

# Security Risk Assessment II

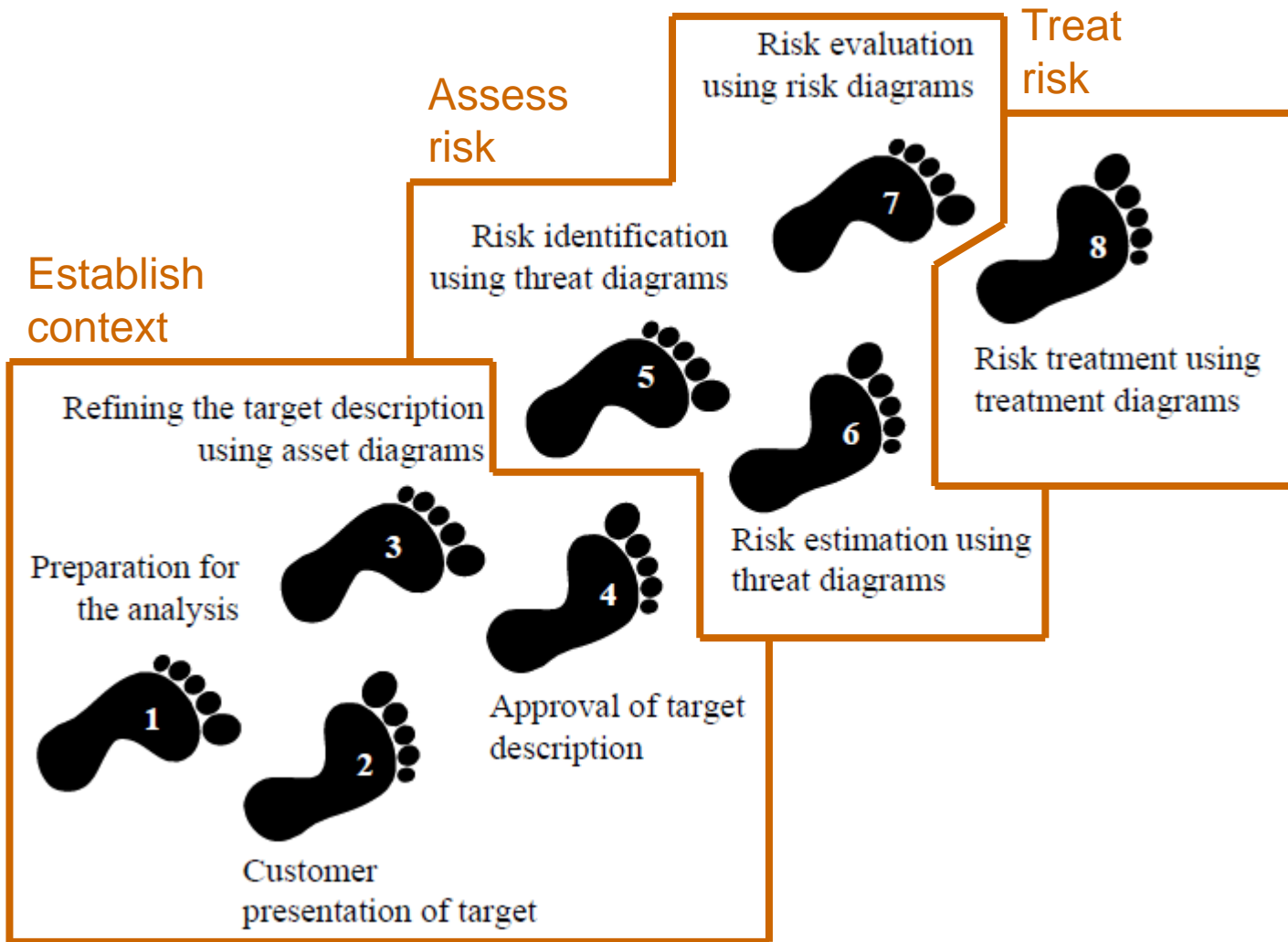
Ketil Stølen



# Overview

- CORAS exemplified
- Walkthrough of the 8 steps based on the ATM example
- Calculation of frequencies

# The 8 Steps of the CORAS Method



# Step 1: Preparation for the assessment

- Objectives
  - Obtain information about customer, purpose and domain of assessment
  - Decide size of assessment
  - Ensure customer is prepared
  - Practical organization of analysis
- Interaction between the customer and the analysis team
  - By mail, phone or face-to-face

# Preliminaries

- Customer is a national air navigation service provider
- The customer decides on an assessment of 250 person-hours

# Target of risk assessment

- The role of the Air Traffic Controllers (ATCOs) in the process of arrival management
- Information provisioning
- Compliance



# Air Traffic Control (ATC)

- Maintain horizontal and vertical separation among aircrafts and possible obstacles
- Limited interaction with the external world
- Humans at the centre of decisions and work process

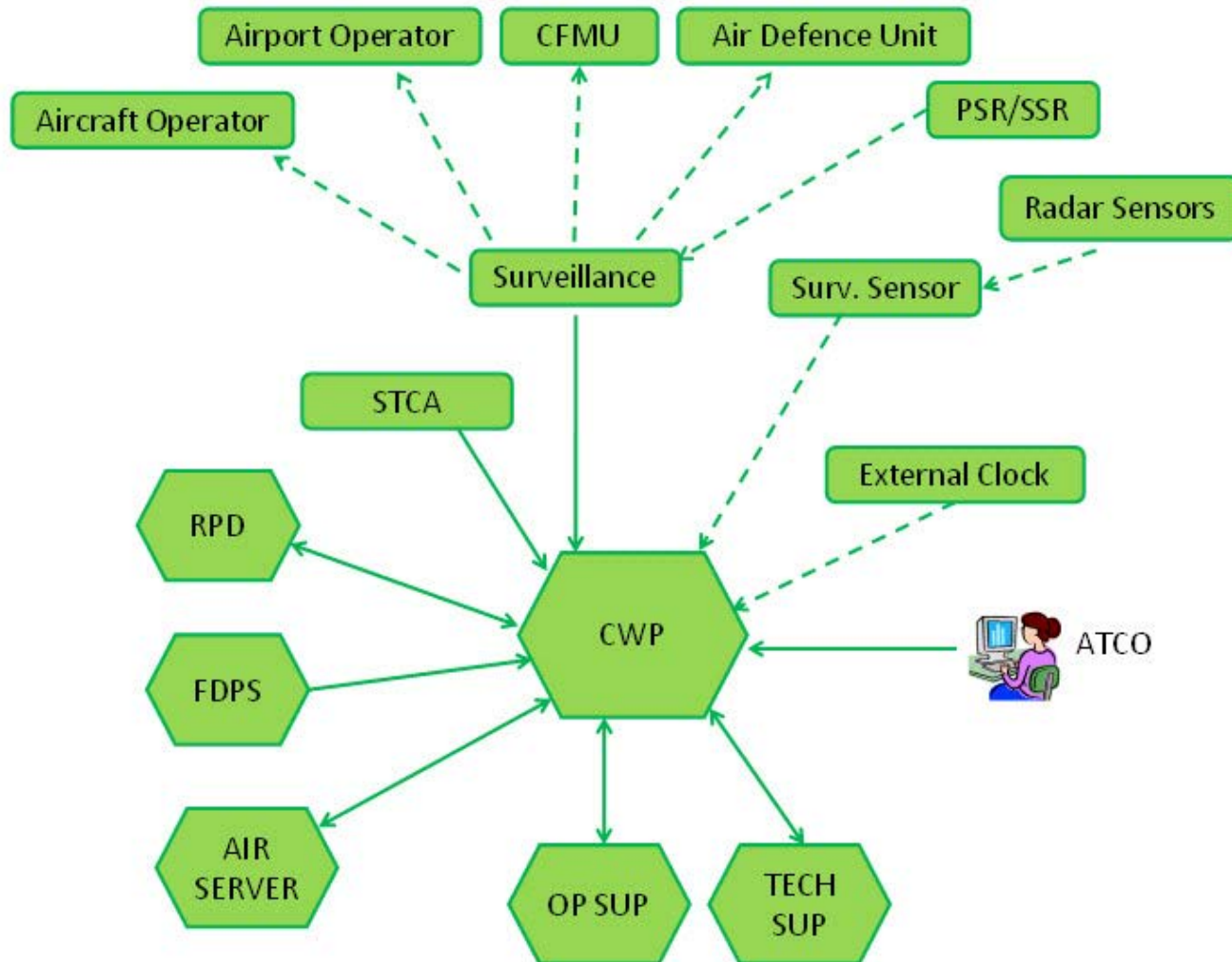


# Step 2: Customer presentation of target

- Objective
  - Obtain understanding of what to assess
  - Identify focus, scope and assumptions
- Face-to-face between the customer and the assessment team
  - Present CORAS terminology and method
  - Collect as much information as possible



# Example documentation



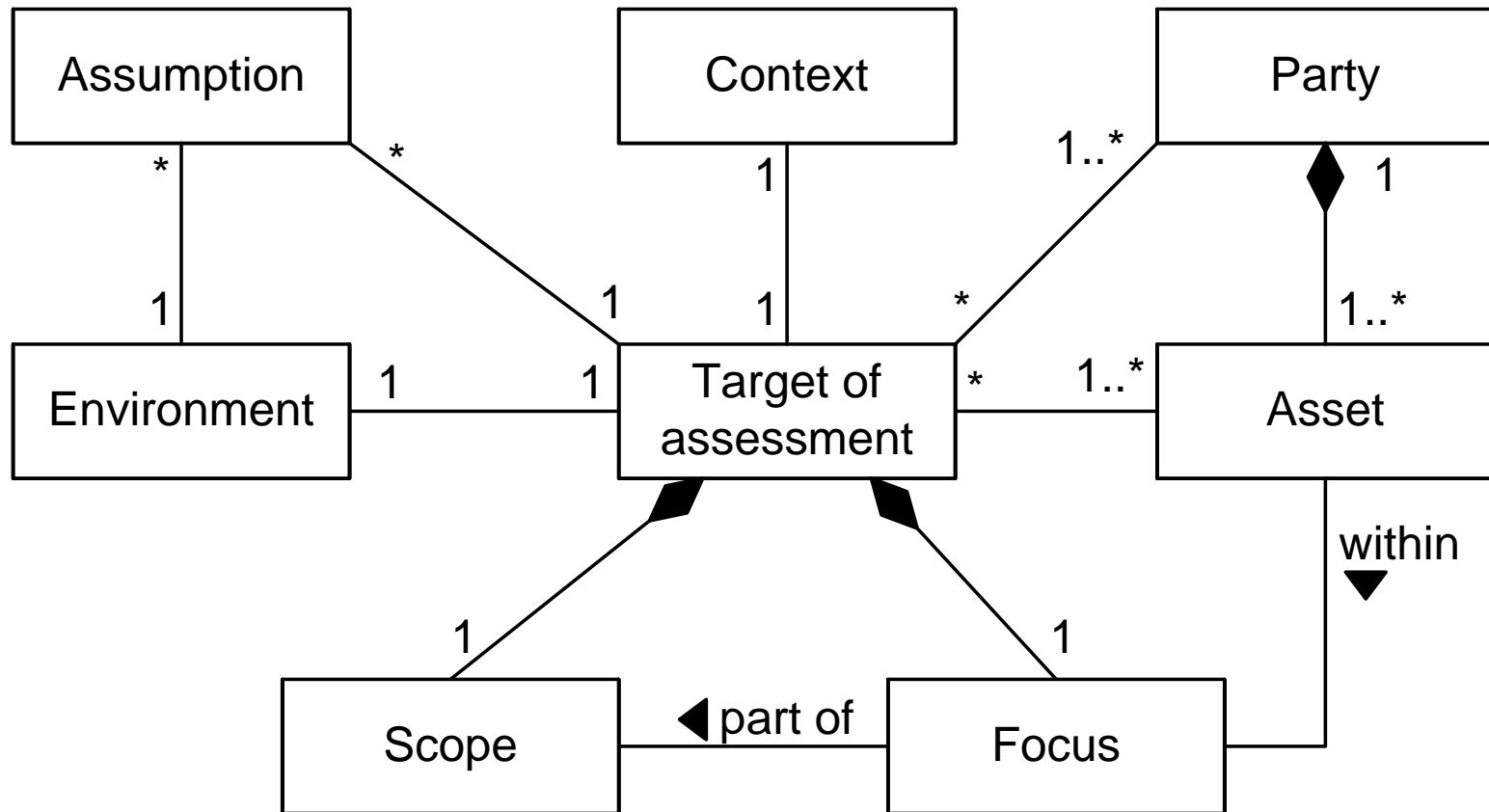
# Step 3: Refine target description using asset diagrams

- Objective
  - Ensure common understanding of target including scope, focus and assets
- Face-to-face meeting
  - Assessment team presents their understanding of the target
  - Assets are identified
  - High-level assessment

# Target Description

- **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 assessment:** The premises for and the background of a risk assessment, including its purposes
- **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 assessment:** The main issue or central area of attention in a risk assessment
- **Party:** An organization, company, person, group or other body on whose behalf a risk assessment is conducted
- **Scope of assessment:** The extent or range of a risk assessment. The scope defines the border of the assessment, in other words what is held inside of and what is held outside of the assessment
- **Target of assessment:** The system, organization, enterprise, or the like that is the subject of a risk assessment

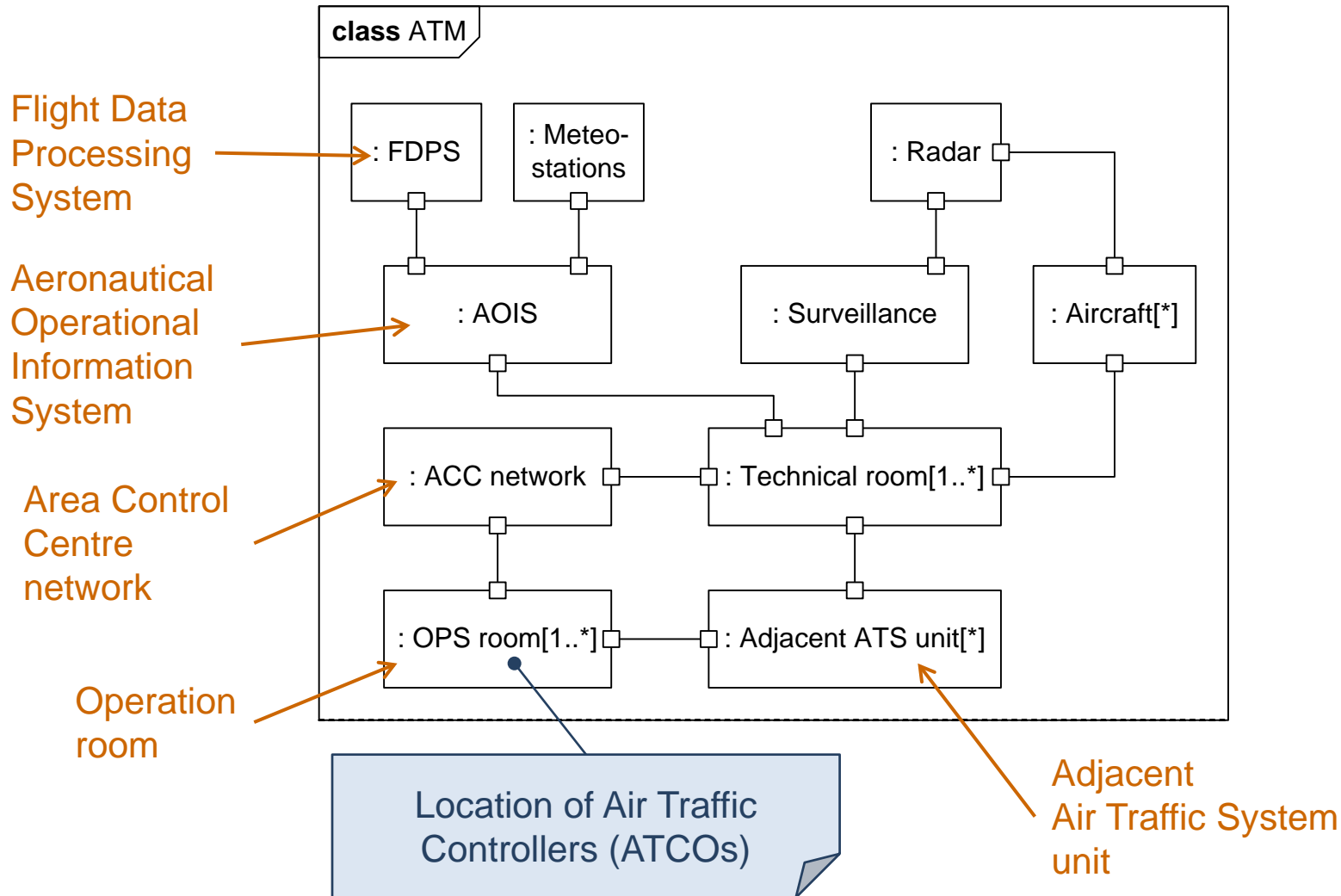
# Target Description



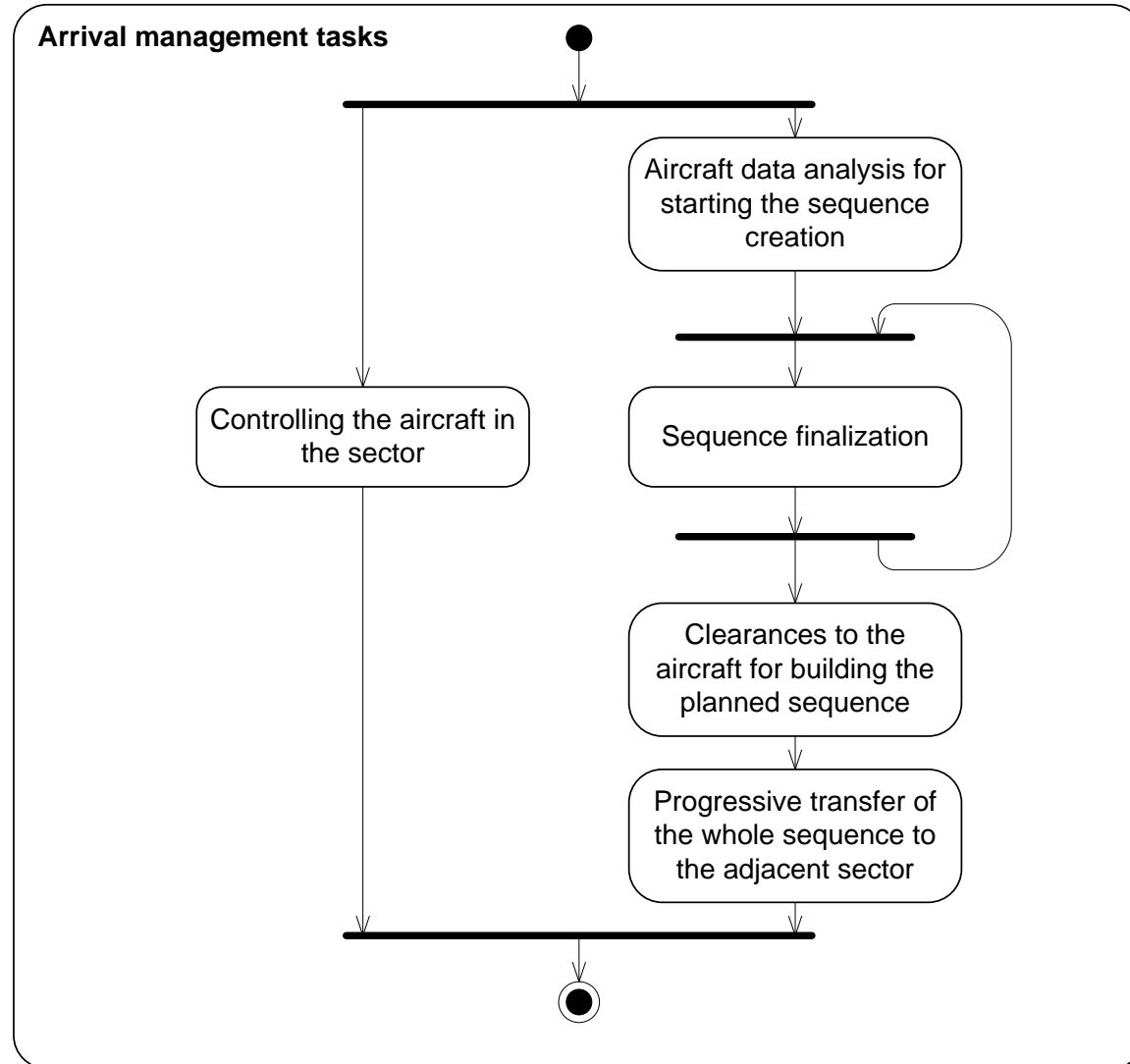
# ATM target description

- Conceptual overview using UML class diagrams
- Activities using UML structured classifier and activity diagrams

# ATM Example: Target Description

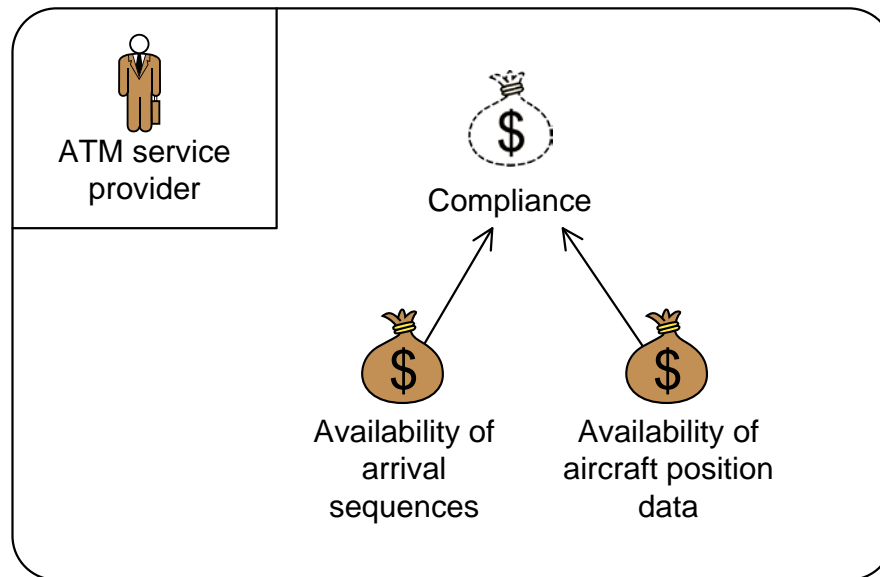


# ATM Example: Target Description



# 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

		
<b>Who/what causes it?</b>	<b>How? What is the scenario or incident? What is harmed</b>	<b>What makes it possible?</b>
Component failure; power loss	Provisioning of information to ATCO fails due to loss of CWP (Controller Working Position)	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

- The same 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

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 never occurred yet throughout the total lifetime of the system

# ATM Example: Risk Evaluation Criteria

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Rare					
	Unlikely					
	Possible					
	Likely					
	Certain					

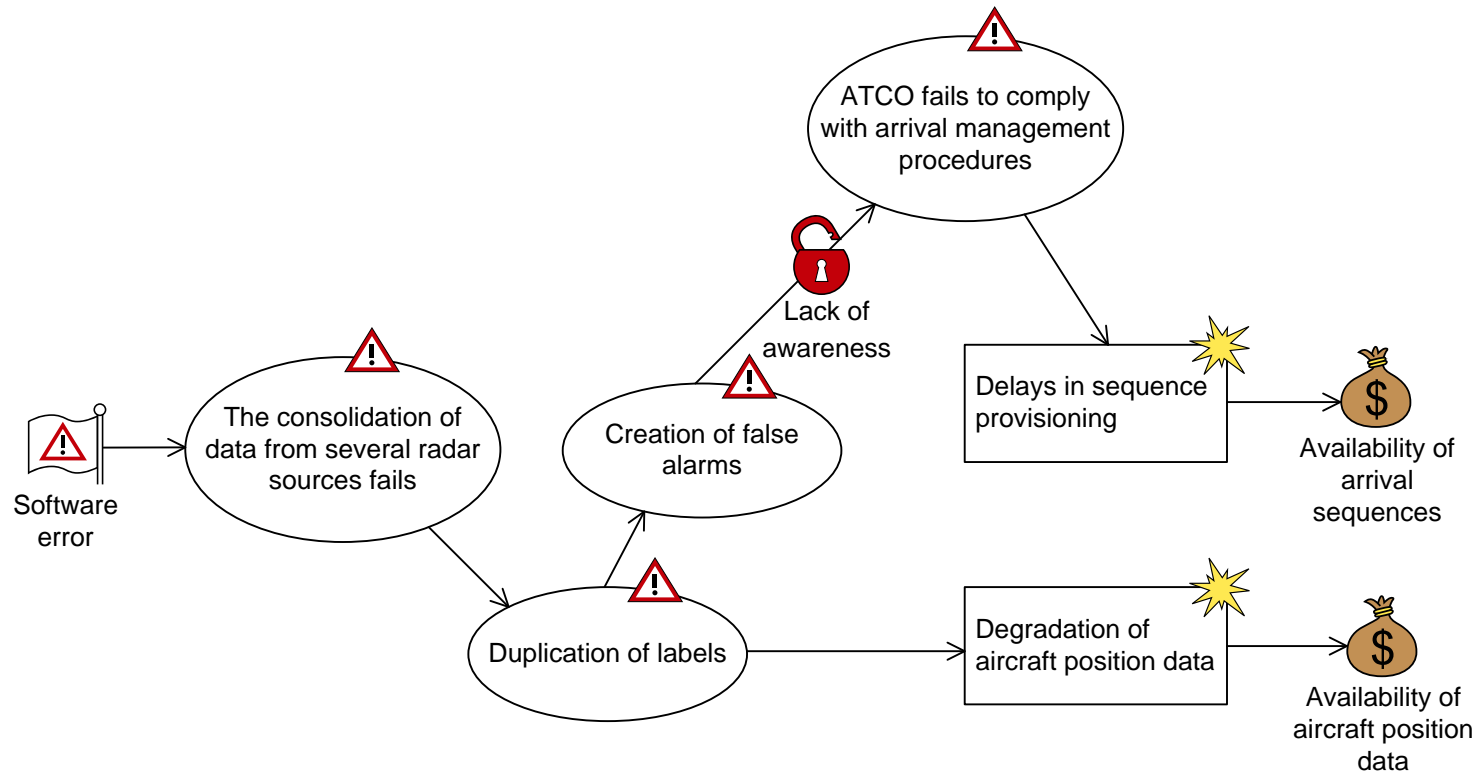
- **High risk:** Unacceptable and must be treated
- **Medium risk:** Must be evaluated for possible treatment
- **Low risk:** Must be monitored



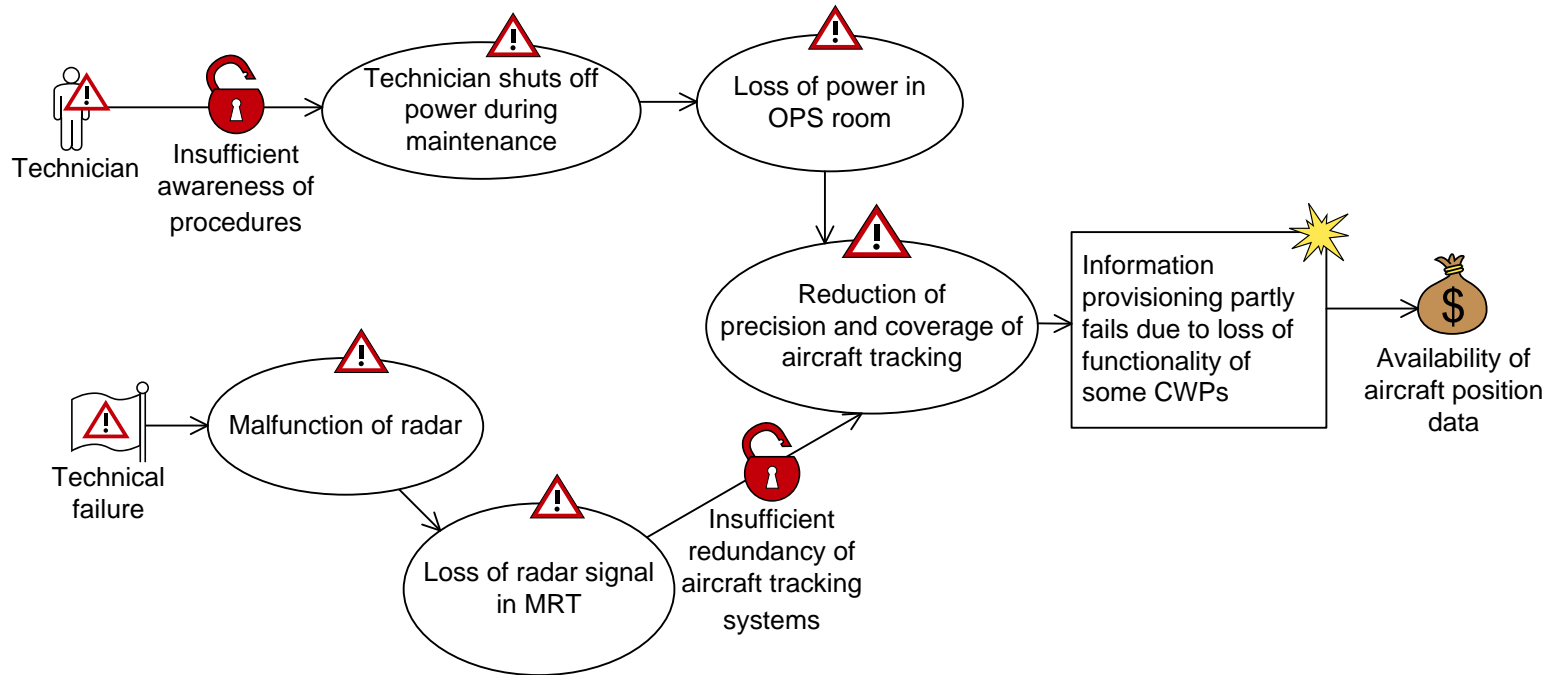
# Step 5: Risk Identification Using Threat Diagrams

- 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



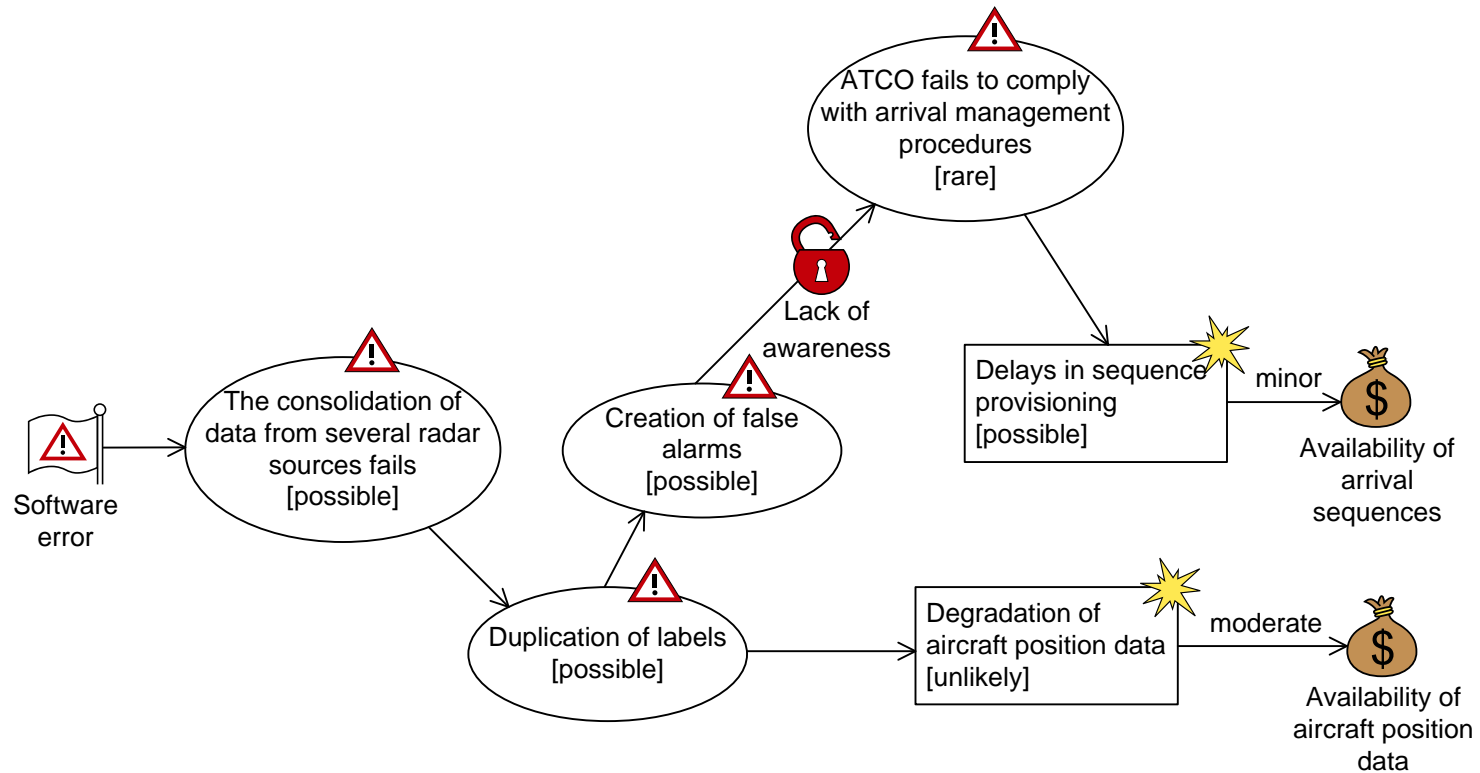
# ATM Example: Risk Identification



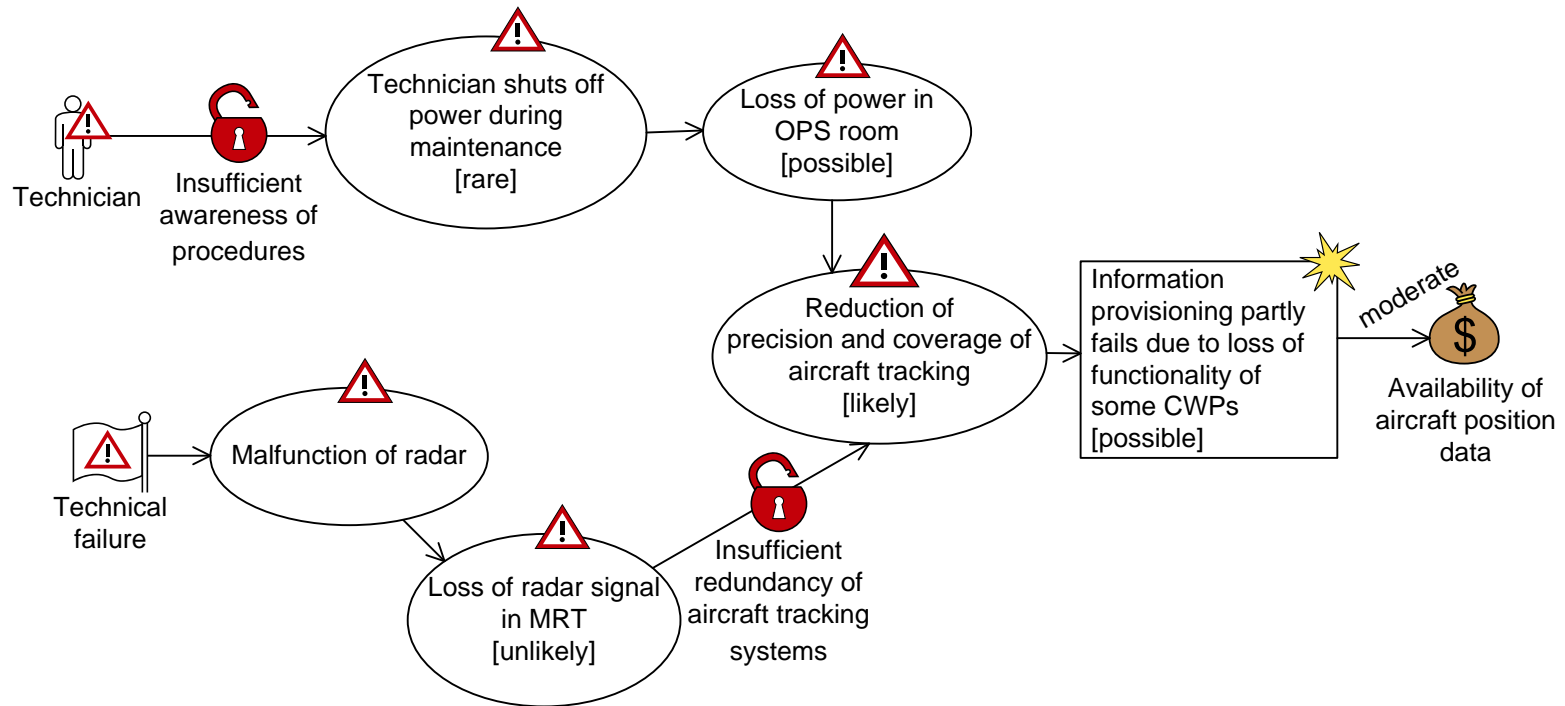
# Step 6: Risk Estimation Using Threat Diagrams

- 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



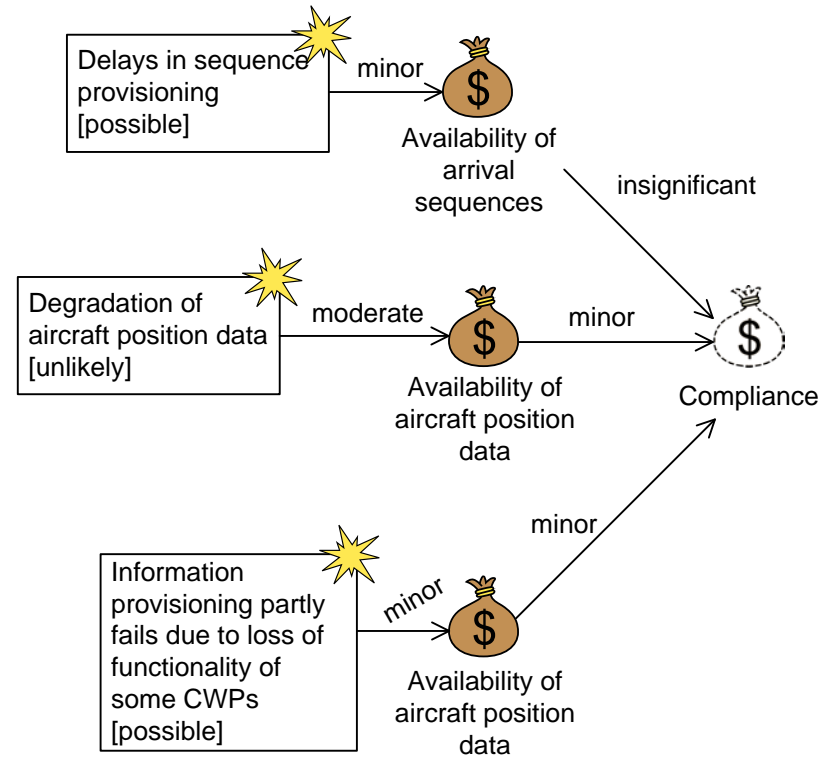
# ATM Example: Risk Estimation



# Step 7: Risk Evaluation Using Risk Diagrams

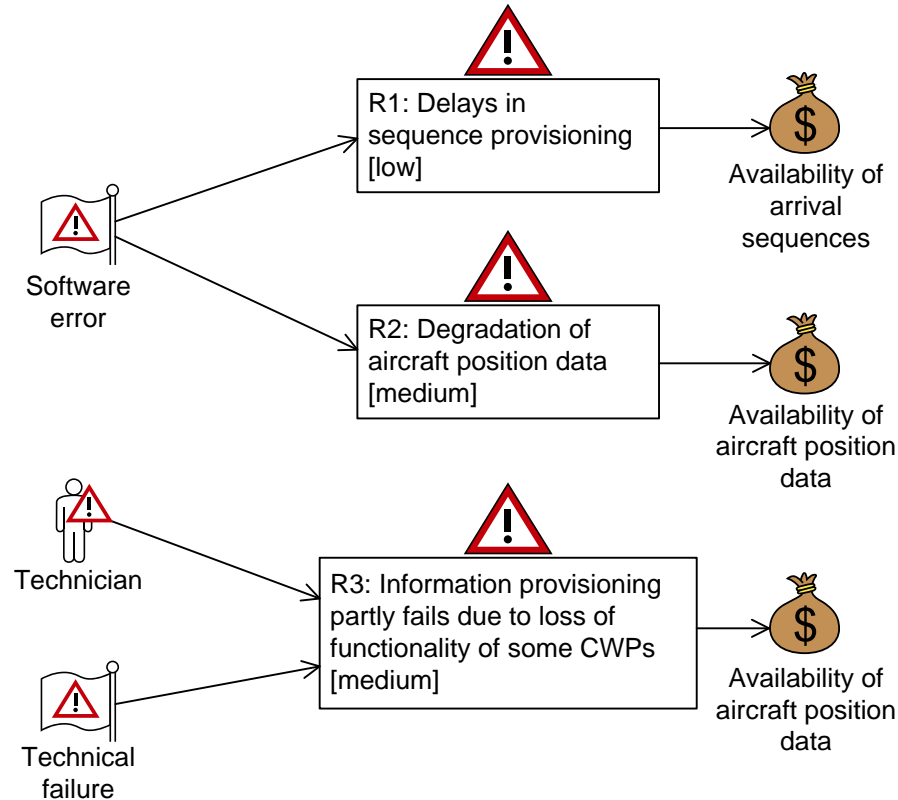
- Objective
  - Determine which risks are unacceptable and must be evaluated for treatment
- Off-line activity
  - Calculate risk levels from estimates
  - Present risks in risk diagrams
- Assess potential impact of identified risk
  - Risks that accumulate
  - Risks with respect to indirect assets

# ATM Example: Indirect Assets

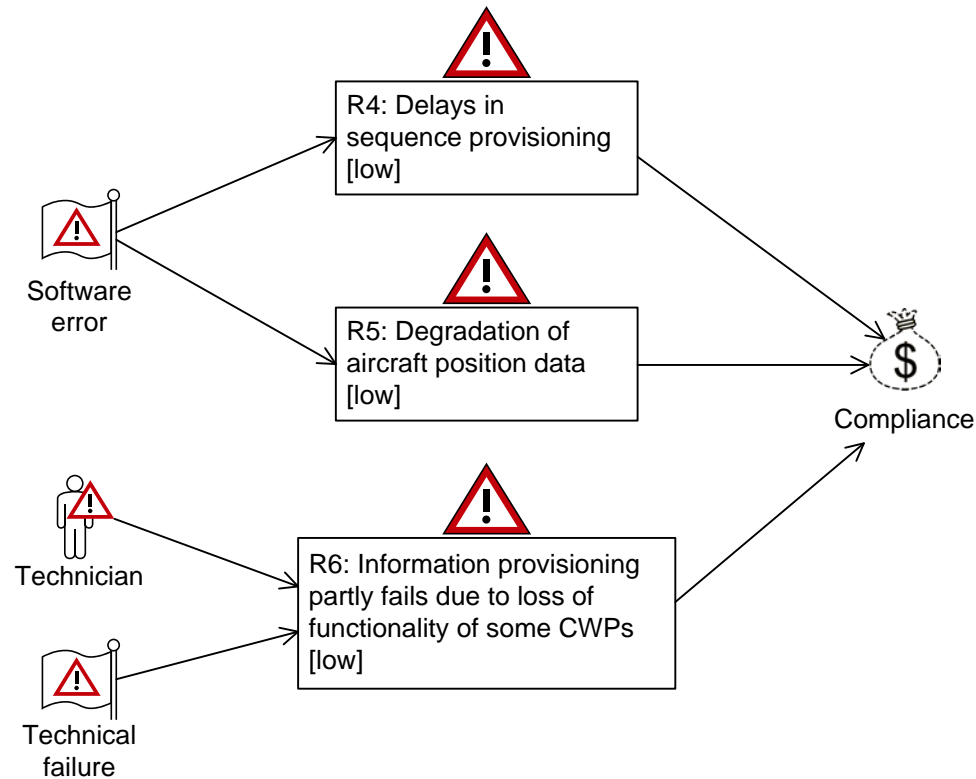




# ATM Example: Risk Diagrams



# ATM Example: Risk Diagrams



# ATM Example: Risk Evaluation

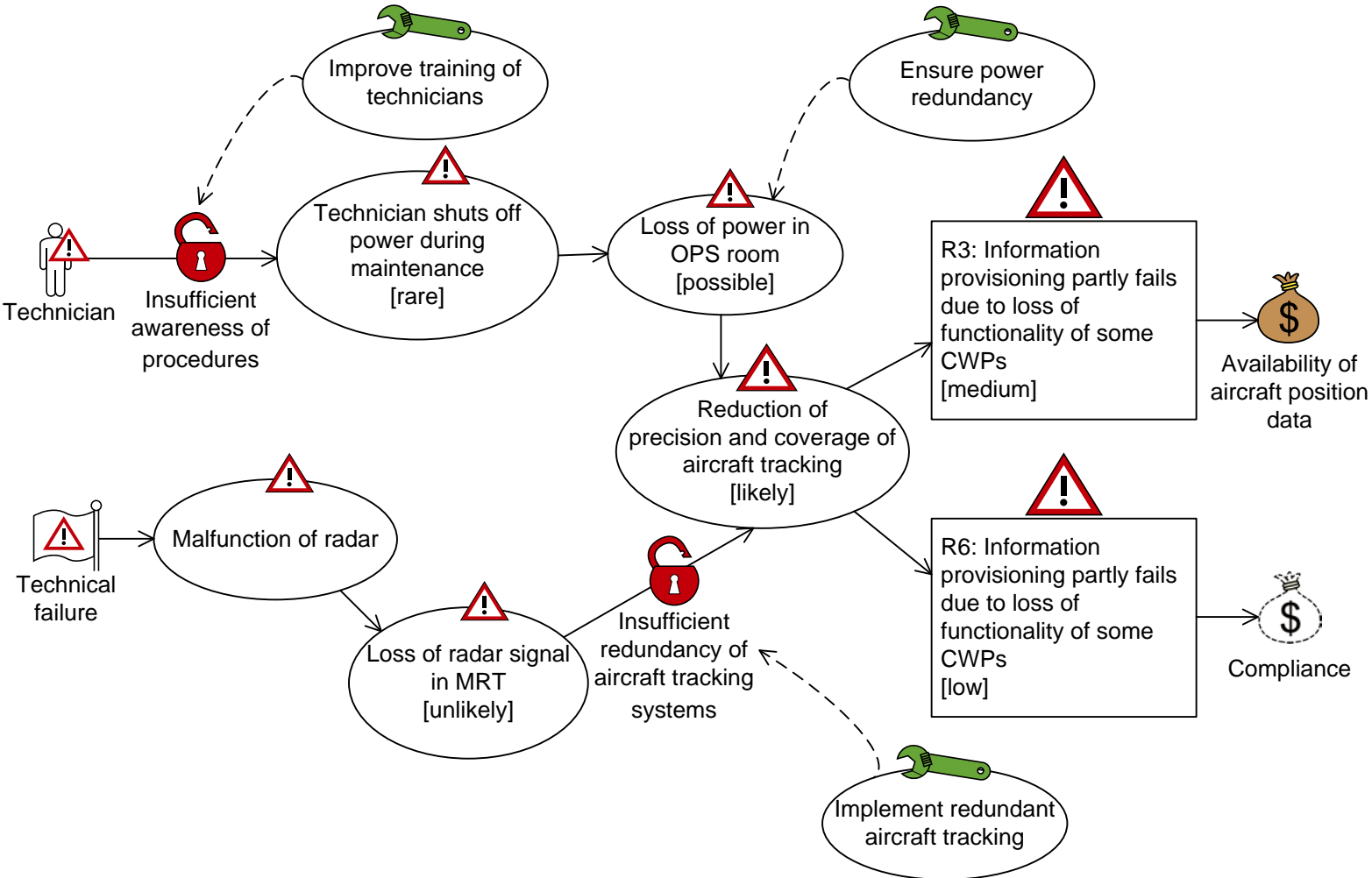
		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Rare					
	Unlikely		R5	R2		
	Possible	R4	R1, R6	R3		
	Likely					
	Certain					

- 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

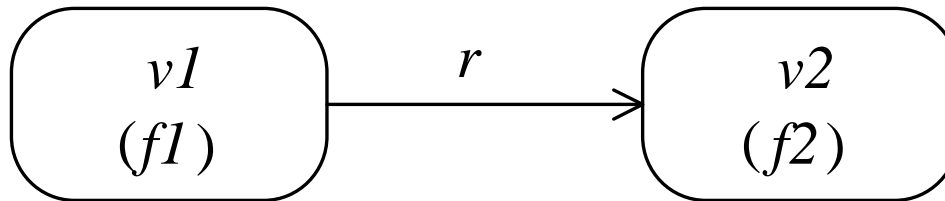
- Objective
  - Identify cost effective treatments for unacceptable risks
- Workshop with brainstorming session
  - Involving people of different background
  - Walk-through of threat diagrams
  - Identify treatments to unacceptable risks

# ATM Example: Treatment Diagram



# Frequency calculation

# CORAS leads-to relation



*vertex  $v1$*  is either a threat scenario or an unwanted incident

*vertex  $v2$*  is either a threat scenario or an unwanted incident

$f1, f2$  are frequencies

$r$  is a conditional ratio

Given  $f1$  and  $r$ , what do we know about  $f2$ ?

# Frequency of vertex

$$v(f)$$

the vertex  $v$  occurs with frequency  $f$



# Conditional ratio of relation

$$v \xrightarrow{r} v'$$

an occurrence of vertex  $v$  will lead to  
an occurrence of vertex  $v'$  with  
conditional ratio  $r$

# Occurrences due to

$$v_1 \sqsupseteq v_2$$

the vertex representing  
occurrences of vertex  $v_2$  that are  
due to an occurrence of vertex  $v_1$

# Aggregation

$$v_1 \sqcup v_2$$

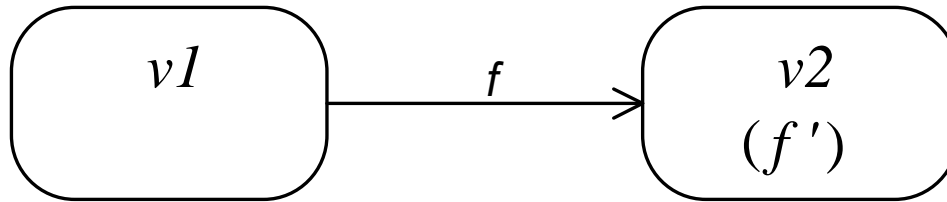
the vertex representing an  
occurrence of vertex  $v_1$  or an  
occurrence of vertex  $v_2$

# Leads-to rule

If  $v_1$  occurs with frequency  $f$  and  $v_1$  leads-to  $v_2$  with conditional ratio  $r$ , then the number of occurrences of  $v_2$  due to  $v_1$  is  $f$  multiplied by  $r$

$$\frac{H \vdash v_1(f) \quad H \vdash v_1 \xrightarrow{r} v_2}{H \vdash v_1 \sqcap v_2(f \cdot r)}$$

# CORAS initiate relation



*vertex v1* is a threat  
*vertex v2* is either a threat scenario or an unwanted incident  
*f, f'* are frequencies

Given *f*, what do we know about *f'* ?

# Initiate rule

If  $v_1$  initiates  $v_2$  with frequency  $f$ , then the number of occurrences of  $v_2$  due to  $v_1$  is  $f$

$$\frac{H \vdash v_1 \xrightarrow{f} v_2}{H \vdash v_1 \sqcap v_2(f)}$$

# Aggregation rule

If

$v_1$  occurs with frequency  $f_1$

$v_2$  occurs with frequency  $f_2$

an occurrence of  $v_1$  cannot be an occurrence of  $v_2$

an occurrence of  $v_2$  cannot be an occurrence of  $v_1$

then

$v_1$  or  $v_2$  occurs with frequency  $f_1+f_2$

$$\frac{H \vdash v_1(f_1) \quad H \vdash v_2(f_2) \quad s(v_1) \cap s(v_2) = \emptyset}{H \vdash v_1 \sqcup v_2(f_1 + f_2)}$$