Safety Architecture Overview Framework

for the prediction, explanation and control of risks of ERTMS

Katja Schuitemaker, G. Maarten Bonnema, Marco Kuijsten, Heidi van Spaandonk and Mohammad Rajabali Nejad
19/12/2018

UNIVERSITY OF TWENTE.

ProRail

Katja Schuitemaker

- 2012 →   Bsc Engineering, Design and Innovation
- 2015 →   Msc Emerging Technology Design, focus on Systems Engineering
- 2015 →   Writing research proposal + acquiring funds
- 2016 →   Start PHD

Agenda

1. ERTMS and safety
2. Safety Architecture Overview Framework
   - RA
   - RE
   - Scenario specific
3. KPIs
4. Example

ERTMS and Safety

European Railway Traffic Management System: "Improved safety for passengers" (ertms.net) (only L2 B3)
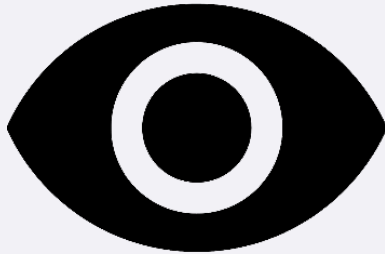
Continuous supervision
Train speed

By use of the
communicationsystem
GSM-R (Level 2)

Reducing the risk
for human errors

By improving the
work environment

Decreasing the amount
of Signals Passed At
Danger (SPAD)

By monitoring
braking curves

Model

Creating the integral safety architecture

Complex, interdisciplinary systems

Substantiators, consultants of the safety architecture

The model

Pilot

Raw data:
- Existing documentation
    - System Description

Raw data:
- Oral examinations
    - Risk analysis

Raw data:
- Oral examinations
    - Risk evaluation

Raw data → Information → Safety architecture → Layered scenarios → Presentation customized views

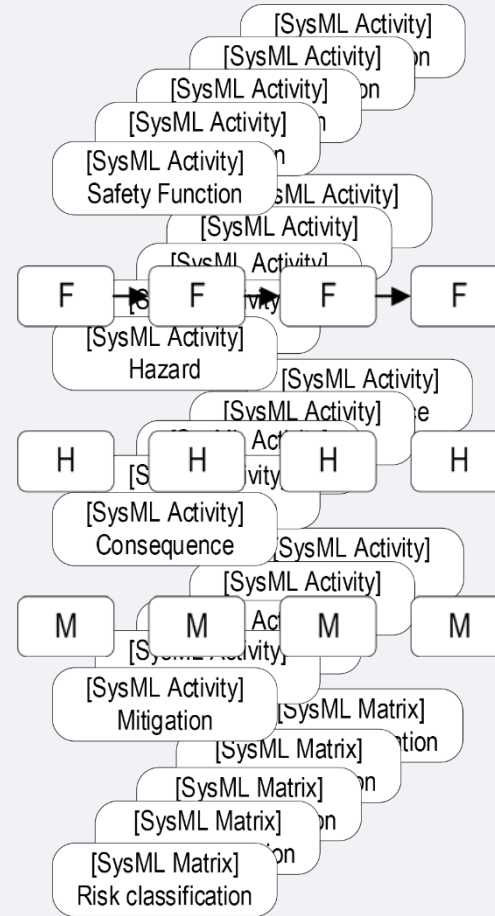| Select data | Translate | Filter | Group | Structure | Generate scenarios | Generate layers | Select view | Present |

The model

Pilot

Raw data

Information

Safety architecture

Layered scenarios

Presentation customized views

| Select data | Translate | Filter | Group | Structure | Generate scenarios | Generate layers | Select view | Present |

The model

Pilot

The model

Pilot

Raw data

Information

Safety architecture

Layered scenarios

Presentation customized views

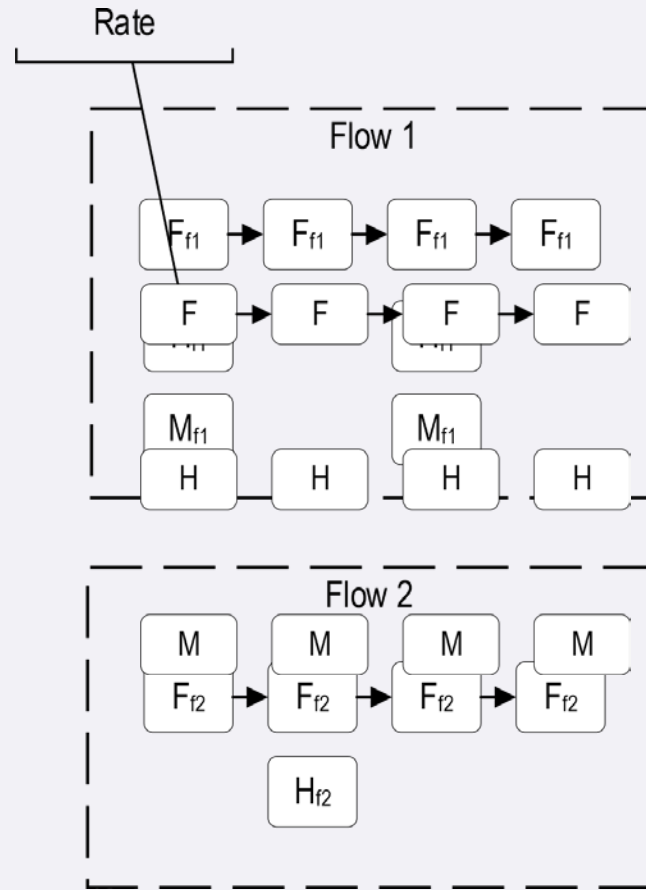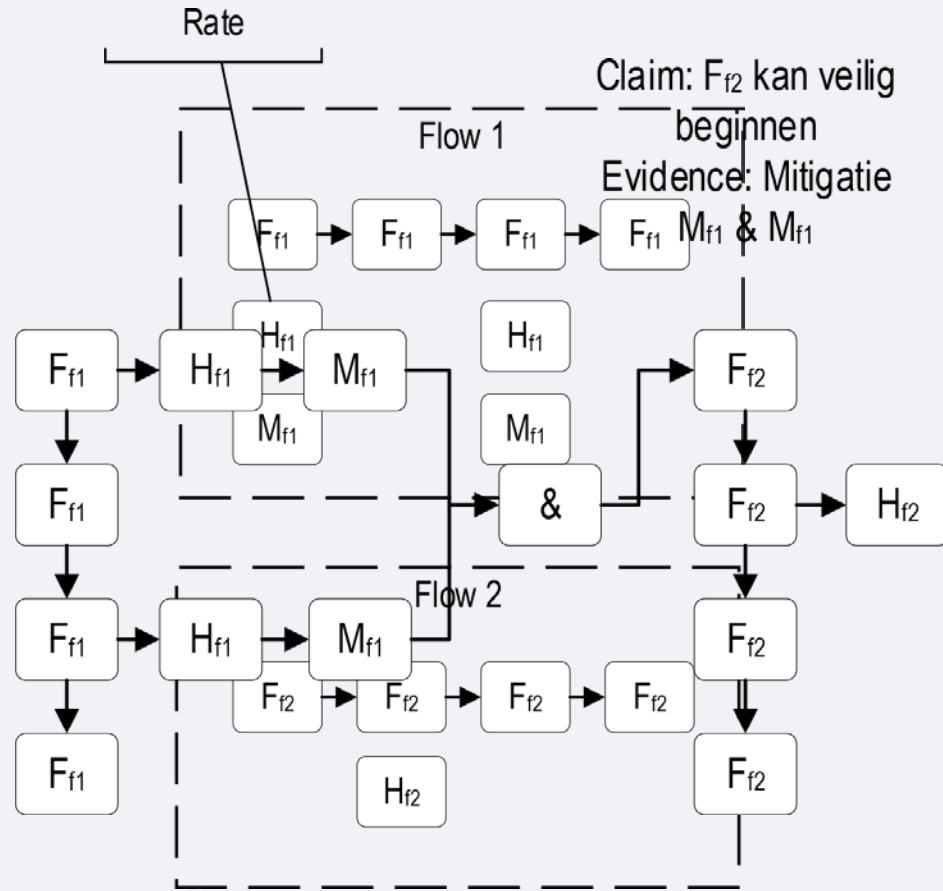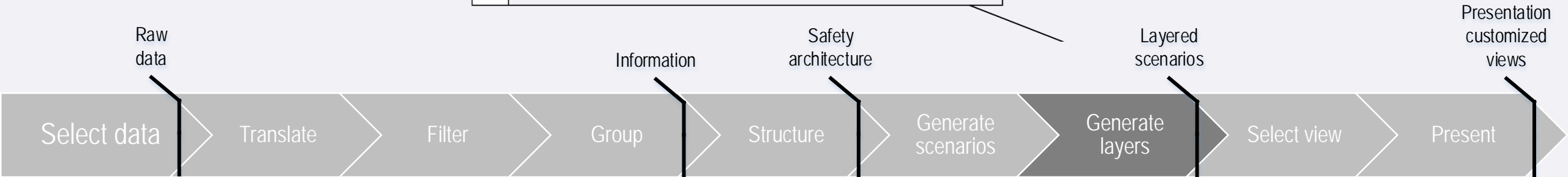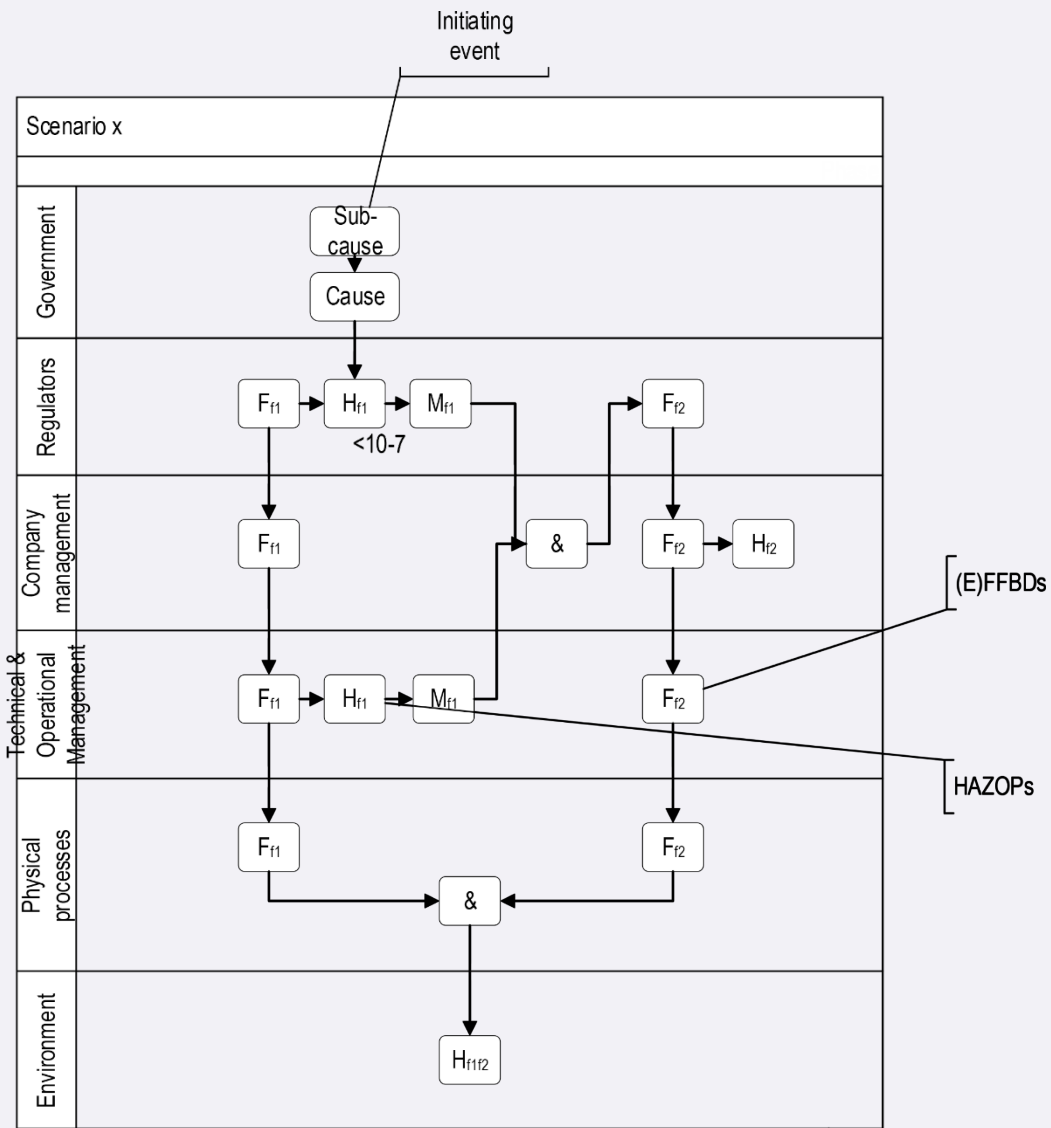Select data | Translate | Filter | Group | Structure | Generate scenarios | Generate layers | Select view | Present

Sub-cause

Cause

F_{f1} → H_{f1} → M_{f1}

$<10^{-7}$

Claim: F_{f2} kan veilig beginnen
Evidence: Mitigatie M_{f1} & M_{f1}

F_{f1} → H_{f1} → M_{f1}

F_{f2}

F_{f1}

F_{f2} → H_{f2} → F_{f2}

F_{f1} → H_{f1} → M_{f1}

&

F_{f2}

F_{f2} → H_{f2}

F_{f2}

(E)FFBDs

F_{f1} → H_{f1} → M_{f1}

F_{f2}

HAZOPs

F_{f1}

F_{f1} → &

F_{f2}

F_{f2}

H_{f1f2}

Raw data

Information

Safety architecture

Layered scenarios

Presentation customized views

Select data | Translate | Filter | Group | Structure | Generate scenarios | Generate layers | Select view | Present

Initiating event

Scenario x

Government

Sub-cause

Cause

Regulators

F_{f1} → H_{f1} → M_{f1} → F_{f2}

<10-7

Company management

F_{f1} & F_{f2} → H_{f2}

Technical & Operational Management

F_{f1} → H_{f1} → M_{f1} → F_{f2}

(E)FFBDs

HAZOPs

Physical processes

F_{f1} & F_{f2}

Environment

H_{f1f2}

Raw data | Information | Safety architecture | Layered scenarios | Presentation customized views

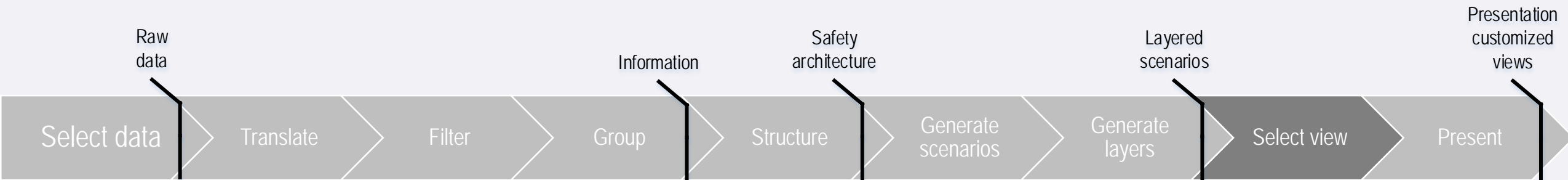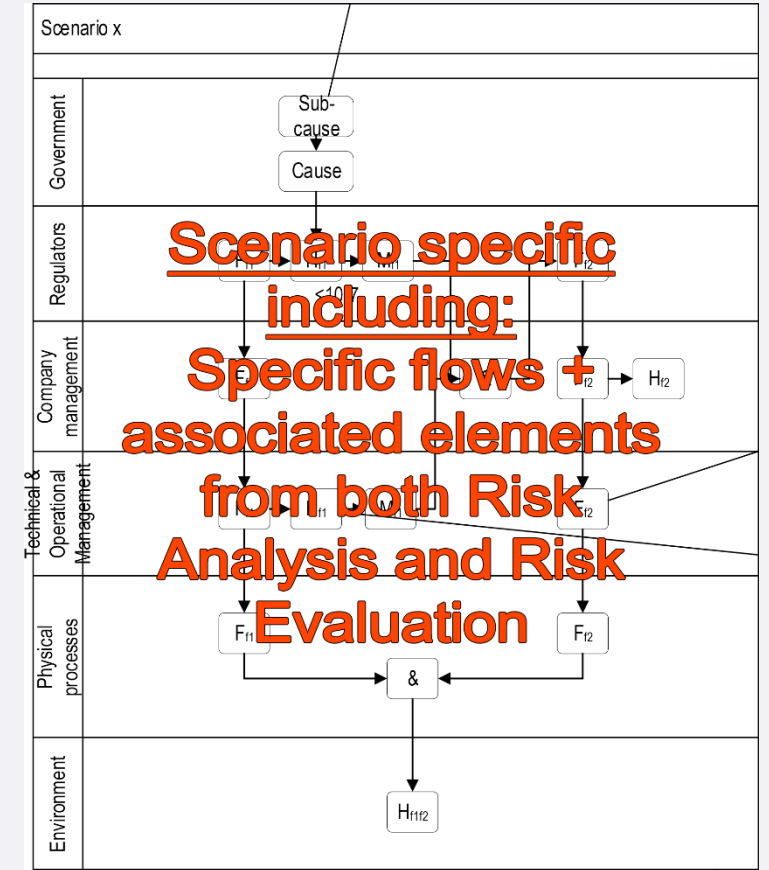Select data > Translate > Filter > Group > Structure > Generate scenarios > Generate layers > Select view > Present

Top Risk Analysis architecture including:
- Top flows
- Top claims
- Top hazards + frequencies
- Top related functions
- Top related decisions
- Precursors
- Assumptions

Top Risk Evaluation architecture including:
- Top Consequences and their estimation of injuries and fatalities
- Top Hazards and their risks classifications in likelihood and severity
- ALARP control measures
- Assumptions

Scenario specific including:
Specific flows + associated elements from both Risk Analysis and Risk Evaluation

Raw data

Information

Safety architecture

Layered scenarios

Presentation customized views

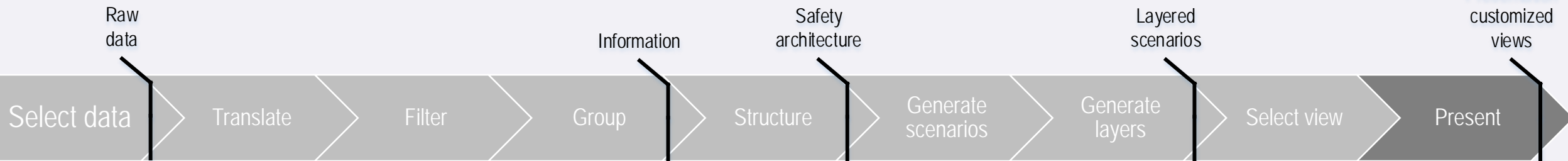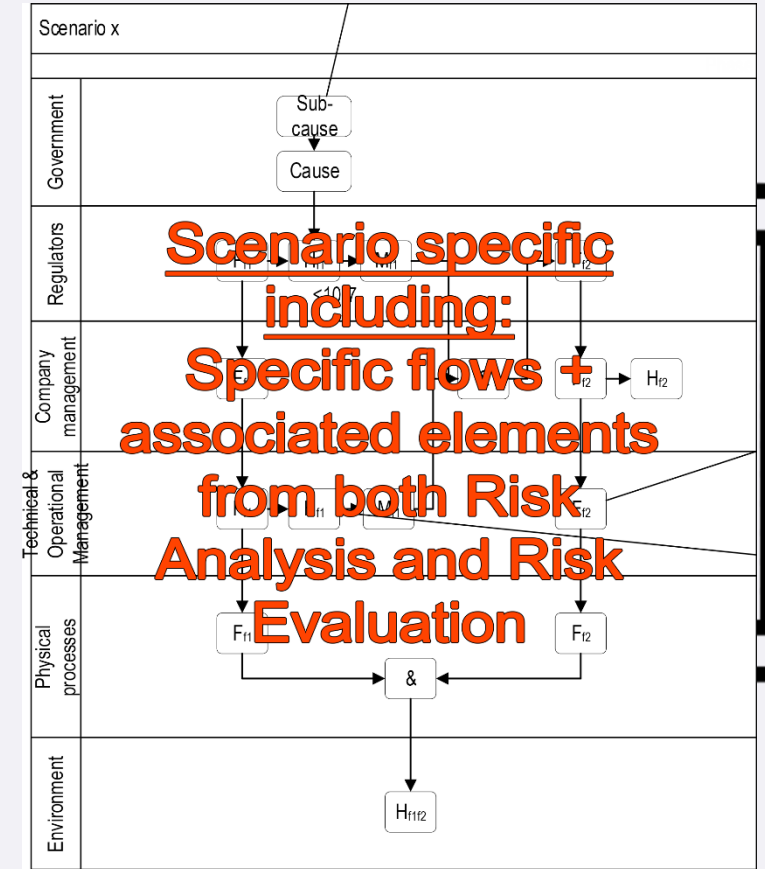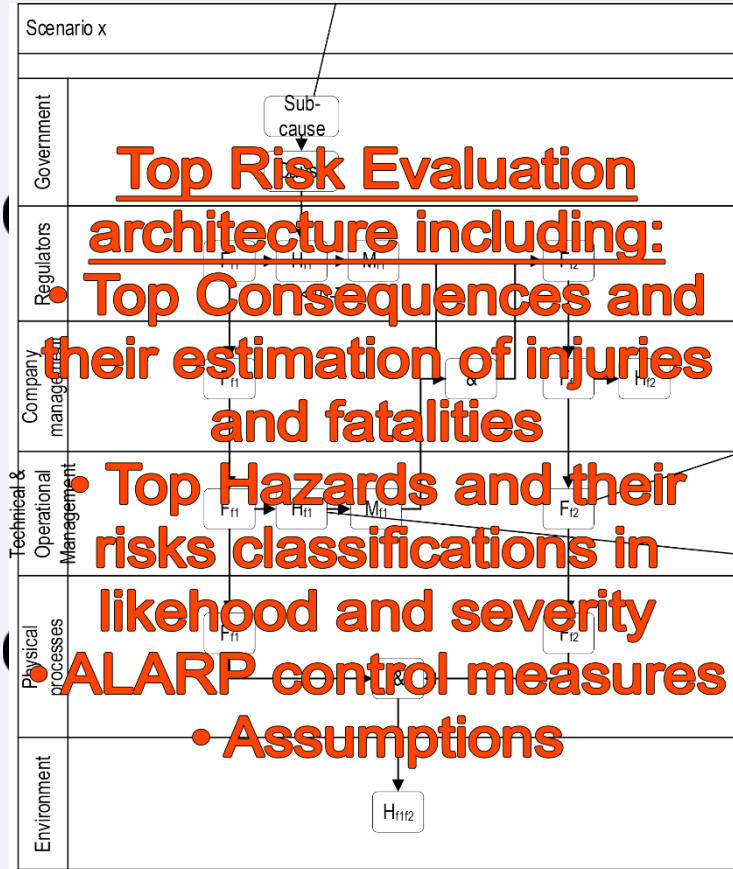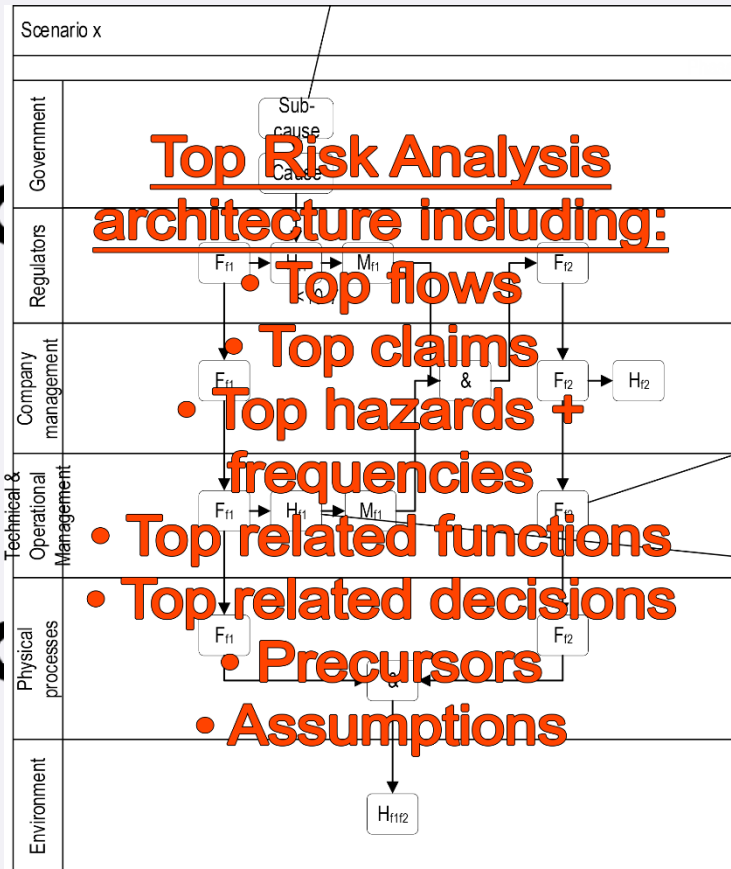Select data | Translate | Filter | Group | Structure | Generate scenarios | Generate layers | Select view | Present

Cases

What:
- Real-life case
- Experiments
- Student

How:
- Test
- ±4 participants
- 60-90 min test, ± 10 questions