



SINTEF

Supporting CORAS

Online, model-driven risk analysis

Risk

- A *Risk* is the likelihood of an incident and its consequence for an asset.
- Multiple definitions depending on field
 - "Uncertainty about gains and loss"
 - "Chance of harm to health and environment"
 - "Uncertainty about financial returns"

Risk Assessment

- Understanding, managing and mitigating risk
- An important and growing field
- A pillar of security and safety
- Helps prevent accidents and malicious attacks
- Multiple approaches
- Offensive vs defensive



SINTEF

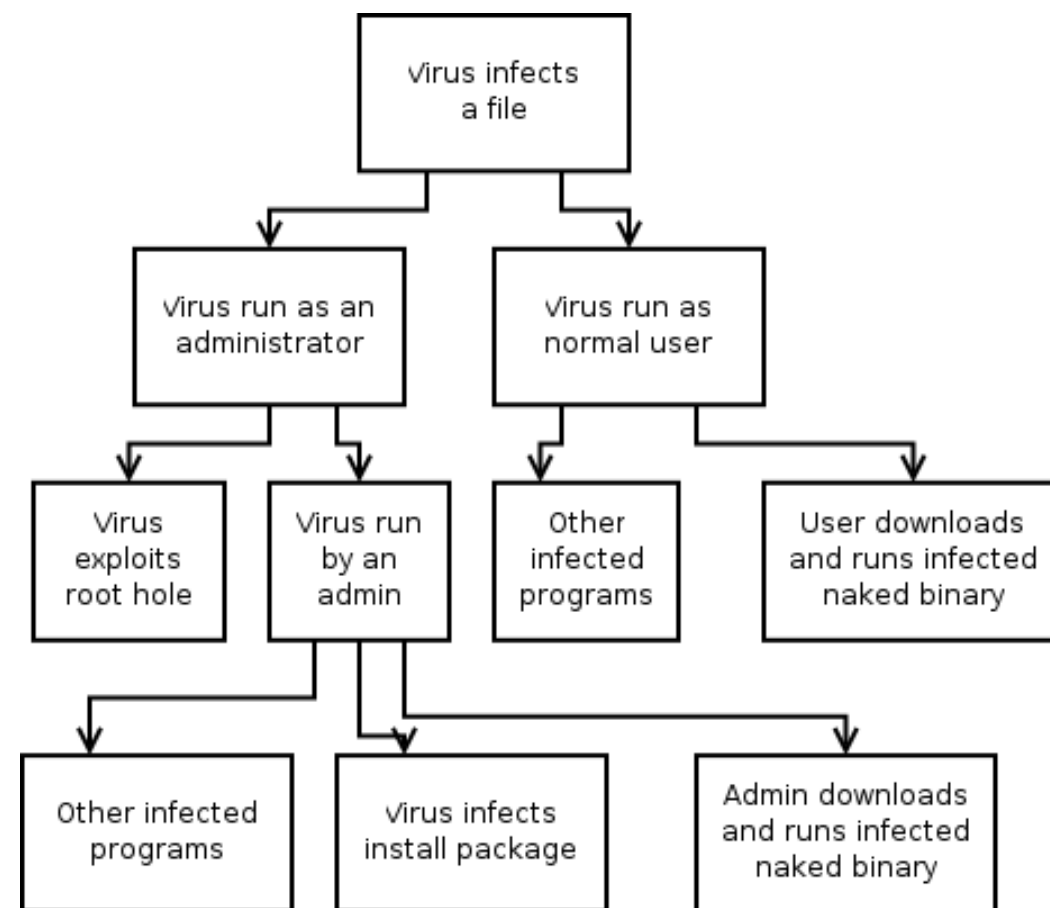
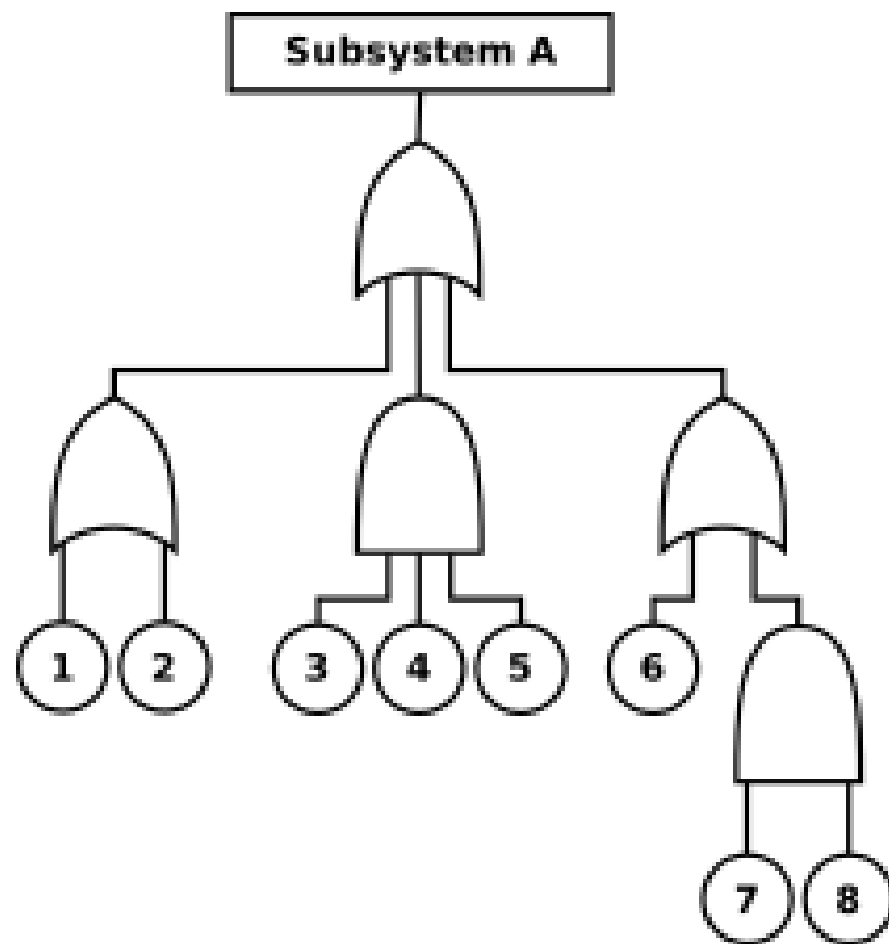
Risk modelling languages

- A way to visualize and document the process
- More specialized than general modeling languages
- Fault Tree Analysis, Attack trees, Cause-Consequence Analysis, etc.
- Different foci and different strengths and weaknesses



SINTEF

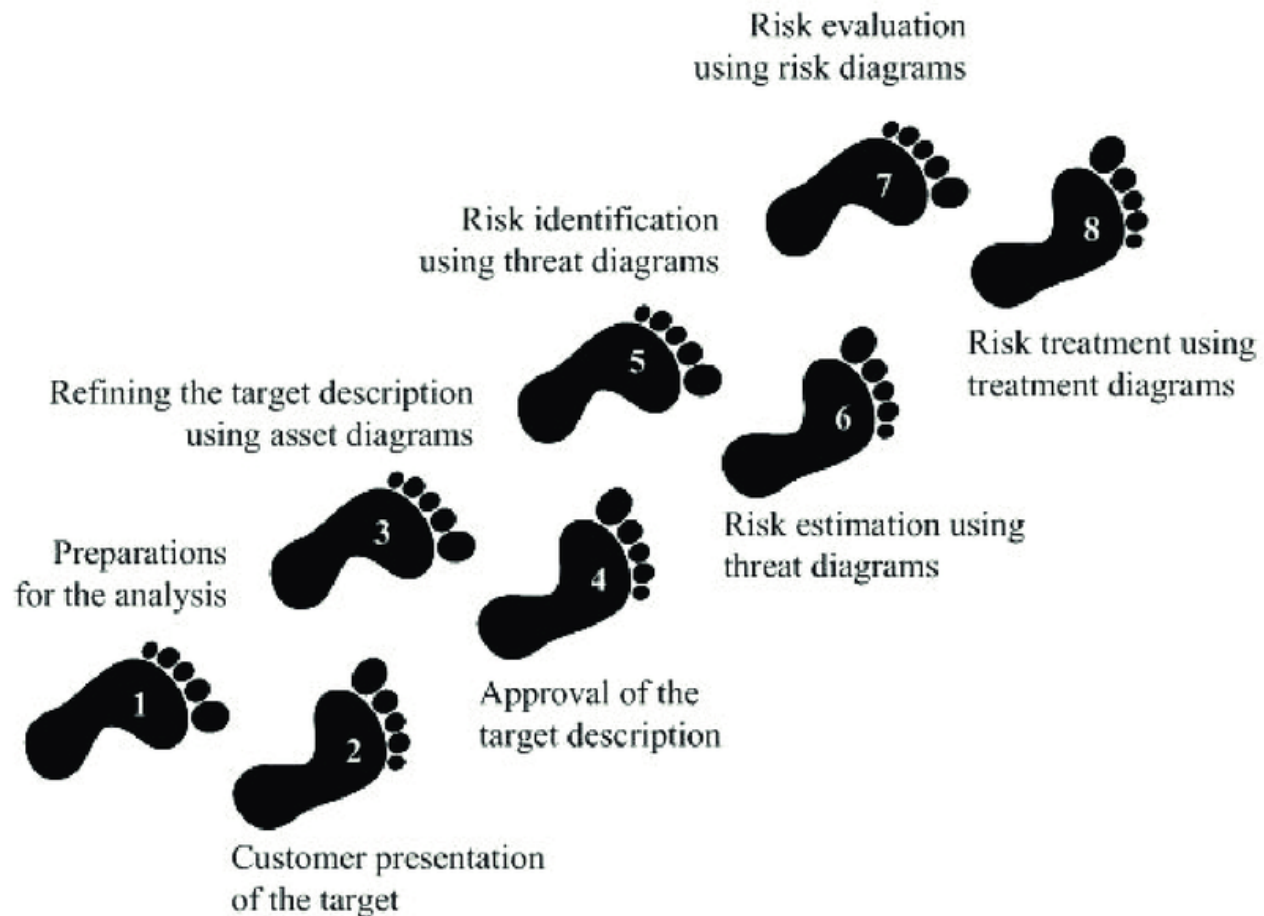
Examples



- A model-driven risk analysis approach
- Started development in 2001
- Developed and maintained at SINTEF
- Consists of a language, a method and a tool
- Defensive risk analysis
- Supports the entire analysis process
- Facilitates communication and interaction

CORAS Methodology

- Consists of eight steps
 - Context Establishment (1 to 4)
 - Risk Identification
 - Risk Analysis/Estimation
 - Risk Evaluation
 - Risk Treatment
- ISO 31000
 - Establishing context
 - Identification
 - Assessment
- "Structured brainstorming"

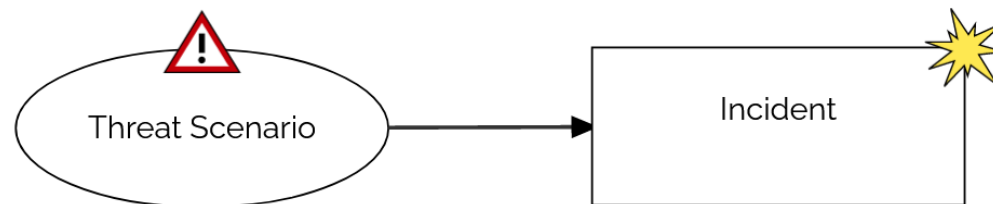


CORAS Language

- A graphical modelling language for communication, documentation and analysis of security threat and risk scenarios
- Contains 5 diagram types
 - Asset diagram
 - Threat diagram
 - Risk diagram
 - Treatment diagram
 - Treatment overview diagram

CORAS Language

- Relation types
 - Initiates
 - Leads-to
 - Impacts
 - Treats
- Diagram types and their respective elements
 - Each of the five diagram types have their respective elements
 - Most overlap

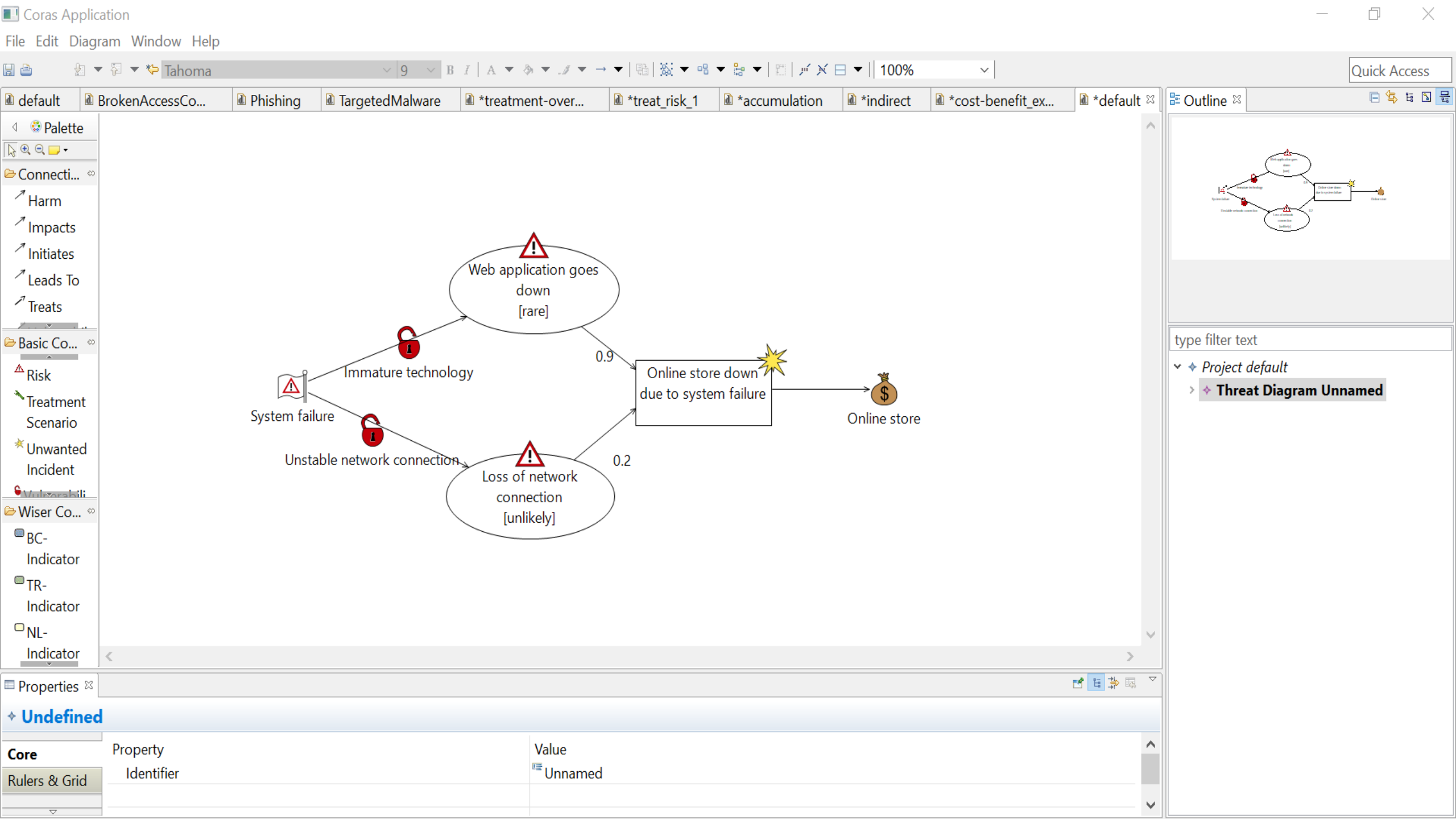


CORAS Tool support

- Visio stencils
- Offline tool
- Online tool

Offline tool

- Feature-rich
- Built with Java
- Lower compatibility
- Higher barrier of entry
- Lack of updates
- Used in many industrial risk analyses and research projects





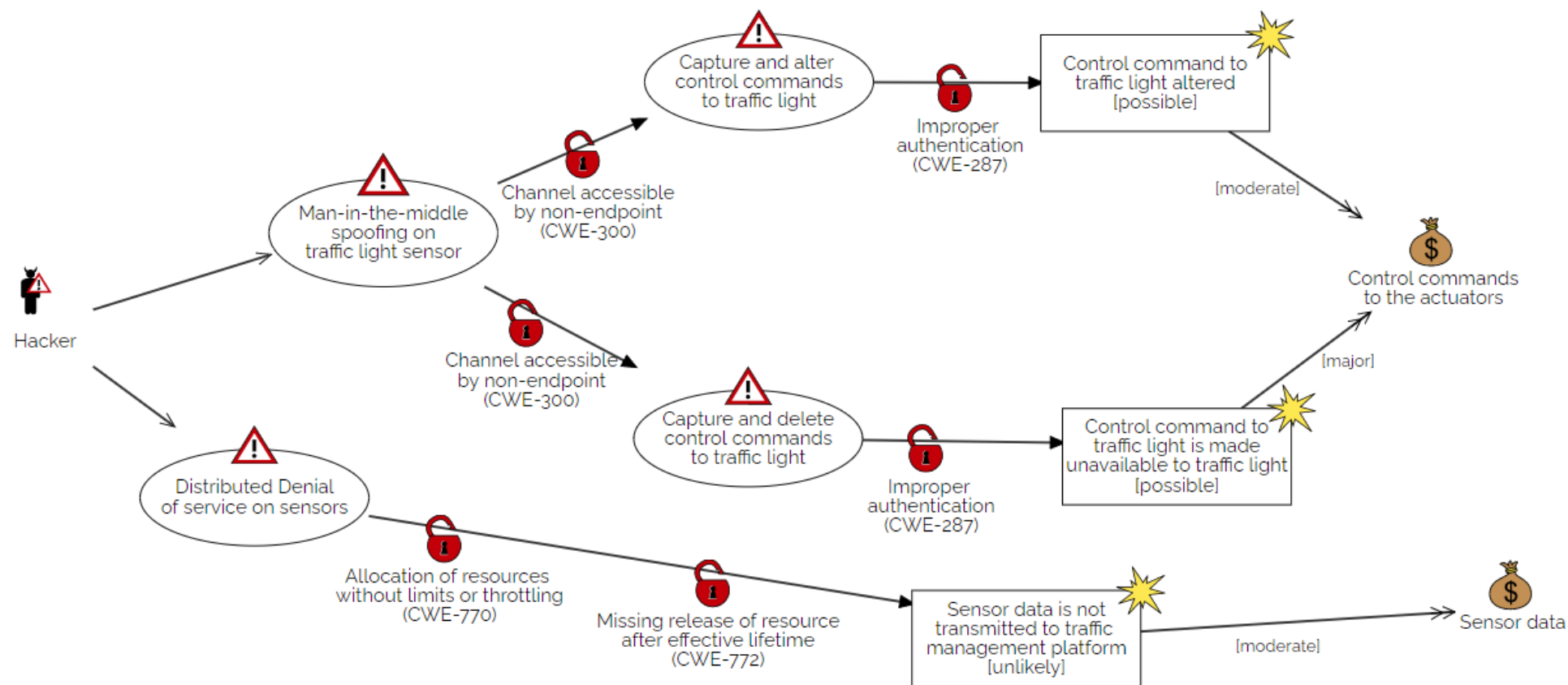
SINTEF

Motivation for an online version

- Issues with portability
- The offline version takes time to set up and learn
- Increased barrier of entry
- A need for a tool that can be used anywhere, anytime and by anyone

Online tool

- High compatibility
- Simple interface
- Low barrier of entry
- MIT license
- <https://coras.tools/>

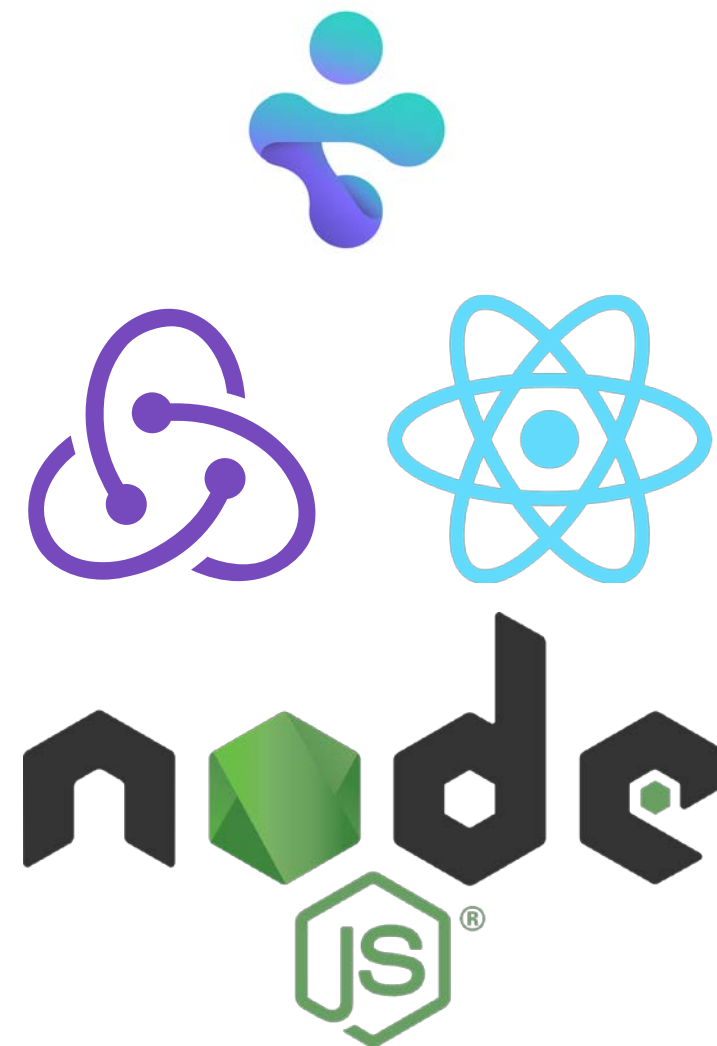


Development

- Developed in two main iterations
- Intended to:
- Make the tool easier to use
 - Make the tool represent the methodology
 - Disallow illegal relations and elements
- Present more information to the user in a clearer way
 - Visual differences where relevant
 - Information popups

Technology

- Implemented in Javascript, using the React library
- Utilizes Nodejs
- Based on the modeling framework JointJS
 - JointJS is further based on Backbone.JS
- Utilizes Redux for state management



Process

- Developed with Agile(ish) practices
- New updates released periodically.
- New requirements identified during the process due to interaction with users.
 - Students
 - Research projects
- Kanban board used to track changes
- Initial focus on usability/ease of use
- Clarity and syntax became a focus later
- First hosted on a github website, later on the domain coras.tools
- Version 1.0 released early this year

Demonstration

- <https://coras.tools/>

Finally

- Don't hesitate to let me know of any bugs you find
- Thank you for listening



SINTEF

Teknologi for et bedre samfunn