Bruk av CORAS i praksis
Eksemplifisert med luftfartskontroll
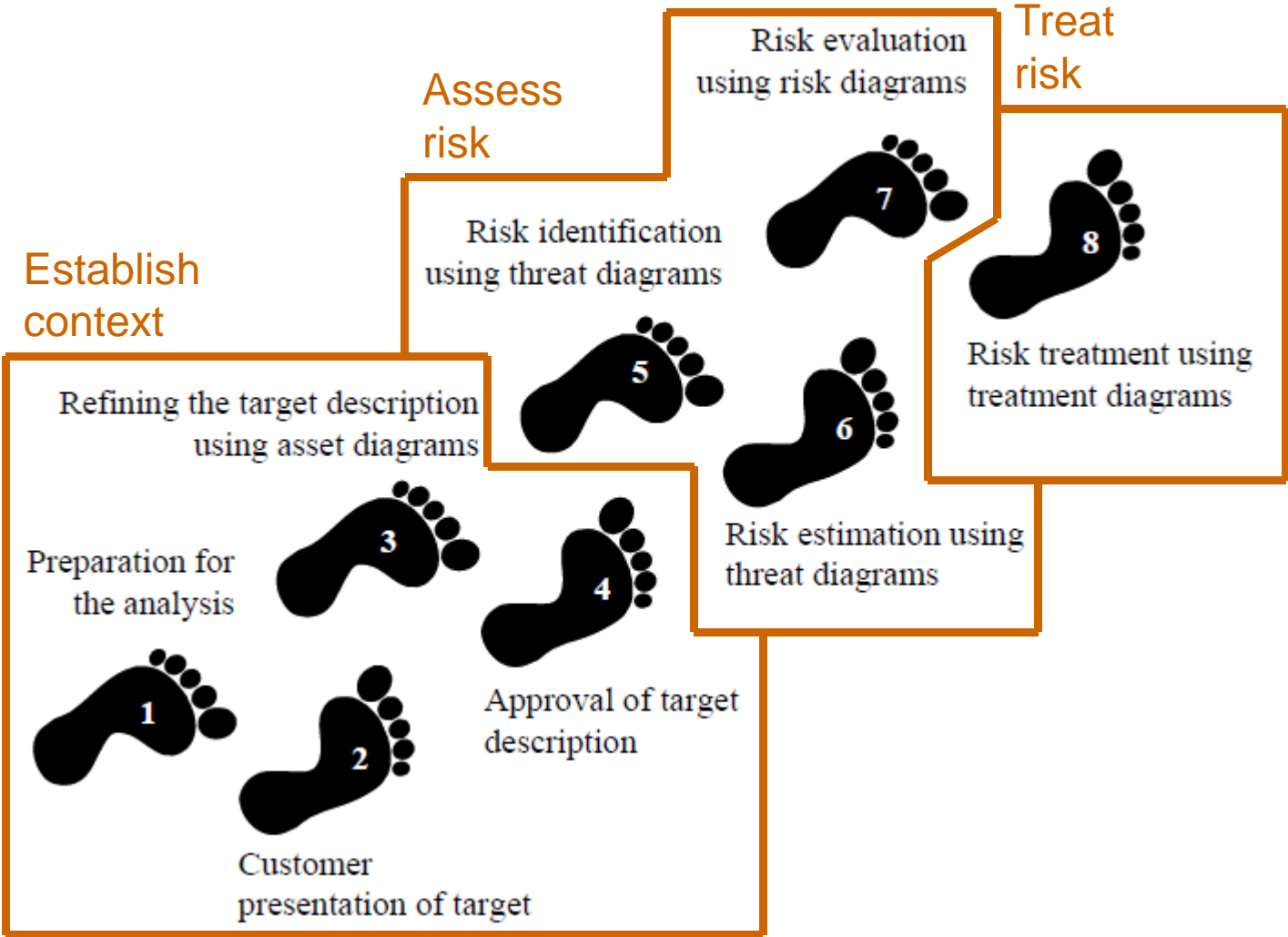
Bjørnar Solhaug

SINTEF, 2011-12-07

Overview

- The CORAS method

- ATM example

- Walkthrough of the 8 steps

- Summary

The CORAS Method

- Asset-driven defensive risk analysis method

- Operationalization of ISO 31000 risk analysis process in 8 steps

- Detailed guidelines explaining how to conduct each step in practice

- Modeling guidelines for how to use the CORAS language

The 8 Steps of the CORAS Method

Establish context

1. Preparation for the analysis
2. Customer presentation of target
3. Refining the target description using asset diagrams
4. Approval of target description

Assess risk

5. Risk identification using threat diagrams
6. Risk estimation using threat diagrams
7. Risk evaluation using risk diagrams

Treat risk

8. Risk treatment using treatment diagrams

Air Traffic Management (ATM)

- Aggregation of services provided by Air Traffic Controllers (ATCOs)
  - Main responsibility is to maintain horizontal and vertical separation among aircrafts and possible obstacles
  - Limited interaction with the external world
  - Humans at the centre of the decision and work process

The ATM Case

- Risk analysis of selected ATM services
  - Arrival management
  - Area Control Center (ACC)
  - The role and responsibilities of the Air Traffic Controllers (ATCOs)
- Main security property:
  - Information provision

Step 1: Preparation for the Analysis

- Objectives
  - Information about customer, purpose and domain of analysis
  - Decide size of analysis
  - Ensure customer is prepared
  - Practical organization of analysis
- Interaction between the customer and the analysis team
 - Preferably face-to-face meeting

ATM Example

- Customer is a national air navigation service provider
- Want risk analysis with focus on
  - Arrival management, esp. the role of the air traffic controllers (ATCOs) in the area control centre (ACC)
- The risk analysis team and the customer decides on an analysis of 250 person-hours

Step 2: Customer presentation of target

- Objective
  - Initial understanding of what to analyze
  - Focus, scope and assumptions
- Interaction between the customer and the analysis team
  - Present CORAS terminology and method
  - Decide the goals and target of the analysis
  - Decide the focus and scope of the analysis

ATM Example

- Customer presents the work environment of ATCOs
- Customer presents the desired focus
  - Information provision
  - Compliance with regulations
  - Work processes at ACCs
  - Arrival management
 - ATCOs roles and responsibilities
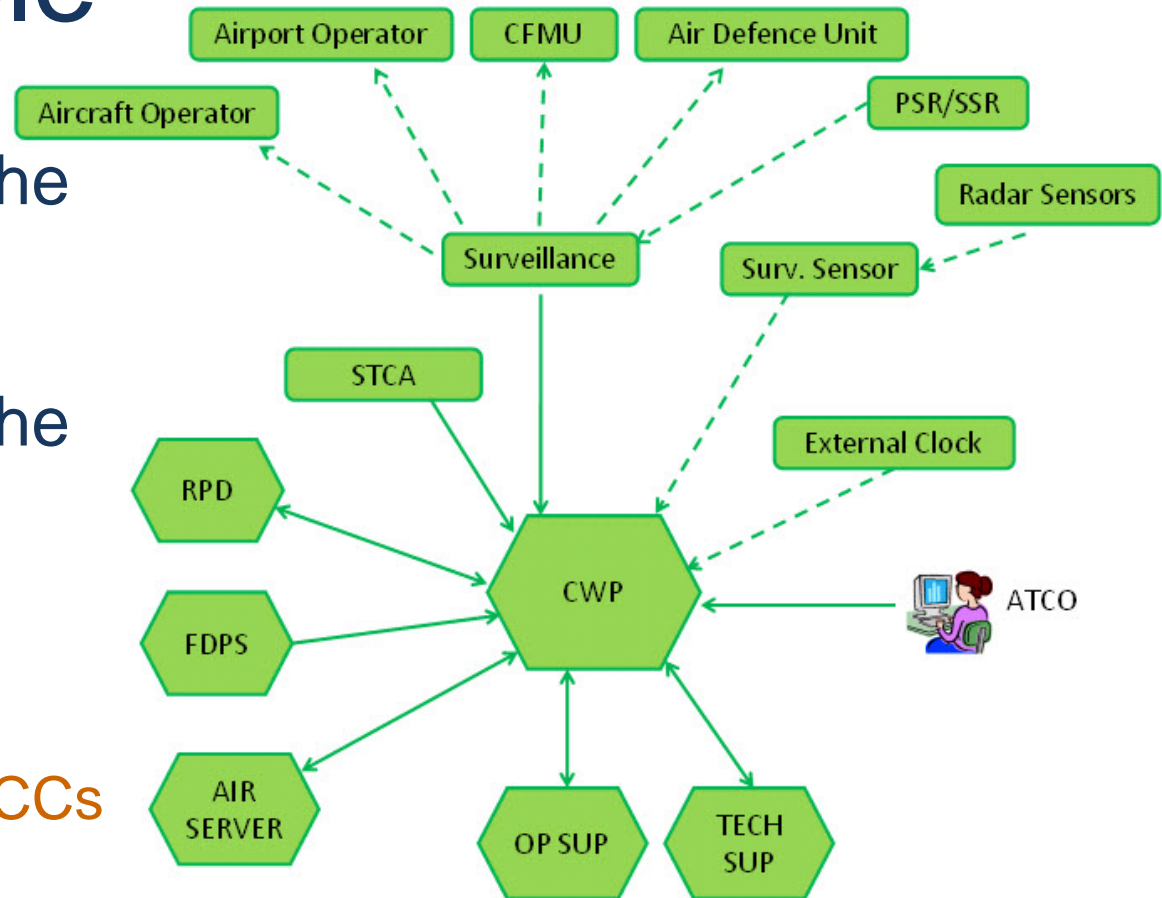
Step 3: Refining the Target Description Using Asset Diagrams

- Objective
  - Ensure common understanding of target including scope, focus and assets
- Face-to-face meeting
  - Analysis team presents the target
  - Asset identification
  - High-level analysis

Target Description

- The **target description** is the documentation of all the information that serves as the input to and the basis for a risk analysis
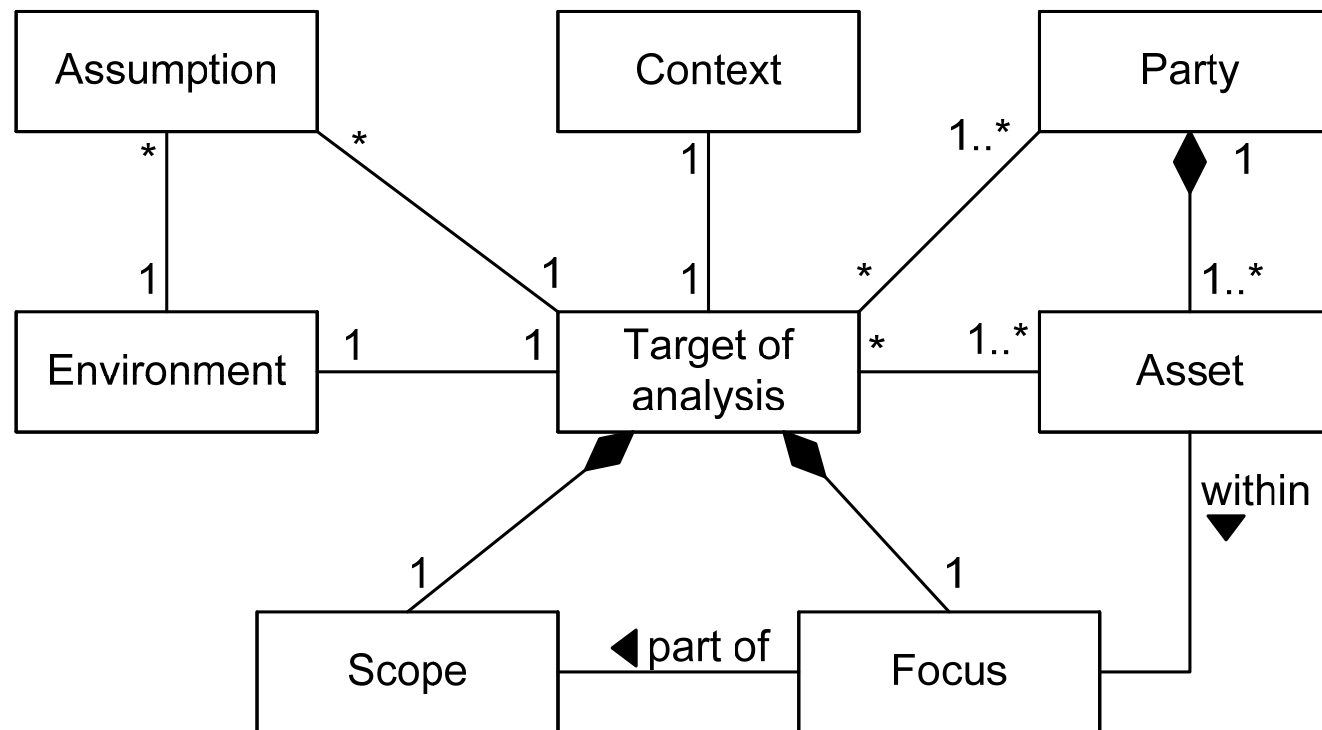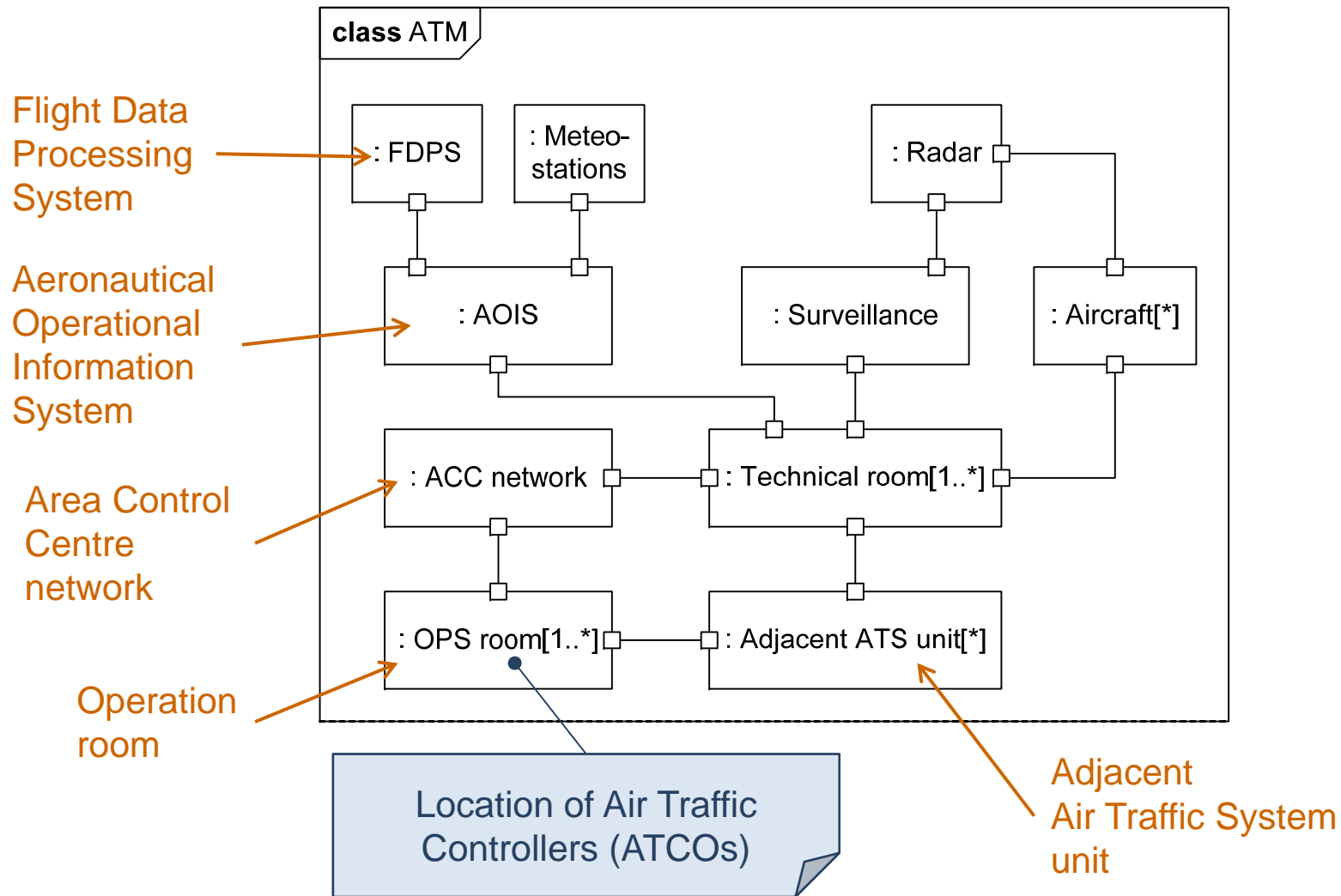
Target Description - Definitions

- **Asset:** Something to which a party assigns value and hence for which the party requires protection

- **Assumption:** Something we take as granted or accept as true (although it may not be so)

- **Context of analysis:** The premises for and the background of a risk analysis. This includes the purposes of the analysis and to whom the analysis is addressed

- **Environment of target:** The surrounding things of relevance that may affect or interact with the target; in the most general case, the rest of the world

- **Focus of analysis:** The main issue or central area of attention in a risk analysis. The focus is within the scope of the analysis

- **Party:** An organization, company, person, group or other body on whose behalf a risk analysis is conducted

- **Scope of analysis:** The extent or range of a risk analysis. The scope defines the border of the analysis, in other words what is held inside of and what is held outside of the analysis

- **Target of analysis:** The system, organization, enterprise, or the like that is the subject of a risk analysis
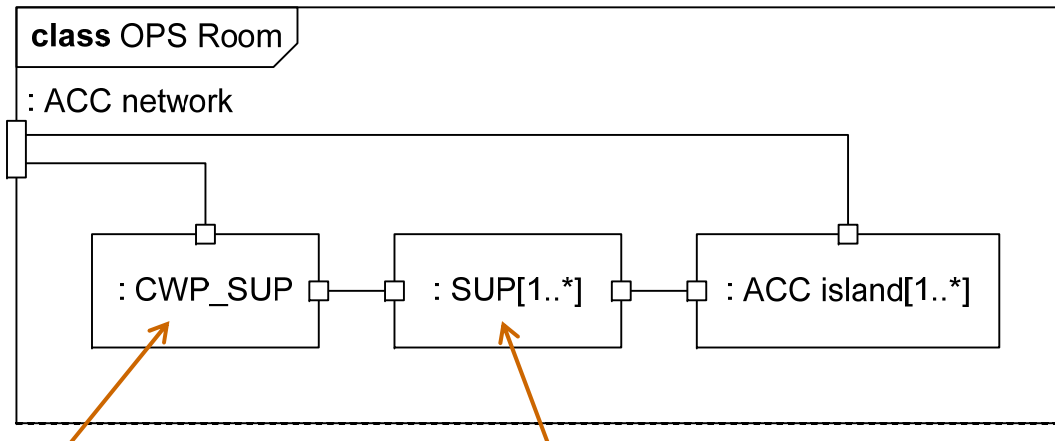
ATM Example: Target Description

- The analysis team presents their understanding of the target
- Target of analysis described using UML
    - Conceptual overview using UML class diagrams
    - Component structure using UML structured classifiers
    - Activities using UML interactions (interaction overview diagrams and sequence diagrams)
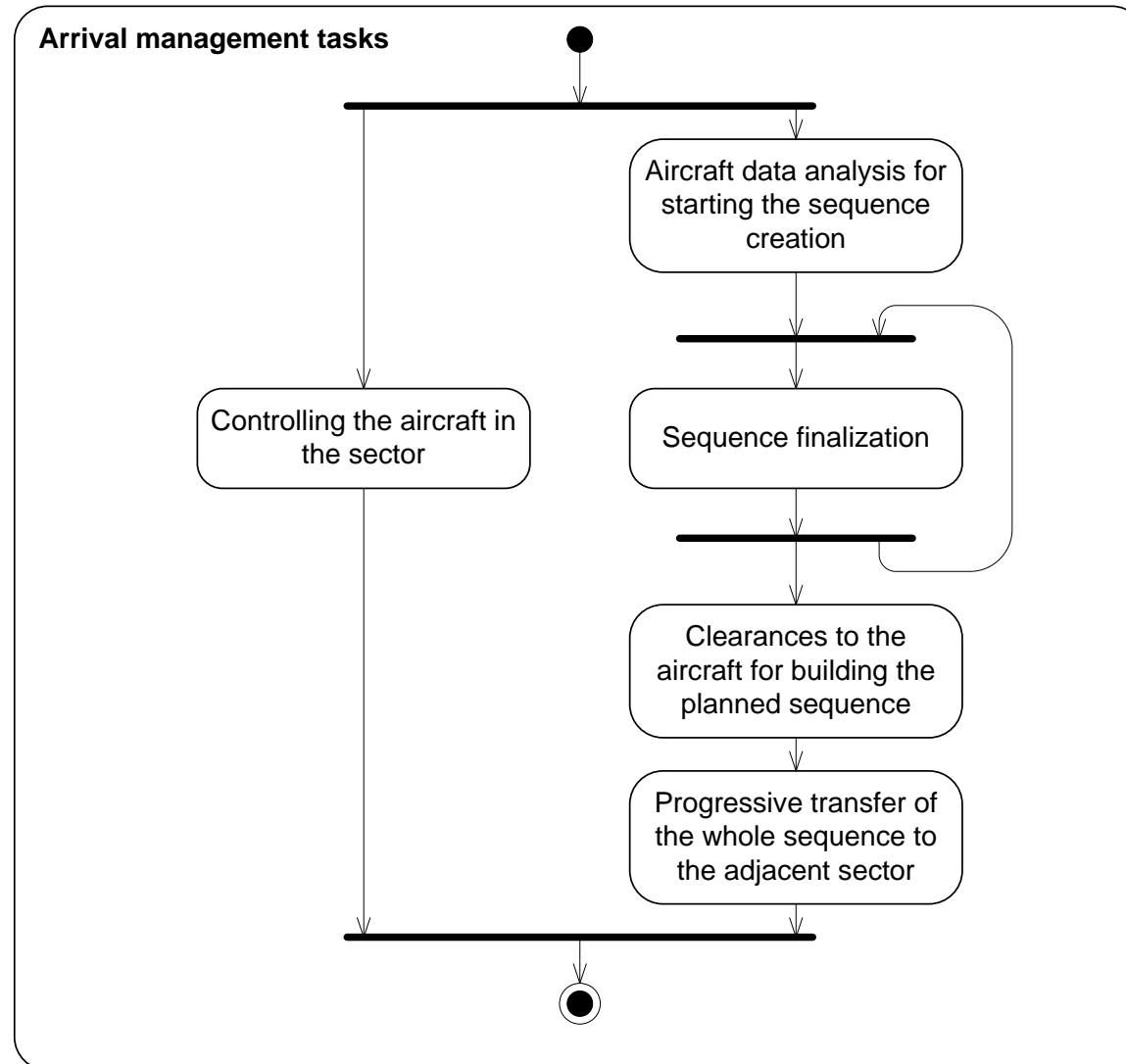
ATM Example: Target Description

Flight Data Processing System → : FDPS

Aeronautical Operational Information System → : AOIS

Area Control Centre network → : ACC network

Operation room → : OPS room[1..*]

Location of Air Traffic Controllers (ATCOs)

Adjacent Air Traffic System unit → : Adjacent ATS unit[*]

class ATM

: FDPS   : Meteo-stations   : Radar

: AOIS   : Surveillance   : Aircraft[*]

: ACC network   : Technical room[1..*]

: OPS room[1..*]   : Adjacent ATS unit[*]

# ATM Example: Target Description

- SUP is an air traffic controller (ATCO) supervising the traffic management of an ACC island
- ATCOs in the ACC island work in teams of two

ATM Example: Target Description

Arrival management tasks

- Aircraft data analysis for starting the sequence creation
- Controlling the aircraft in the sector
- Sequence finalization
- Clearances to the aircraft for building the planned sequence
- Progressive transfer of the whole sequence to the adjacent sector

ATM Example: Asset identification

- Assets are the values the parties of the analysis wants to protect
- Identified assets are presented in CORAS asset diagrams
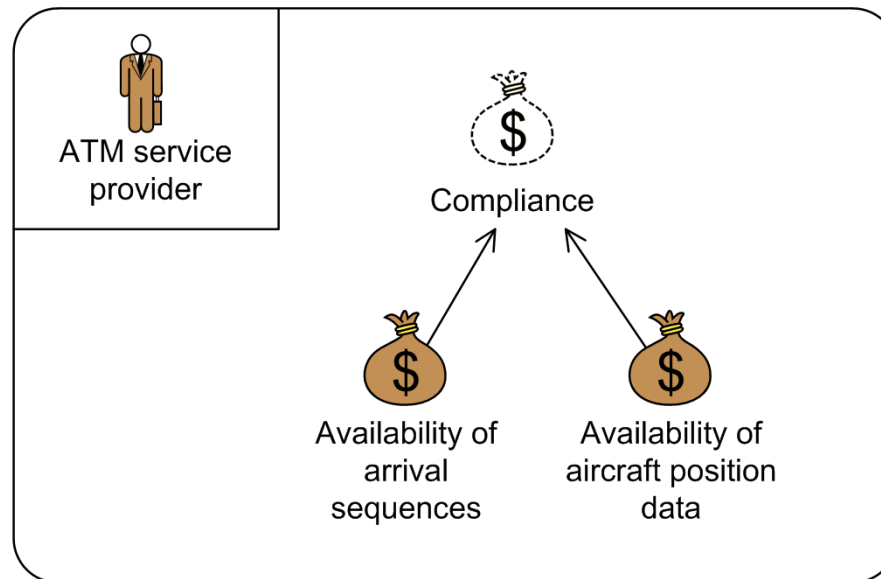
ATM Example: High-level analysis

- Threat, vulnerabilities, threat scenarios and unwanted incidents are identified in a brainstorming session
- Identify biggest worries and increase understanding of focus and scope

ATM Example: High-level analysis

Who/what causes it?	How? What is the scenario or incident? What is harmed	What makes it possible?
Component failure; power loss	Provisioning of information to ATCO fails due to loss of CWP	Insufficient CWP maintenance
Software error	The consolidation of data from several radar sources fails	Lack of redundant aircraft tracking systems
Component failure; radar disturbance	Malfunctioning of radar antenna; loss of aircraft tracking	Insufficient radar maintenance
Software bugs	False or redundant alerts from safety tool	Insufficient software testing

Step 4: Approval of Target Description

- Objective
  - Ensure target description is correct and complete
  - Ranking of assets
  - Scales for risk estimation
  - Risk evaluation criteria
- Face-to-face meeting
  - Structured walk-through of target description
  - Plenary discussion on assets, scales and criteria

Consequence Scales

- One consequence scale for each asset is defined

  - Note: Sometimes one scale applies to several assets

- Consequences can be qualitative or quantitative

- Scales can be continuous, discrete or with intervals

ATM Example: Consequence Scale

- One consequence scale for each of the three assets is defined
  - Two direct assets and one indirect asset
- In the ATM example, one consequence scale applies to the two direct availability assets

Consequence	Description
Catastrophic	Catastrophic accident
Major	Abrupt maneuver required
Moderate	Recovery from large reduction in separation
Minor	Increasing workload of ATCOs or pilots
Insignificant	No hazardous effect on operations

The consequence and likelihood scales are partly based on requirements and advisory material provided by EUROCONTROL

Likelihood Scale

- One likelihood scale is defined
  - The scale is used for all unwanted incidents and threat scenarios
- Likelihoods can be
  - Qualitative or quantitative
  - Probabilities or frequencies
- Scales can be continuous, discrete or with intervals

ATM Example: Likelihood Scale

- Qualitative likelihood scale in terms of frequency

| Likelihood	Description
Certain	A very high number of similar occurrences already on record; has occurred a very high number of times at the same location/time
Likely	A significant number of similar occurrences already on record; has occurred a significant number of times at the same location
Possible	Several similar occurrences on record; has occurred more than once at the same location
Unlikely	Only very few similar incidents on record when considering a large traffic volume or no records on a small traffic volume
Rare	Has (almost) never occurred yet throughout the total lifetime of the system

ATM Example: Risk Evaluation Criteria

Consequence

	Insignificant	Minor	Moderate	Major	Catastrophic
Rare	🟩	🟩	🟨	🟨	🟥
Unlikely	🟩	🟩	🟨	🟨	🟥
Possible	🟩	🟩	🟨	🟥	🟥
Likely	🟩	🟨	🟨	🟥	🟥
Certain	🟩	🟨	🟨	🟥	🟥

(Row label: **Likelihood**)

- **High risk:** Unacceptable and must be treated
- **Medium risk:** Must be evaluated for possible treatment
- **Low risk:** Must be monitored

Step 5: Risk Identification Using Threat Diagrams

- Objective
  - Identify risk: where, when, why and how they may occur
- Workshop conducted as a brainstorming session
  - Involving people of different background
  - Assets and high-level analysis as starting point
  - Threats, threat scenarios, vulnerabilities and unwanted incidents documented on-the-fly using threat diagrams

ATM Example: Risk Identification
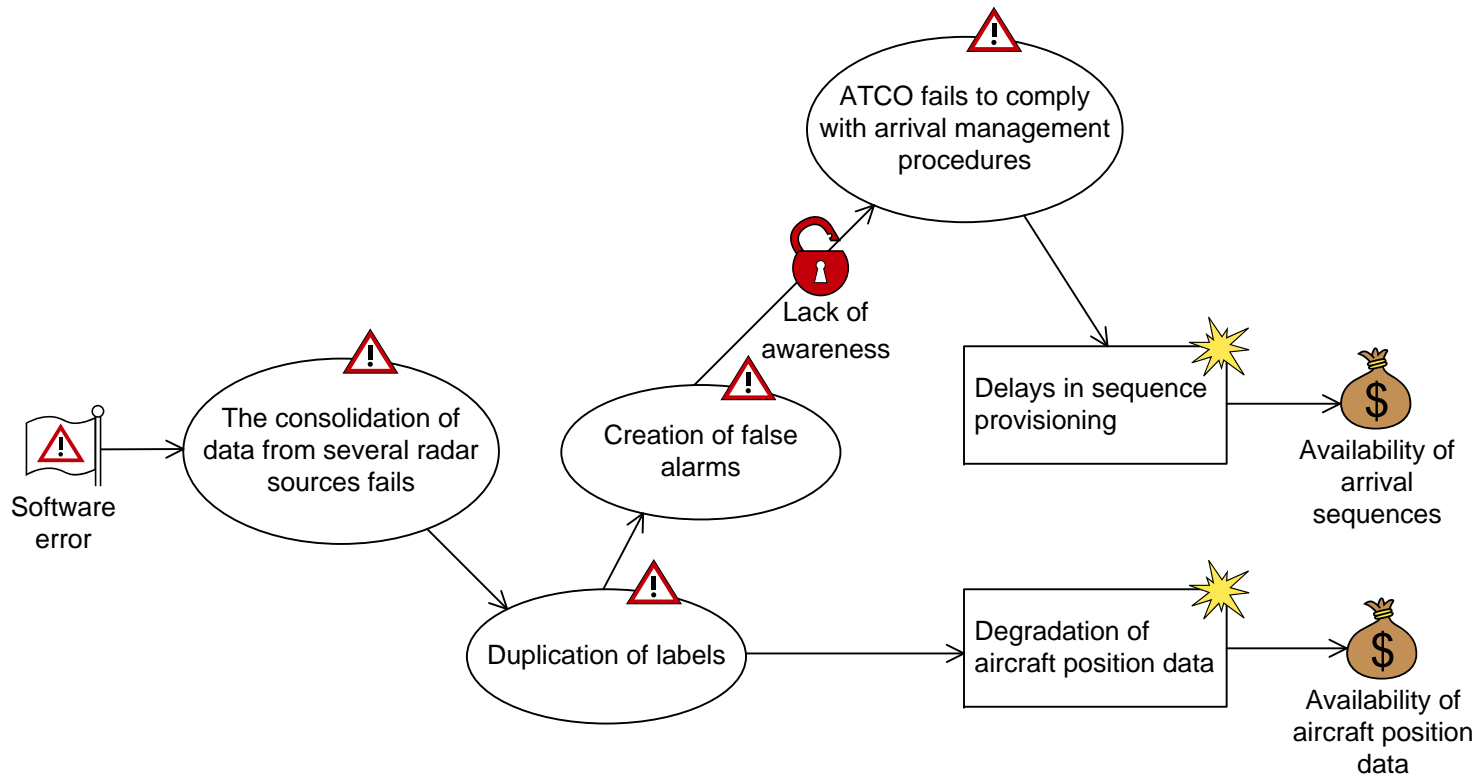
ATM Example: Risk Identification
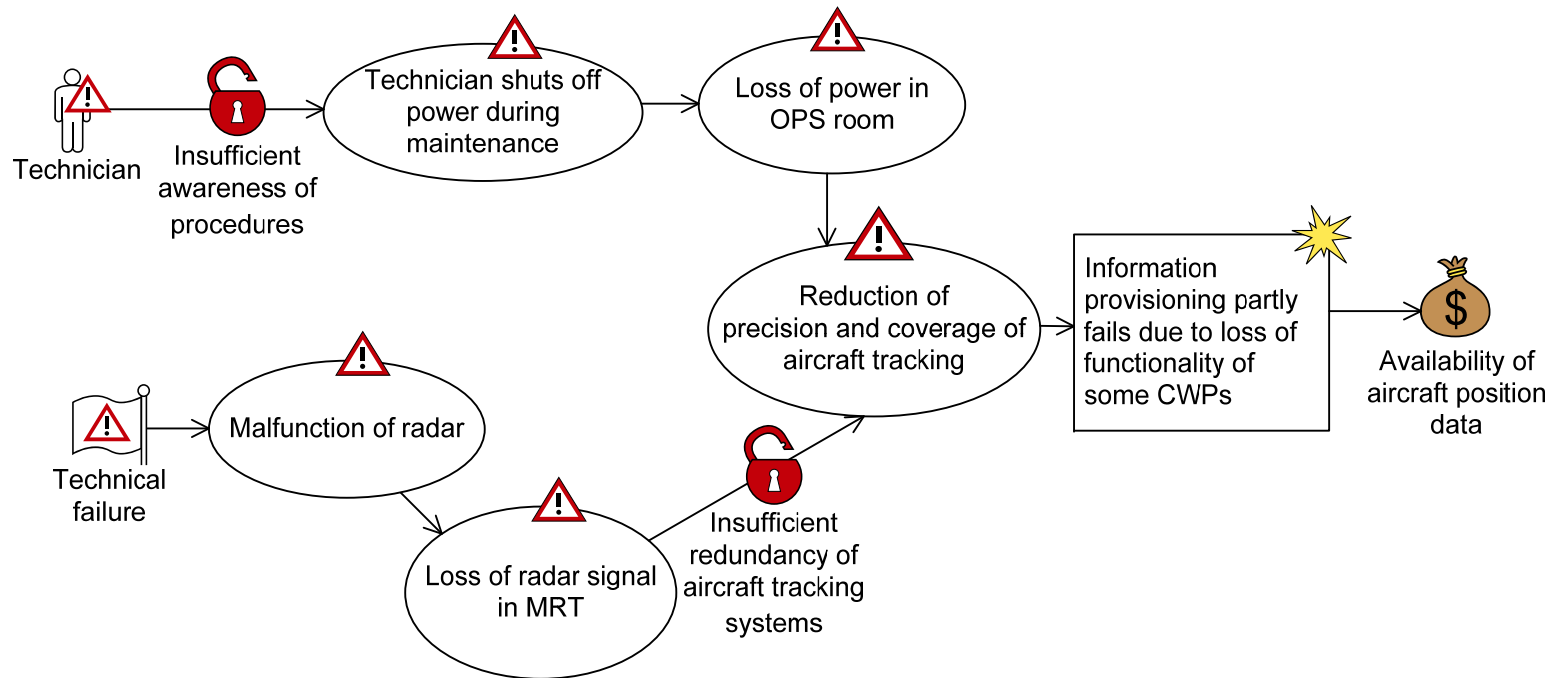
Step 6: Risk Estimation Using Threat Diagrams

- Objective
  - Determine the level of identified risks

- Workshop
  - Involving people of different background
  - Walk-through of threat diagrams
  - Likelihood estimates on threat scenarios, unwanted incidents and relations between them
  - Consequence estimates on relation between unwanted incidents and assets
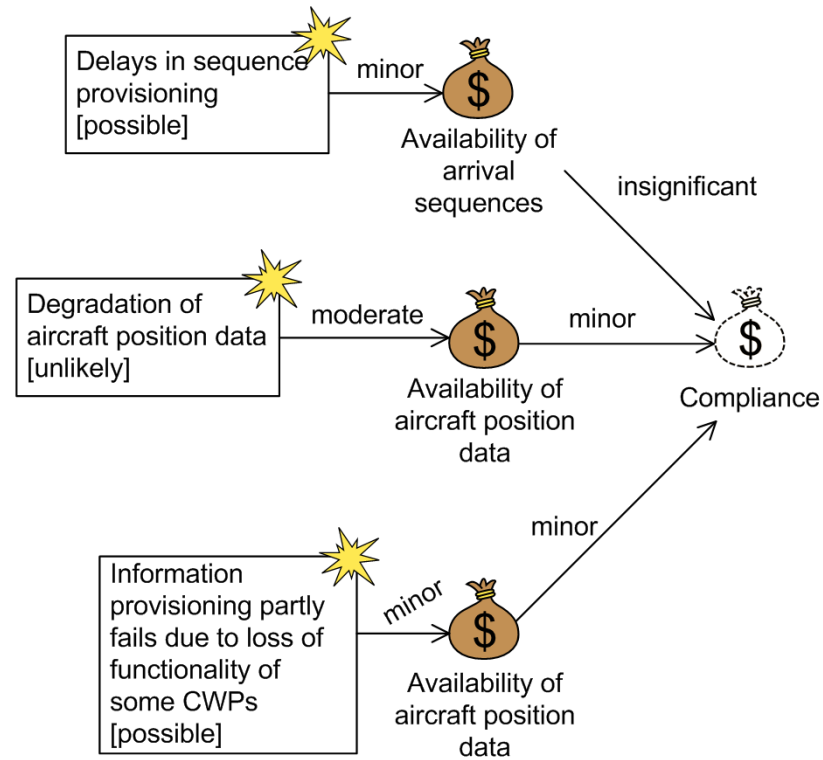
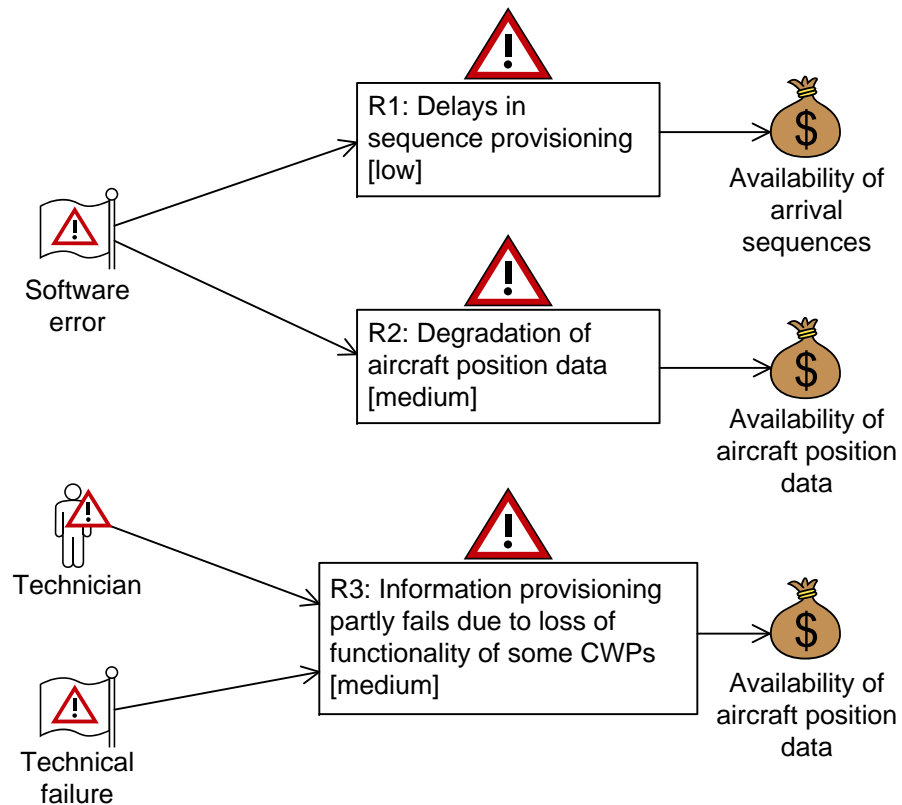# ATM Example: Risk Estimation
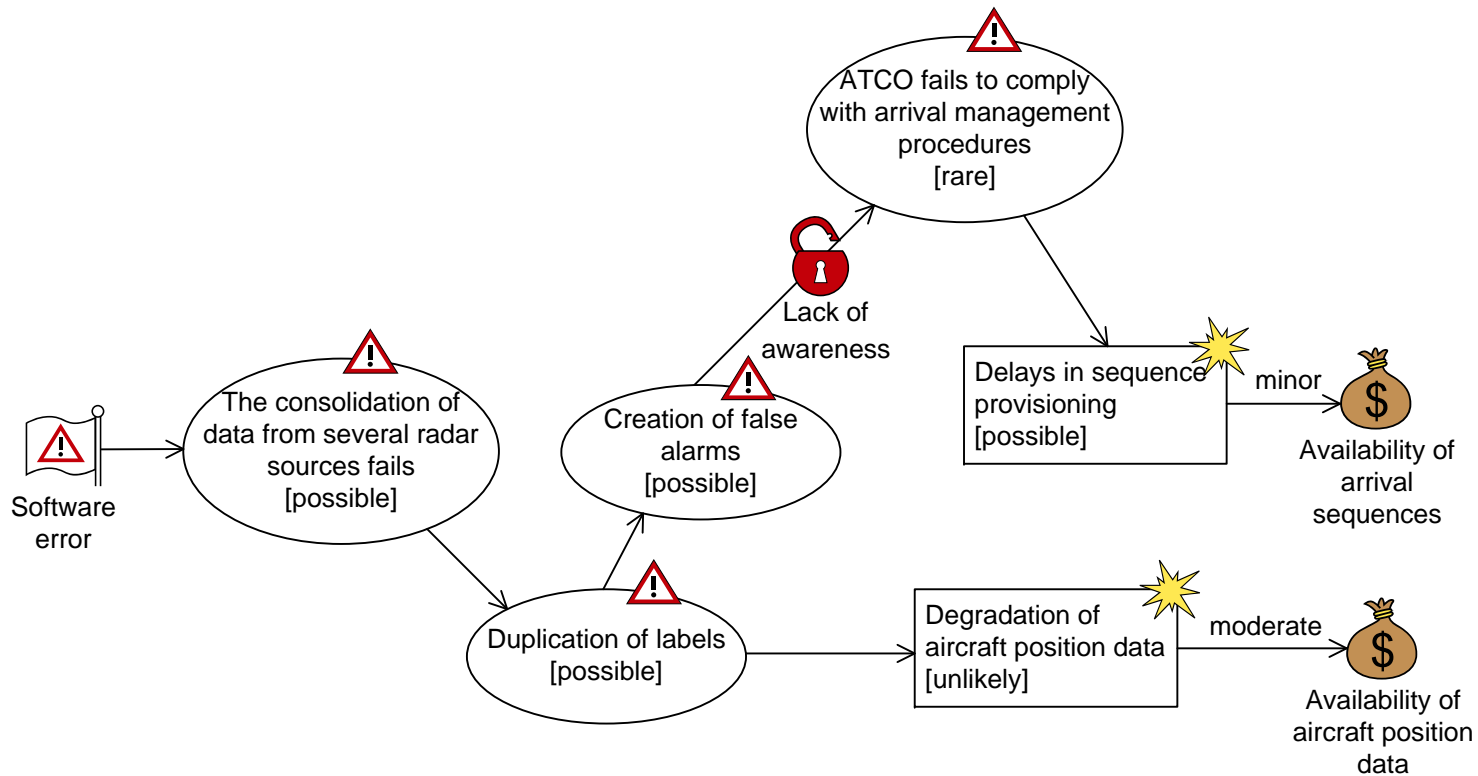
ATM Example: Risk Estimation
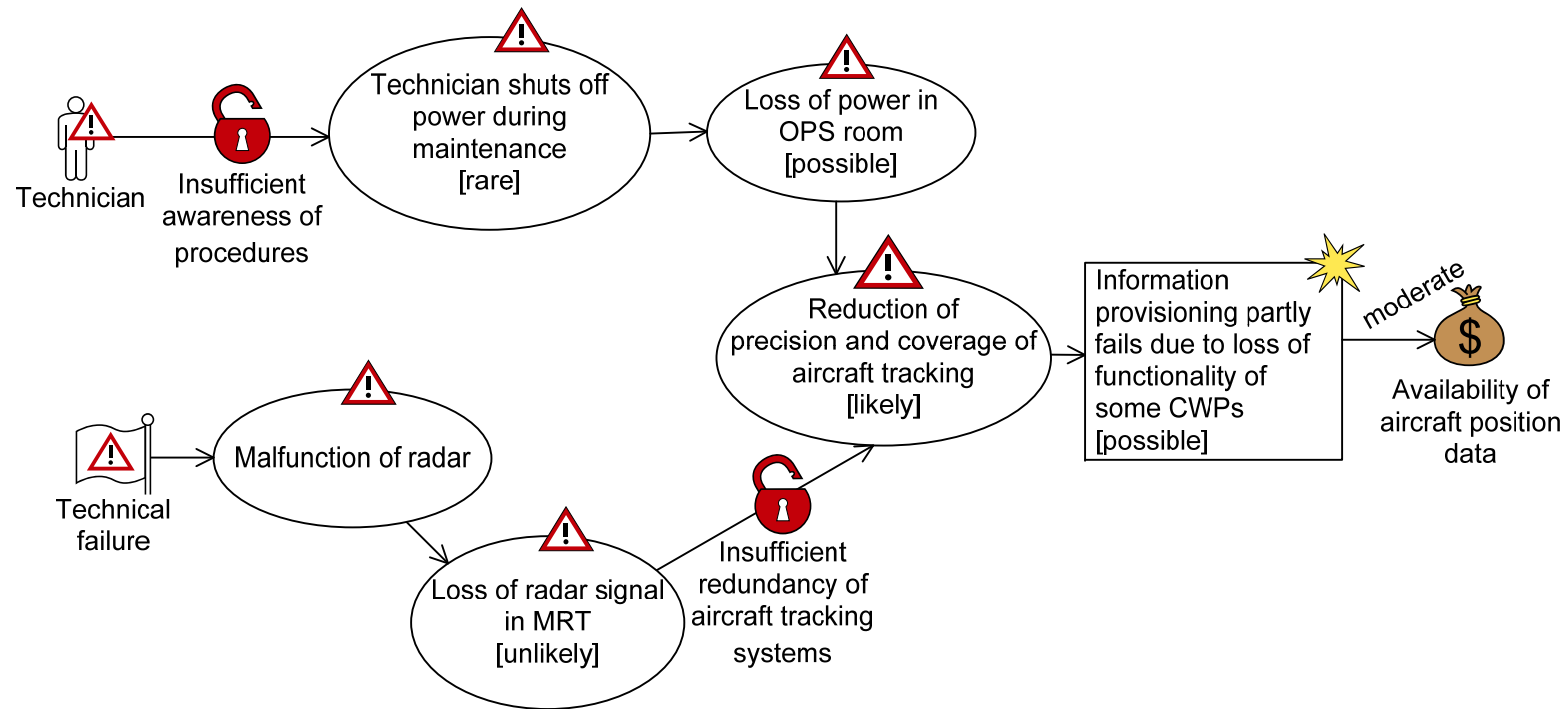
Step 7: Risk Evaluation Using Risk Diagrams

- Objective
  - Determine which risks are unacceptable and must be evaluated for treatment
- Off-line activity
  - Calculate risk levels from estimates
  - Present risks in risk diagrams
- Assess potential impact of identified risk
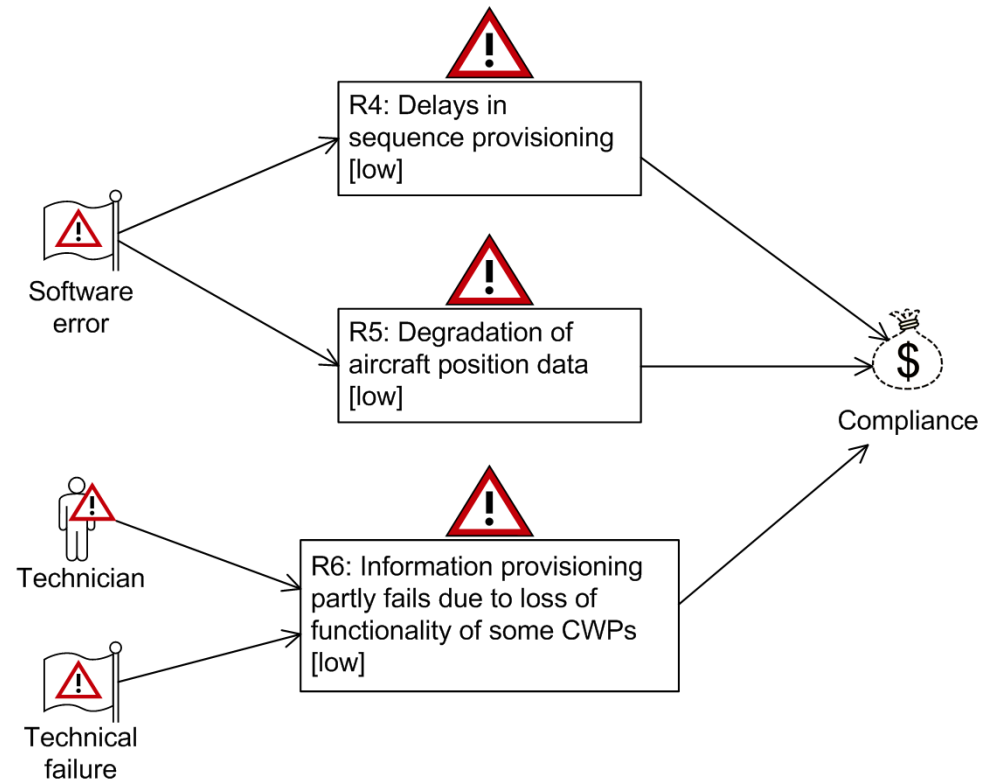 - Risks that accumulate
  - Risks with respect to indirect assets

ATM Example: Indirect Assets

ATM Example: Risk Diagrams

ATM Example: Risk Diagrams

ATM Example: Risk Evaluation

Consequence

	Insignificant	Minor	Moderate	Major	Catastrophic
Rare					
Unlikely		R5	R2		
Possible	R4	R1, R6	R3		
Likely					
Certain					

Likelihood (row axis label)

- Risk levels are calculated using the risk matrix
- The risk matrix moreover serves as the risk evaluation criteria

Step 8: Risk Treatment Using Treatment Diagrams

- Objective
  - Indentify cost effective treatments for unacceptable risks
- Workshop with brainstorming session
  - Involving people of different background
  - Walk-through of threat diagrams
  - Identify treatments to unacceptable risks

ATM Example: Treatment Diagram
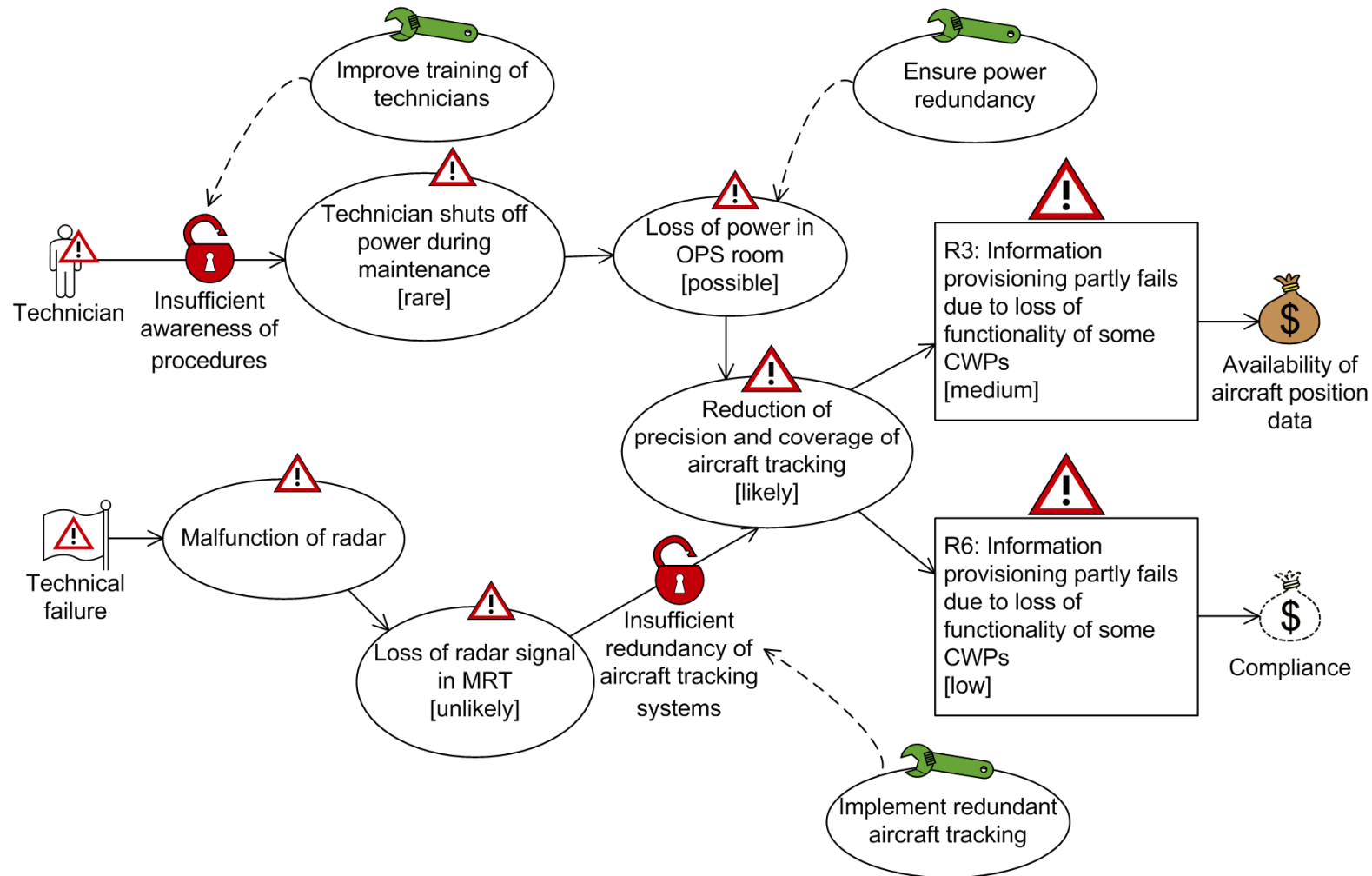
Summary

- **CORAS is a model-driven approach to risk analysis**

- **Language and tool support for all phases**

- **Practical guidelines**
    - How to conduct the various tasks
    - How to do the risk modeling

- **Closely based on the ISO 31000 standard**