Conflicting Incentives
Risk Analysis

Finse FRISC/COINS winter School 2013

Work in progress

Einar Snekkenes

Overview

- Reflections on Risk
- CIRA – The method
- CSRP – Sanitized Risk Analysis
- Scenario Description
- Exercise – CSRP + CIRA
- Plenary discussion of case

Reflections on Risk

Einar Snekkenes

Research

Questioning old `truth's´ ?

Or

Solving new problems ?

For the future

- Be better at distinguishing between
  - facts,
  - truths,
  - assumtions,
  - hypothesis,
  - beliefs,
  - etc.

Risk analysis

- What is `Risk´?
- Why are we doing Risk Analysis/Management?

But first some critical thinking…

- How should we interprete the following protocol description?

  A -> B: Na

  B -> A: {Na}kB

Where A,B refers to Alice and Bob, Na is a nonce, {}k denotes encryption.

What are the implicit assumptions?

Consider the following issues

- How many principals are there?
- What can the principals do?

- Two principals?
- Alice can decrypt (xor encrypt)?
- Bob can encrypt?

- Or something else?

A mer realistic (anarchistic?) interpretation/set of assumption if we are doing protocol analysis could be:

- A, B are roles rather than principal names.
- Any number of principals can participate
- Each principal can play roles as both Alice and Bob
- Each principal can be participating in many instances of the protocol in parallel, both as Alice and Bob

Reflection

- Fact: There are protocols whose security depend on interpretations/assumptions like the above…
  - Snekkenes, E., "Roles in cryptographic protocols," Proceedings of IEEE *Symposium on Research in Security and Privacy, IEEE Computer Society.* pp.105-119, 1992. doi: 10.1109/RISP.1992.213267

Lets get back on track…

- Some say that
  - Risk exist in its own right
  - Risk can be measured objectively
  - Risk is the combination of incident consequence and incident probability (product)
  - Risk must be captured using conditional probabilities (conditioned on knowledge)

Critical thinking about risk analysis

- What is the objective of risk analysis?
- To what extent does a particular risk analysis method contribute towards this objective?
- To what extent does a particular risk analysis method posess the VALIDITY property?
- Are there situations where the RA objective can be fulfilled without resorting to probabilities?
- Can alternative perspectives on risk give rise to new insight into the case being investigated?

The CIRA method (as of spring 2013)

Einar Snekkenes

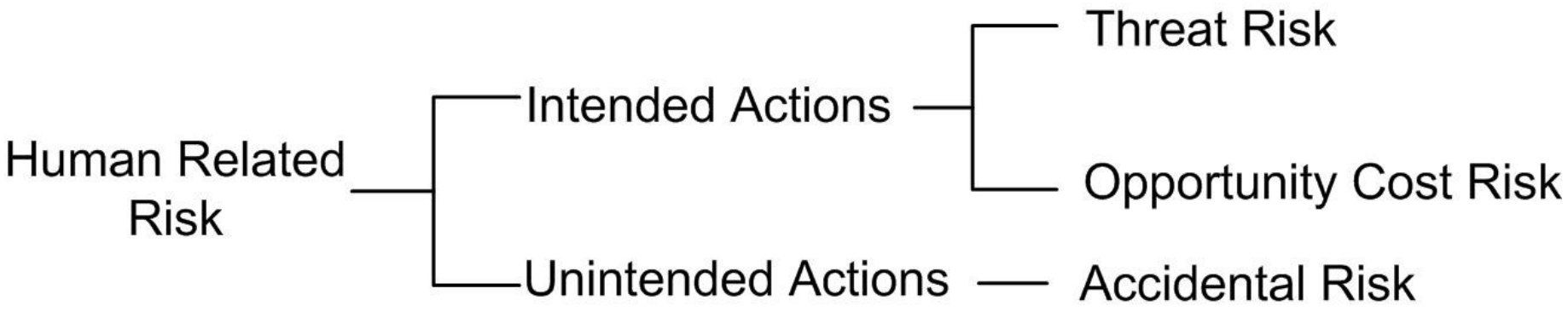
Overview

- Motivation
- Scope of CIRA
- The underlying idea
- The CIRA notion of RISK
- CIRA engineering

Reflections on current RA methods

- Lack of historical (frequency) data?
- `Low´ probability high consequence incidents – how can we audit the soundness of such claims?
- Distance mestric for `similar´ systems is somewhat unclear
- Systems may not be stationary
- The nature of the phenmenon of interest may have evolved since the RA ideas were formed
  - Technology vs people
- Unclear if `experts´ are in fact experts (subjective probabilities)
- Most RA methods rely on objective/subjective incident probability data – we want to challenge this

Scope of CIRA: Human Risks



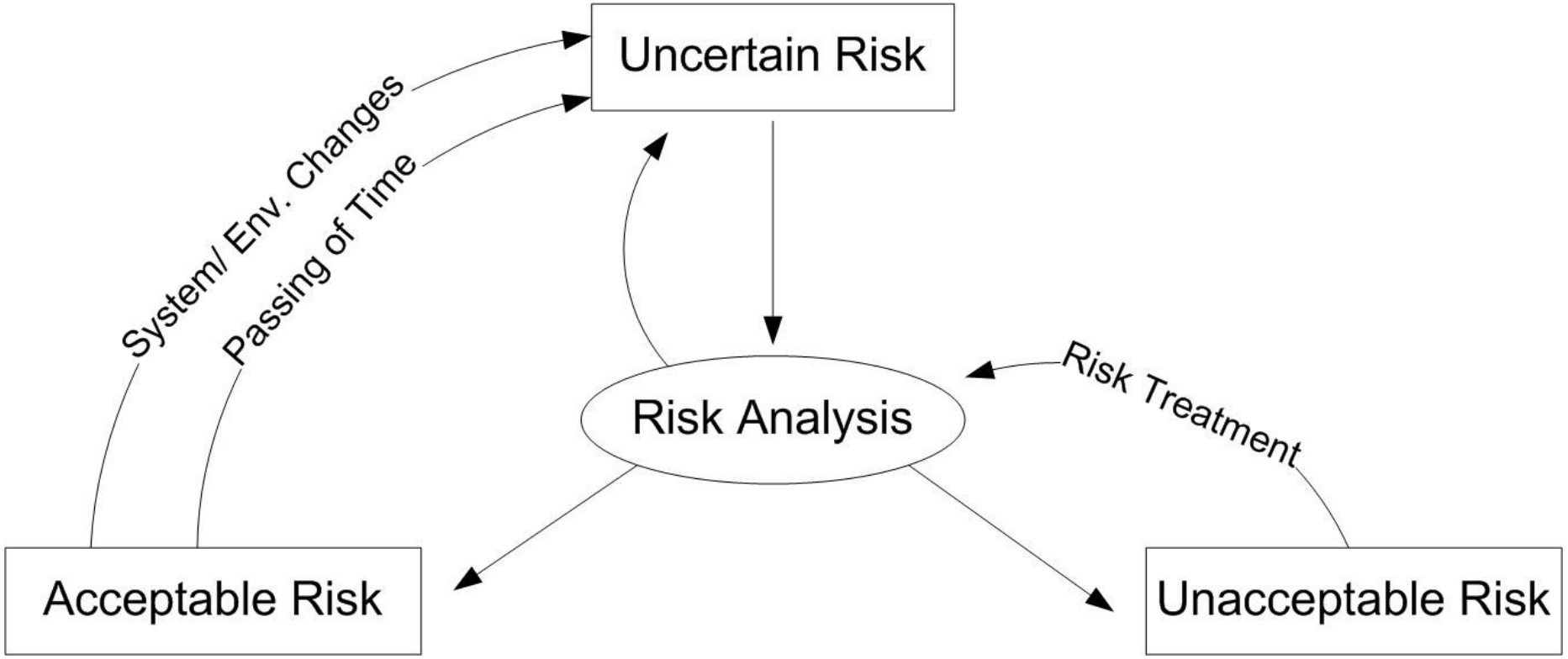
Claim

- Most risks can be lifted `up´ to human behaviour level

- Ex 1. A Lightning incident
  - The risk (probability and consequence) of the lightening occcuring outside my house
    - Possibly a stochastic phenomenon
  - The risk that I will be affected by the incident
    - Depends on how the electrican, builder, electricity board etc. have done their job.

- Ex. 2 Traffic accidents
  - A purely stochastic phenomenon?
  - A direct consequence of how people behave – (but people may bahave `stochastically´)?

Where CIRA fits in RM



CIRA underlying idea

IF

- You understand what motivates those that can influence your gains or losses

THEN

- You will have a good understanding of your risk

CIRA RISK

You are exposed to risk

IFF

Somebody

perceives a gain if doing something that results in a consequence that you perceive as a loss

OR

fails to perceive a gain from some action that you reasonably would expect he/she should perform and where you perceive the outcome as a gain.

CIRA VS classical RA

Replace

- Incident probability

By

- Stakeholder incentives and motivation

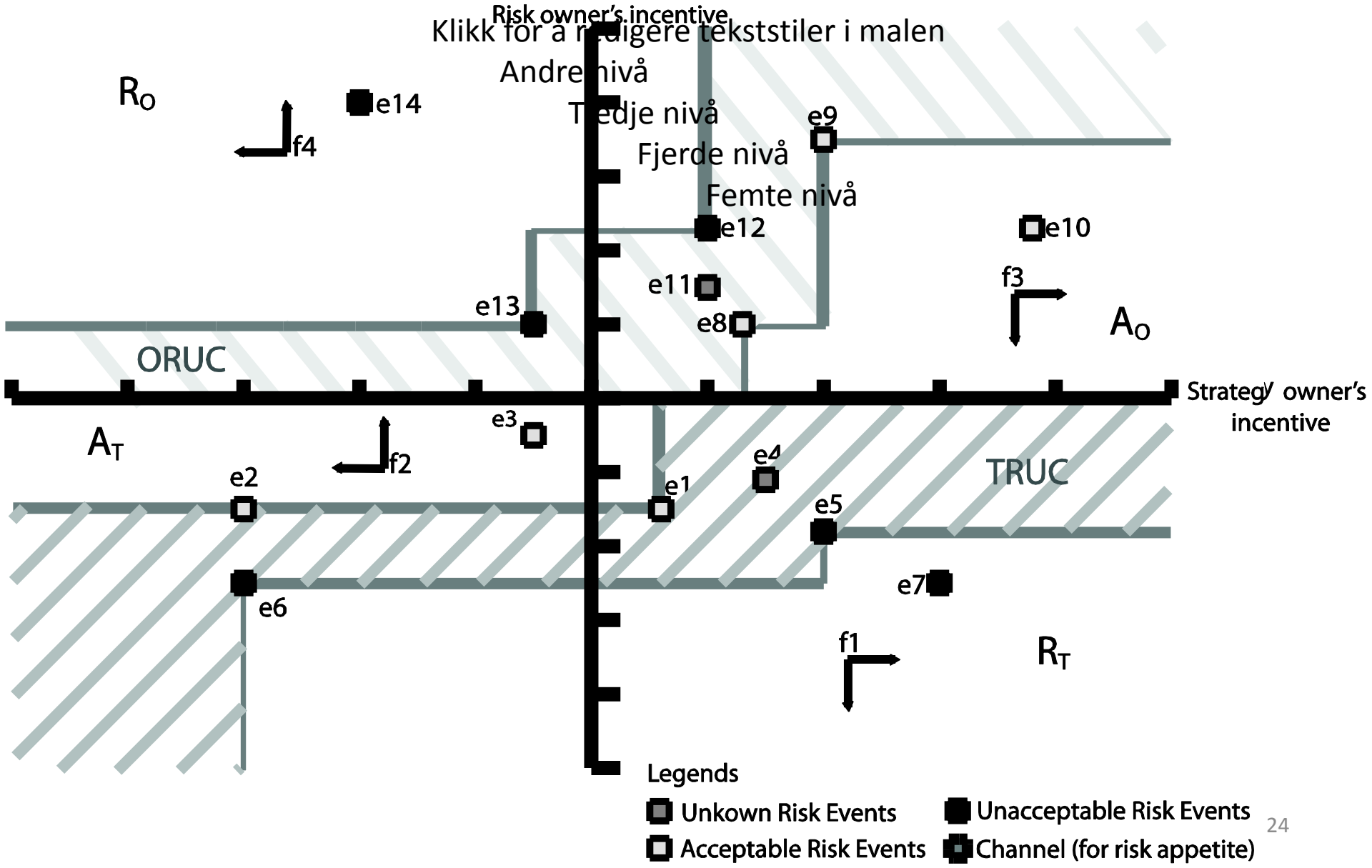
CIRA is an attempt to engineer this replacement

CIRA engineering overview

- What do people value?
  - Utility factors (e.g. wealth, freedom, power, reputation,…)
- What motivates people to do/not do ’things’?
  - Utility factors
- How strong is the motivation
  - How are the various utility factors weighted relative to each other
  - What is risk CIRA?

CIRA Quadrants

The CIRA Risk Picture



The CIRA Process

Data Collection

Structural

1. Identify the Risk Owner
2. Identify the risk owners' key utility factors
3. Given an intuition of the scope/ system - identify the kind of strategies/ operations can potentially influence the above utility factors
4. Identify roles/ functions that may have the opportunities and capabilities to perform these operations
5. Identify the named strategy owner(s) that can take on this role
6. Identify the utility factors of interest to this strategy owner(s)

Numerical

7. Determine how the utility factors can be operationalized
8. Determine how the utility factors are weighted by each of the stakeholders
9. Determine how the various operations result in changes to the utilities for each of the stakeholders

Analysis

10. Estimate the utility for each stakeholder
11. Compute the incentives
12. Determine Risk
13. Evaluate Risk

Modelling assumptions

- CIRA process/risk owner insight from CIRA does not influence strategy owner perceptions
- Stakeholder strategies and outcomes correspond to outcomes of complete `games'

Case Study Role Play

Einar Snekkenes

Security, Risk Analysis and Research

- Security
  - Live in a world where things can og wrong
  - I **C** A
- Risk analysis
  - Understanding threats, vulnerabilities, consequences
- Research
  - Publish new knowledge/ evidence that can be validated

- **Can you see a problem?**

We are not the first to recognize that there is a problem…

- M. Siponen and R. Willison. Information security management standards: Problems and solutions. Information & Management, 46(5):267 – 270, 2009.
- A. Kotulic and J. Clark. Why there aren't more information security research studies. Information & Management, 41(5):597–607, 2004.

CSRP idea

- Mimick a complete organization (including people) in such a way that it is sufficiently `close´ to an actual organization.
- I.e. mimick such that any potential findings from the the role play scenario also would have been findings in the real operational organization being mimicked.

CSRP steps

1. Persona and Scenario Construction
   - Smalltown University Scenario Description
   - Identify stakeholders
2. Role Play Selection and Guidance
   - Assign roles to group members (e.g. use age as a proxy for seniority)
3. Gather Data from the Participants
   - Collect data required by CIRA from each of the players. I.e. each player is interviewed by the rest of the group.

Scenario Description Smalltown University

Einar Snekkenes

Scenario content

- Terms of reference
- University objectives
- University Performance Indicators
- University Organizational Structure
- University use of Information Technology
  - IT equipment
  - Software
  - Electronic security measures
- Physical access control
- University funding
- ECTS production

CIRA exercise

Einar Snekkenes

What you need

- Scenario description
- Data collection sheets
  - Stakeholder list
  - Several stakeholder utility factor forms
  - Several strategy forms
  - Risk magnitude form

Instructions

- Write group number on all sheets

What to do

1. Define Scope/system boundaries
2. Identify Stakeholders
3. Chose risk owner, i.e. perspective
4. Identify stakeholder utility factors and suggest how they can be assessed/measured
5. Determine what weights stakeholders assign to utility factors
6. Identify stakeholder actions