Tool-Supported Cyber-Risk Assessment

Security Assessment for Systems, Services and Infrastructures (SASSI'15)

Bjørnar Solhaug (SINTEF ICT)

Berlin, September 15, 2015

RASEN

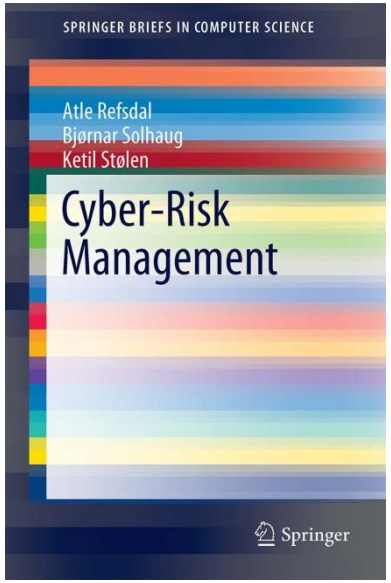
SEVENTH FRAMEWORK PROGRAMME

Me

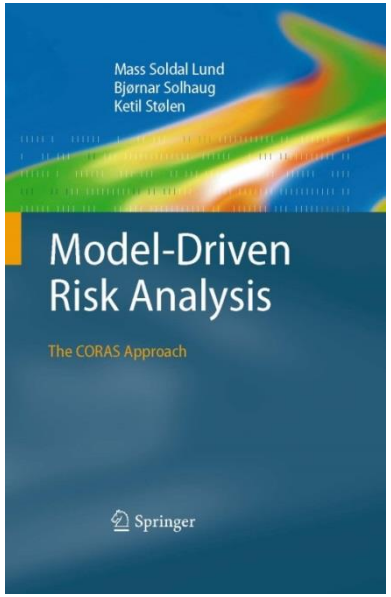
- Bjørnar Solhaug
  - Bjornar.Solhaug@sintef.no
  - www.solhaugb.byethost11.com
- Research scientist at SINTEF ICT since 2010
  - www.sintef.no
- MSc in Logic, Language and Information, University of Oslo, 2004
- PhD in Information Science, University of Bergen, 2009
- Co-author of two books:
  - *Cyber-Risk Management* (Springer, 2015)
  - *Model-Driven Risk Analysis – The CORAS Approach* (Springer, 2015)

Background to this Tutorial

- Atle Refsdal, Bjørnar Solhaug and Ketil Stølen: *Cyber-Risk Management* (Springer, 2015)



- Mass Soldal Lund, Bjørnar Solhaug and Ketil Stølen: *Model-Driven Risk Analysis – The CORAS Approach* (Springer, 2011)



- CORAS resources, including free tool download and demo video: http://coras.sourceforge.net

Relevant Standards

- **ISO 31000** – Risk management – Principles and Guidelines (2009)
- **ISO/IEC 27000** – Information technology – Security techniques – Information security management systems – Overview and vocabulary (2014)
- **ISO/IEC 27001** – Information technology – Security techniques – Information security management systems – Requirements (2013)
- **ISO/IEC 27005** – Information technology – Security techniques – Information security risk management
- **ISO/IEC 27032** – Information technology – Security techniques – Guidelines for cybersecurity

Overview

- Risk assessment
  - Background terminology
  - Risk assessment process
- Cyber-risk assessment
  - Cybersecurity and cyber-risk terminology
  - Cyber-risk assessment process
- Example and demo
  - Smart Grid example
  - Demo of CORAS tool

Risk Assessment

What is Risk?

- Health
- Safety
- Security
- Compliance (legal and regulatory)
- Environmental protection
- Product quality
- Reputation
- Defense
- Finance
- …

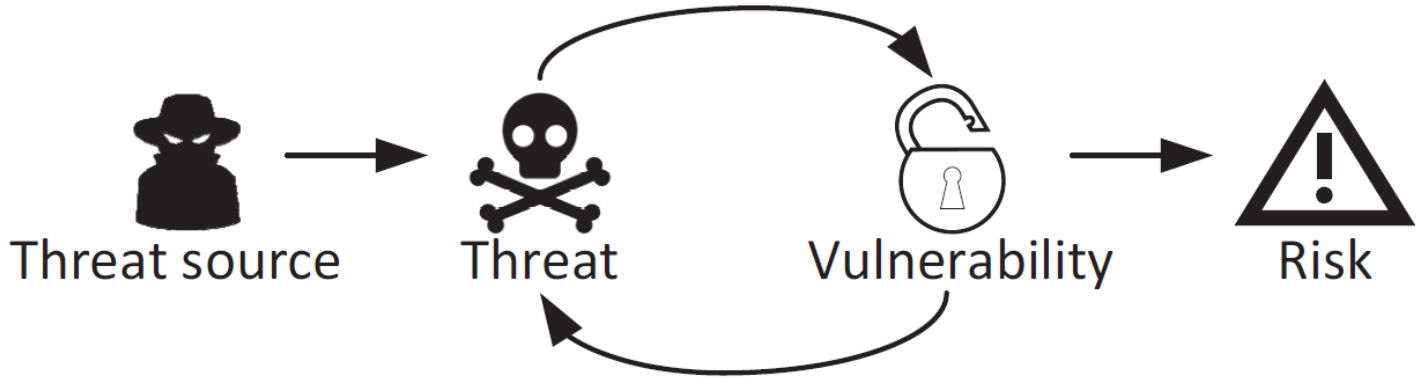
- What do we want to protect?
- What do we want to achieve?
- What do we want to protect from?

Definitions 1/2

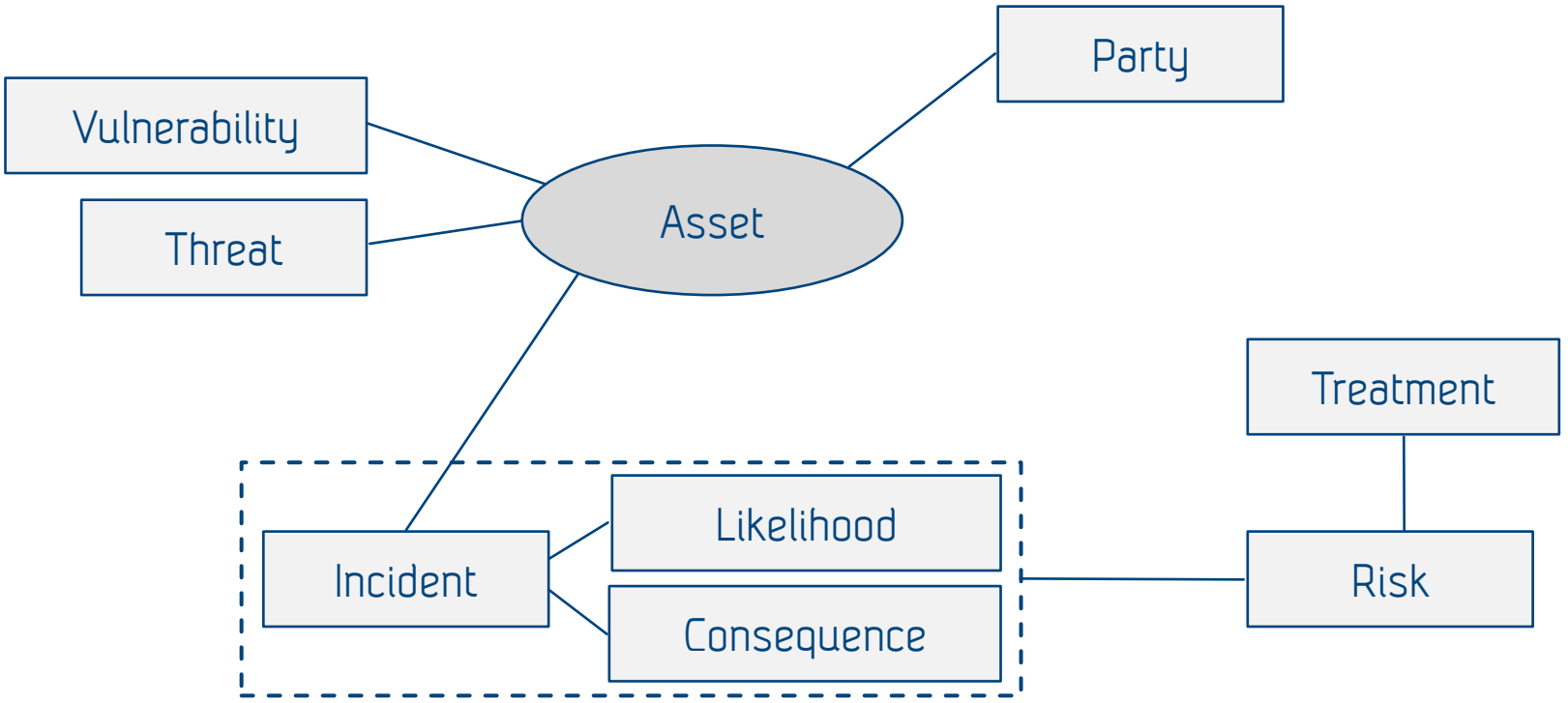
- A **risk** is the likelihood of an incident and its consequence for an asset
- An **incident** is an event that harms or reduces the value of an asset
- An **asset** is anything of value to a party
- A **party** is an organization, company, person, group or other body on whose behalf a risk assessment is conducted
- A **likelihood** is the chance of something to occur
- A **consequence** is the impact of an incident on an asset in terms of harm or reduced asset value
- **Risk level** is the magnitude of a risk as derived from its likelihood and consequence

Definitions 2/2

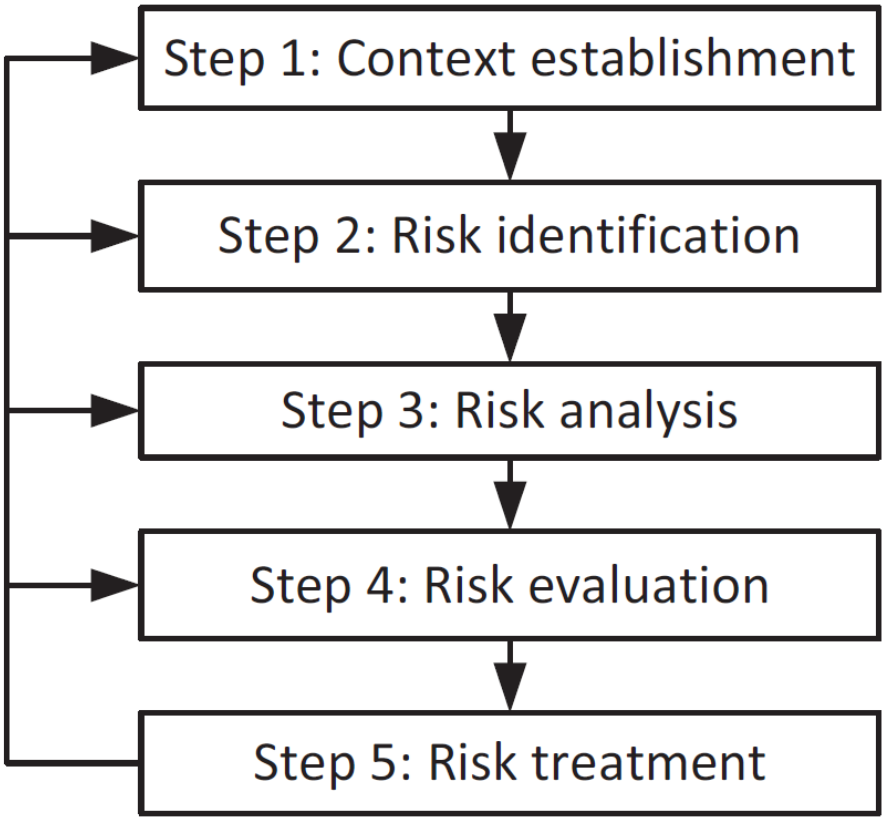
- A **vulnerability** is a weakness, flaw or deficiency that can be exploited by a threat to cause harm to an asset
- A **threat** is an action or event that is caused by a threat source and that may lead to an incident
- A **threat source** is the potential cause of an incident
- A **treatment** is an appropriate measure to reduce risk level



Concept Overview



Risk Assessment Process



Cyber-Risk Assessment

Cyberspace and Cyber-Systems

- Cybersecurity concerns systems that make use of cyberspace

- A **cyberspace** is a collection of interconnected computerized networks, including services, computer systems, embedded processors and controllers, as well as information in storage or transit
  - For most organizations and other stakeholders, cyberspace is for all practical purposes synonymous with the Internet
  - The Internet is a global cyberspace in the public domain
- A **cyber-system** is a system that makes use of a cyberspace
  - A cyber-system may include information infrastructures, as well as other entities that are involved in the business processes and other behavior of the system
  - Cyber-systems are therefore part of the structure of most organizations

Cybersecurity

- **Cybersecurity** is the protection of cyber-systems against cyber-threats
  - Cyber-threats are those that arise via a cyberspace, and are therefore a kind of threat that any cyber-system is exposed to
- A **cyber-threat** is a threat that exploits a cyberspace
  - A cyber-threat can be *malicious*
    - For example DoS attack and malware injection attacks that are caused by intention
  - A cyber-threat can be *non-malicious*
    - For example system crash due to programming error, or some accidental loss of Internet connection

Remark on Cybersecurity

- What defines cybersecurity is not what we seek to protect, but rather what we seek to *protect from*

- Cybersecurity is not defined by the kinds of assets that are to be protected, but rather by the kinds of *threats* to assets
  - The assets of concern depend on the organization and the cyber-system in question
  - Often, cybersecurity concerns the protection of information assets and information infrastructure assets
  - However, cybersecurity must not be confused with information security or critical infrastructure protection

Cybersecurity vs. Information Security

- Information security is the preservation of confidentiality, integrity and availability of data
  - Information can come in any form: Electronic, material, knowledge, …
- Information in all formats need to be protected from threats of any kind
  - Physical, human, technology related, natural causes, …
- Cybersecurity concerns the protection from threats that use cyberspace
  - Various forms of information assets are relevant, but also others like information infrastructures, compliance, revenue, …

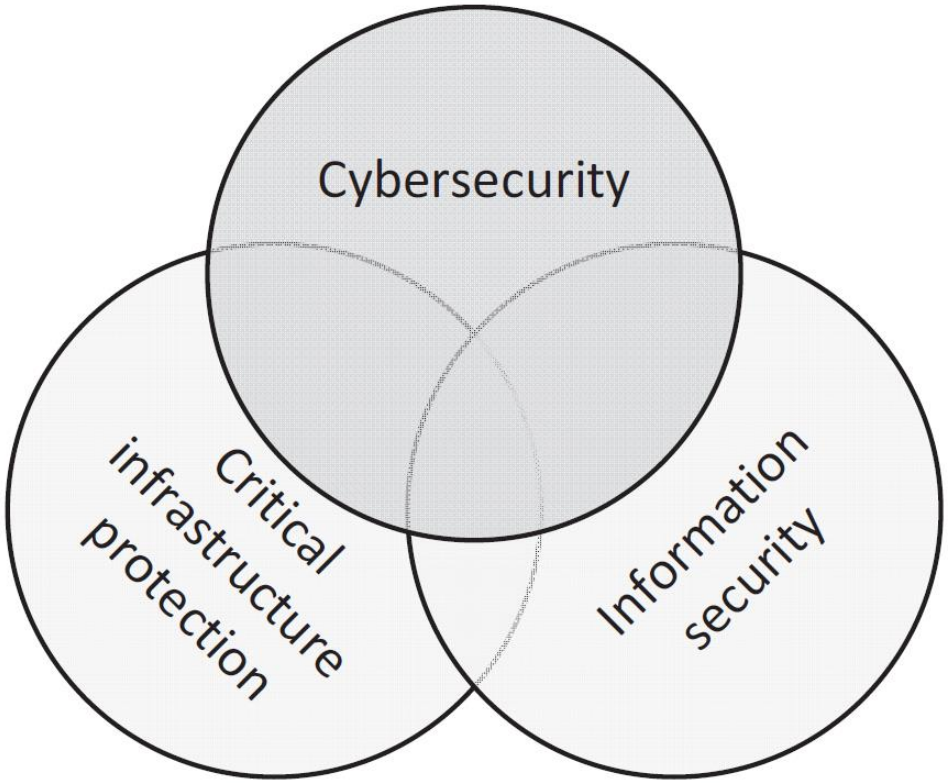
- There is overlap between the two, but:
  - Cybersecurity goes beyond information security
  - Information security goes beyond cybersecurity

Cybersecurity vs. Critical Infrastructure Protection

- Critical infrastructure protection (CIP), or infrastructure security, is concerned with the prevention of the disruption, disabling, destruction or malicious control of infrastructure
  - Telecommunication, transportation, finance, power supply, emergency services, …
- Many critical infrastructures use cyberspace and are therefore cyber-systems
  - Cybersecurity often involves CIP, but is not limited to CIP
  - CIP may involve cybersecurity, but only when the infrastructure is a cyber-system

- There is overlap between the two, but:
  - Cybersecurity goes beyond CIP
  - CIP goes beyond cybersecurity

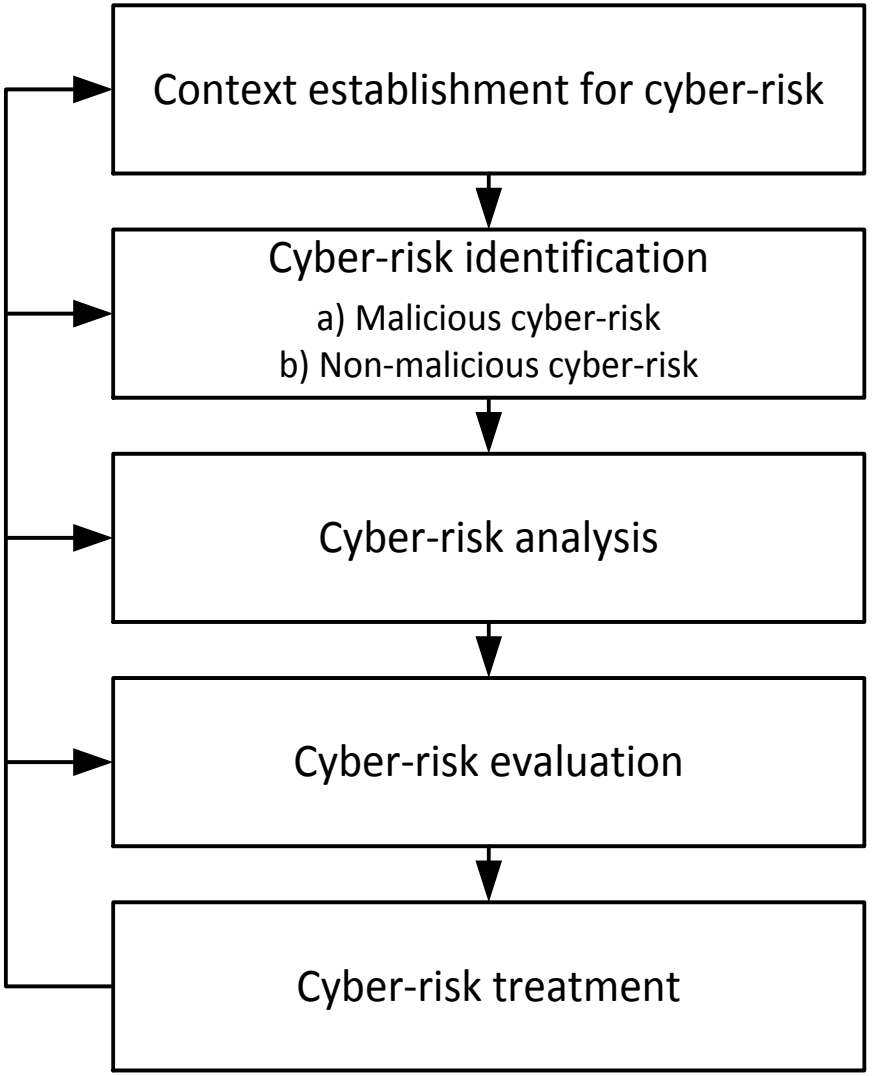
Cybersecurity vs. Information Security and CIP



Cyber-Risk Assessment

- A **cyber-risk** is a risk that is caused by a cyber-threat

- We distinguish between
  - Malicious cyber-risk
  - Non-malicious cyber-risk



Identification of Malicious Cyber-Risk

- Malicious cyber-risks are caused by adversaries with intent
- We need to understand
  - Who or what is the threat source (attacker)?
  - What is the motive and intention?
  - What resources are required?
  - Which skills are required?
  - Which vulnerabilities can be exploited?
  - …
- There are many helpful sources of information
  - Logs, monitored data, security testing, …
  - OWASP, CAPEC, CWE, annual security reports, standards, …

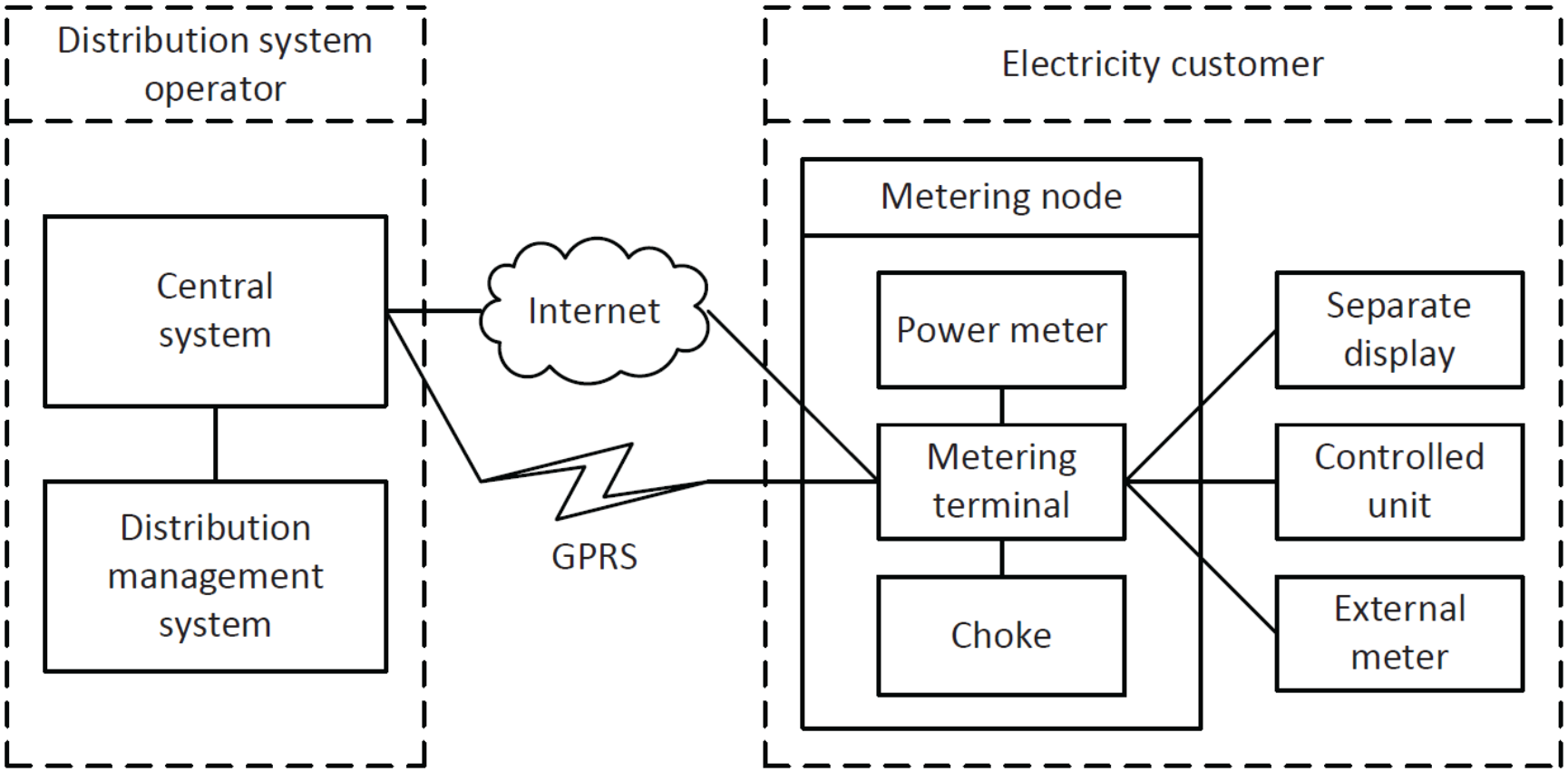
Identification of Non-Malicious Cyber-Risk

- Normally, there is no intent behind non-malicious risks

- To avoid getting overwhelmed during the risk identification, we recommend to start with the assets to identify incidents
- Aspect to take into account:
  - How are assets stored and represented, and how are they related to the target?
    - E.g., how is information stored and processed in the system and in cyberspace, which users and applications have access to read and modify, how is the information transmitted,…?
  - Use logs and monitored data, investigate technical parts of the system, as well as cultures, routines, awareness, etc. of the organization and personnel
  - Take into account unintended external threats
  - Use relevant sources such as ISO 27005 and NIST guide for conducting risk assessments

Example and Demo

Advanced Metering Infrastructure (AMI) of a Smart Grid



CORAS Risk Modeling

- CORAS is a model-driven approach to risk assessment based on ISO 31000
  - Method
  - Language
  - Tool
- The CORAS language is a graphical language for risk identification and modeling
  - Formal syntax: The grammar is precisely defined and implemented in the tool
  - Formal semantics: Mathematical interpretation that enable rigorous analysis
  - Natural language semantics: Any diagram can be systematically translated to paragraphs in English prose
  - Comes with a calculus with rules for calculation, reasoning and consistency checking

CORAS Diagram Elements

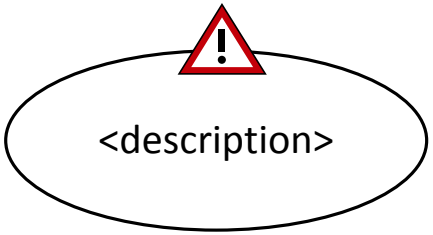
Party

Asset

Malicious threat source

Non-malicious threat source

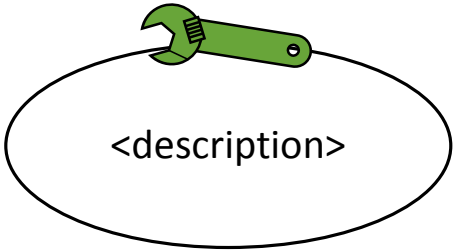
Non-human threat source



Threat

Vulnerability

Incident



Treatment

Risk

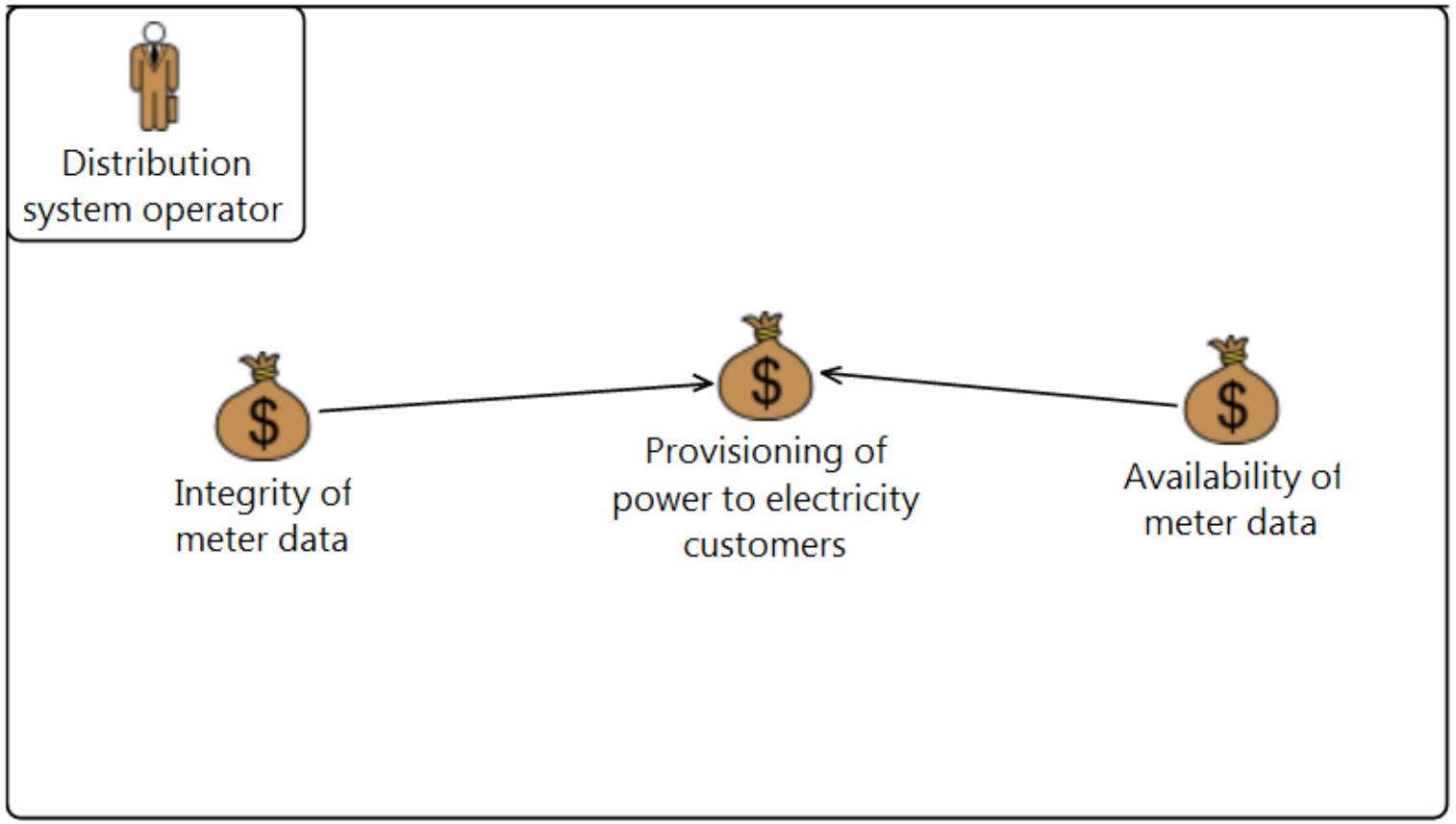
CORAS Diagrams

- The CORAS language supports all steps of the risk assessment process
- Different kinds of diagrams support different steps
  - **Asset diagrams** for identifying and documenting assets during context establishment
  - **Threat diagrams** for risk identification and risk analysis
  - **Risk diagrams** for risk evaluation
  - **Treatment diagrams** for treatment identification
  - **Treatment overview** diagrams for documenting treatments

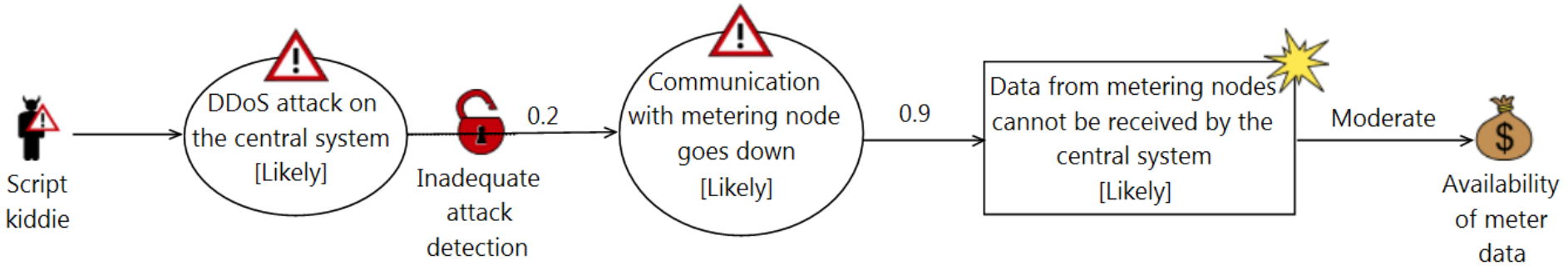
AMI Example: Party and Assets

- The party for the analysis is the distribution system operator
- Assets:
  - Integrity of meter data
    - The integrity of meter data should be protected all the way from **Power meter** to **Distribution system operator**
  - Availability of meter data
    - Meter data from **Metering node** should be available for **Distribution system operator** at all times
  - Provisioning of power to electricity customers
    - Power should only be switched off or choked as a result of legitimate control signals from **Central system**

CORAS Asset Diagram



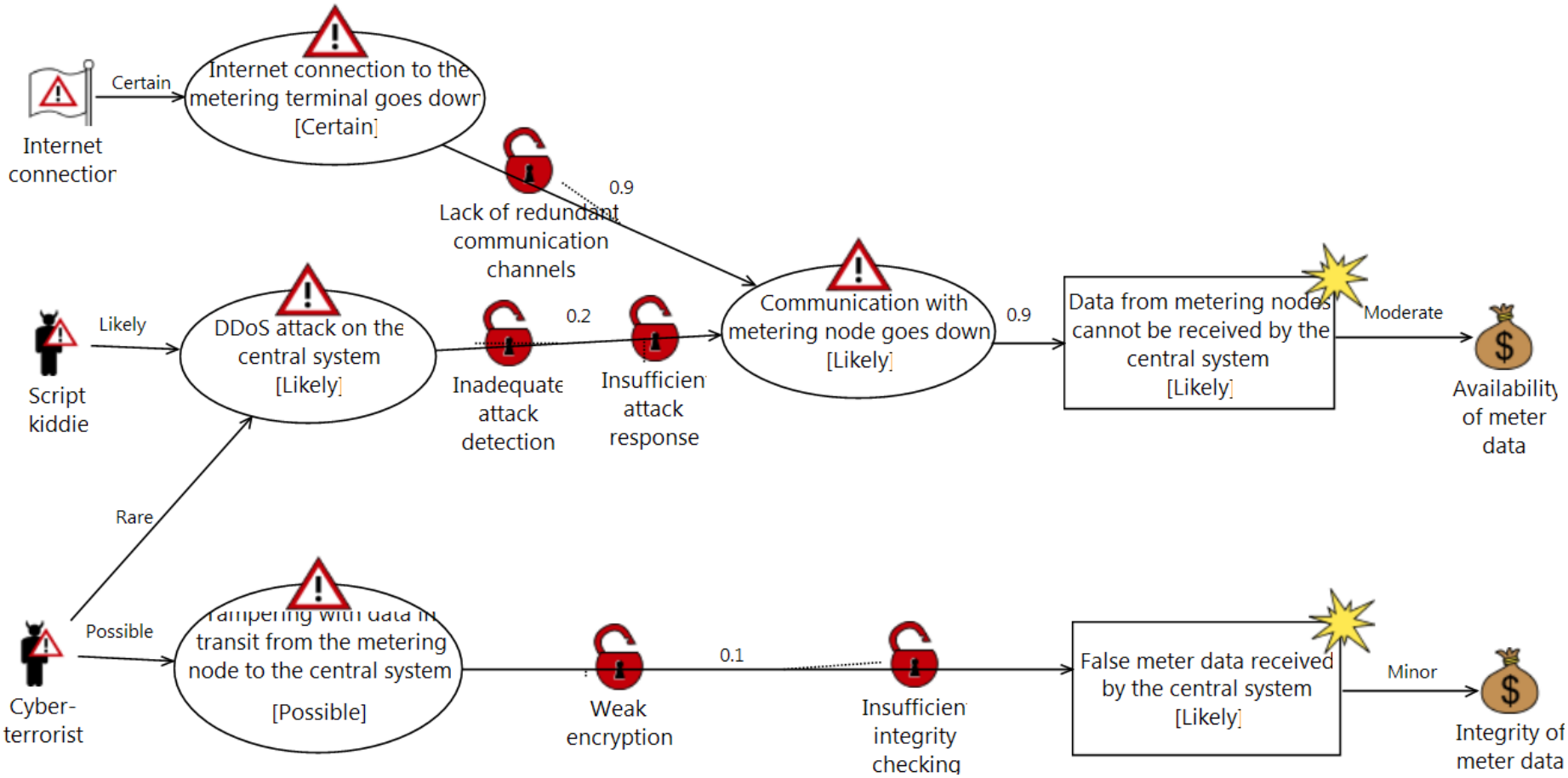
CORAS Threat Diagram



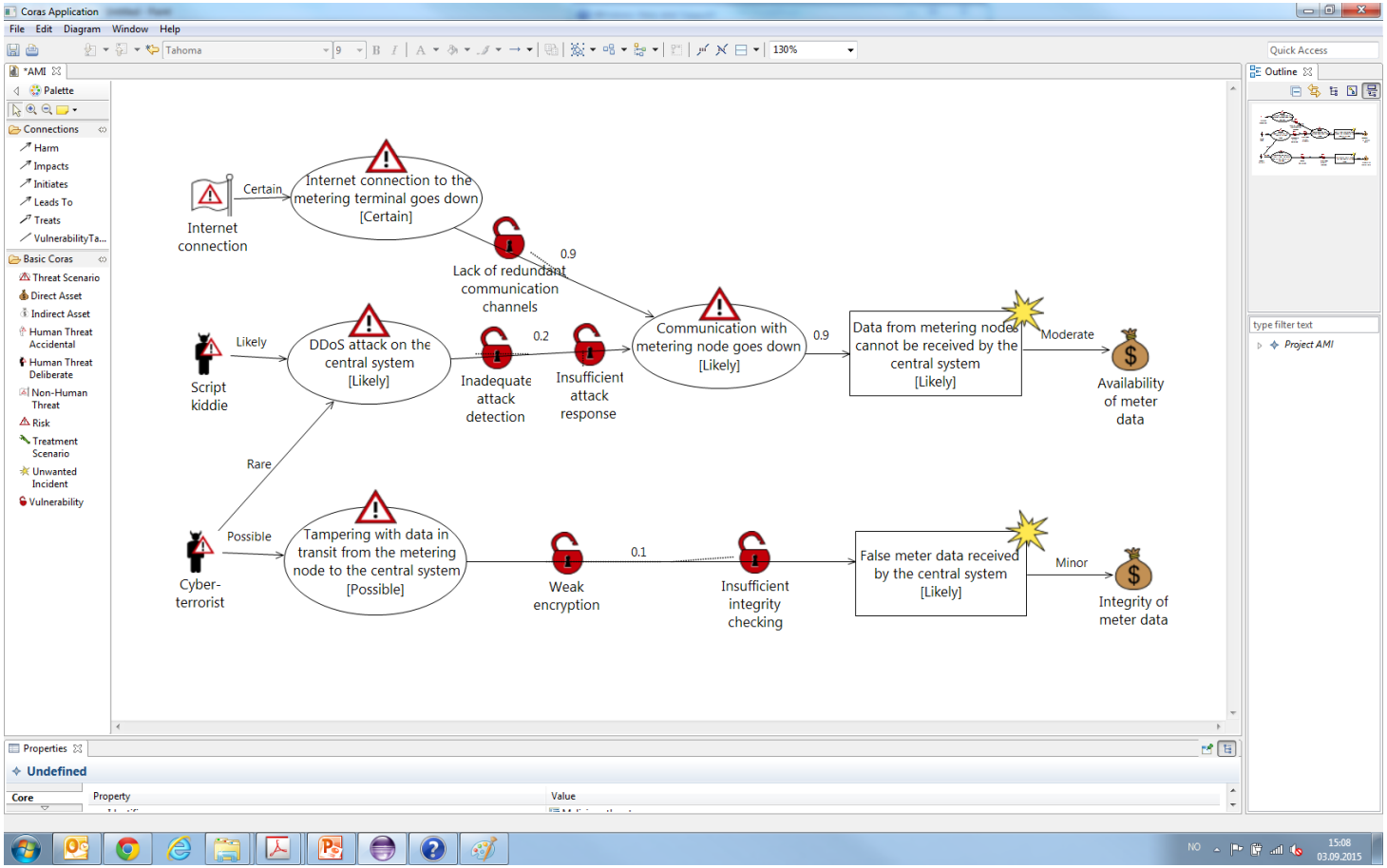
Likelihood Scale

Likelihood	Description	Frequency interval
Seldom	Less than 1 time per 10 years	[0, 0.1›:1y
Unlikely	1-10 times per 10 years	[0.1, 1›:1y
Possible	2-12 times per year	[1, 13›:1y
Likely	13-60 times per year	[13, 60›:1y
Certain	More than 60 times per year	[60, ∞›:1y

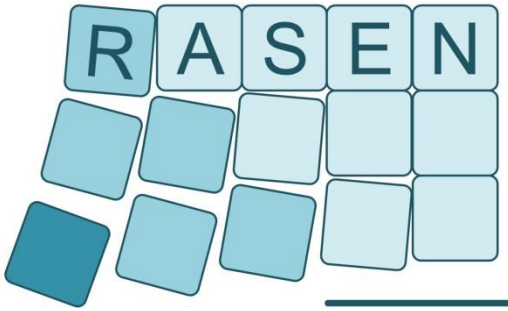
CORAS Threat Diagram



Live Demo


Coras Application
File Edit Diagram Window Help
Internet connection
Certain
Internet connection to the metering terminal goes down [Certain]
Lack of redundant communication channels
0.9
Script kiddie
Likely
DDoS attack on the central system [Likely]
Inadequate attack detection
0.2
Insufficient attack response
Communication with metering node goes down [Likely]
0.9
Data from metering node cannot be received by the central system [Likely]
Moderate
Availability of meter data
Rare
Cyber-terrorist
Possible
Tampering with data in transit from the metering node to the central system [Possible]
Weak encryption
0.1
Insufficient integrity checking
False meter data received by the central system [Likely]
Minor
Integrity of meter data
Undefined

Thank You!



Compositional Risk Assessment and Security Testing of Networked Systems

www.rasenproject.eu

SEVENTH FRAMEWORK PROGRAMME