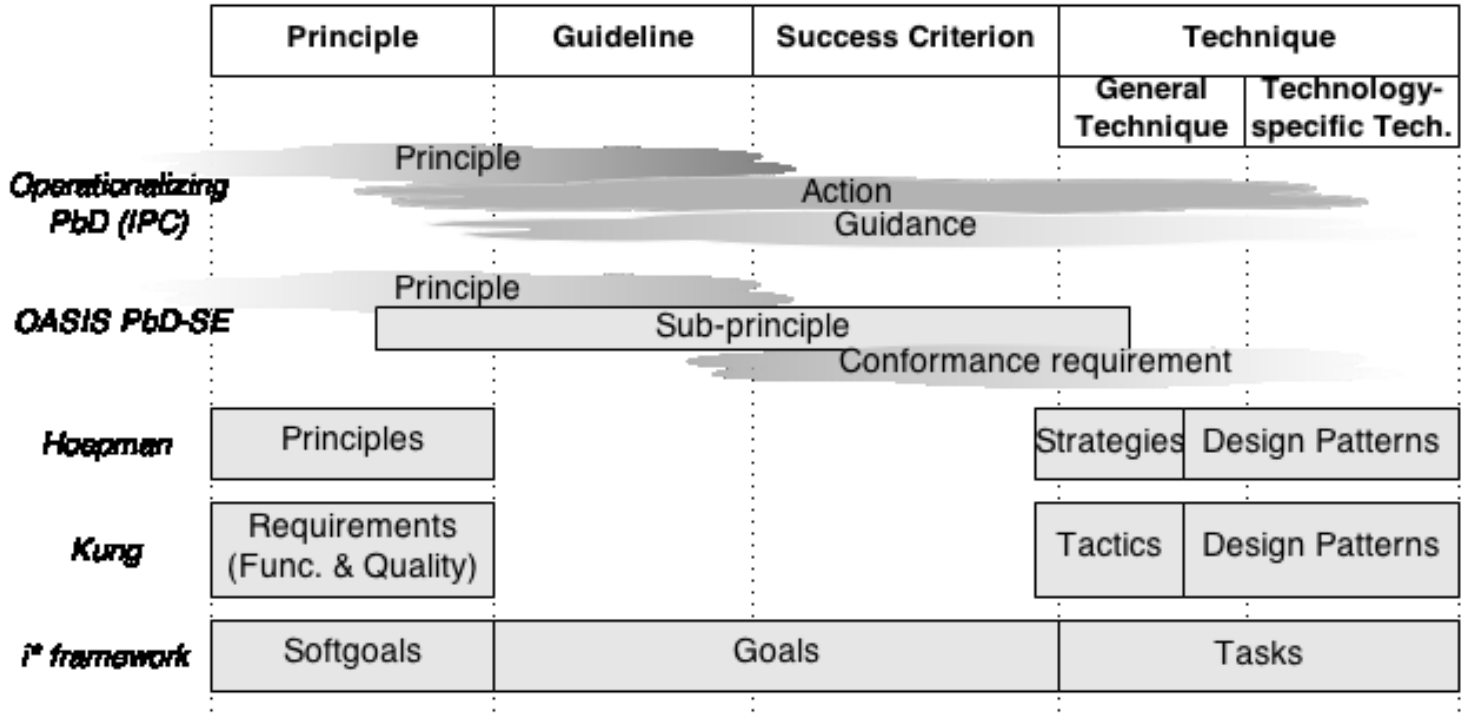


What is already there?

- Families of Privacy Principles:
  - FIPs, OECD's, EU DPD + GDPR, EU-US Safe Harbor, US FTC FIPPs, APEC's
  - Convergence: ISO/IEC 29100, ISTPA and OASIS PMRM
  - PbD foundational principles, academic proposals…
- Roles:
  - Data Subject / Controller / Processor
  - Stakeholder lists
  - Function lists
- Technique catalogues:
  - Many Privacy Enhancing Technologies (PETs)
  - Pattern Collections (PriS, PRIPARE)
  - PMRM, ISO/IEC 29101, NIST Privacy Controls

What is already there?

- Structured privacy requirements and methodologies for privacy requirement elicitation:



- Data-flow: Privacy Impact Analysis (PIAs), Privacy Distillation
- (Anti-)goal-based: KAOS, i*…
- SQuaRE (ISO 25010) based
- Heuristics-based: Proportionality Method

What is missing?

- A catalogue of requirements which are:
  - Stakeholder-neutral
  - Structured
  - Standardized
  - Prioritized
- A neutral point: ISO? OASIS?
- Know whether the approach is applicable
  - STS vs HCI
  - Country differences
  - etc.

Questions?

- What else is already there?
- What difficulties could hinder this approach?
- What would be necessary for it to succeed?
- Any other questions
- Even more questions: samuelm@dit.upm.es