



# EXAMPLE-DRIVEN INTRODUCTION TO CORAS

Ketil Stølen

# Content

---

- Main concepts
- Process of eight steps
- Risk modeling
- Guided tour

Mass Soldal Lund  
Bjørnar Solhaug  
Ketil Stølen

## Model-Driven Risk Analysis

The CORAS Approach

 Springer

# Other Literature

---

- Kristian Beckers, Maritta Heisel, Bjørnar Solhaug, Ketil Stølen. ISMS-CORAS: A structured method for establishing an ISO 27001 compliant information security management system.

<http://heim.ifi.uio.no/~ketils/kst/Articles/2014.NESSOS-ISMS-CORAS.pdf>

- Bjørnar Solhaug, Ketil Stølen. The CORAS Language – Why it is designed the way it is.

<http://heim.ifi.uio.no/~ketils/kst/Articles/2013.ICOSSAR.pdf>

- Mass Soldal Lund, Bjørnar Solhaug, Ketil Stølen. Risk analysis of changing and evolving systems using CORAS.

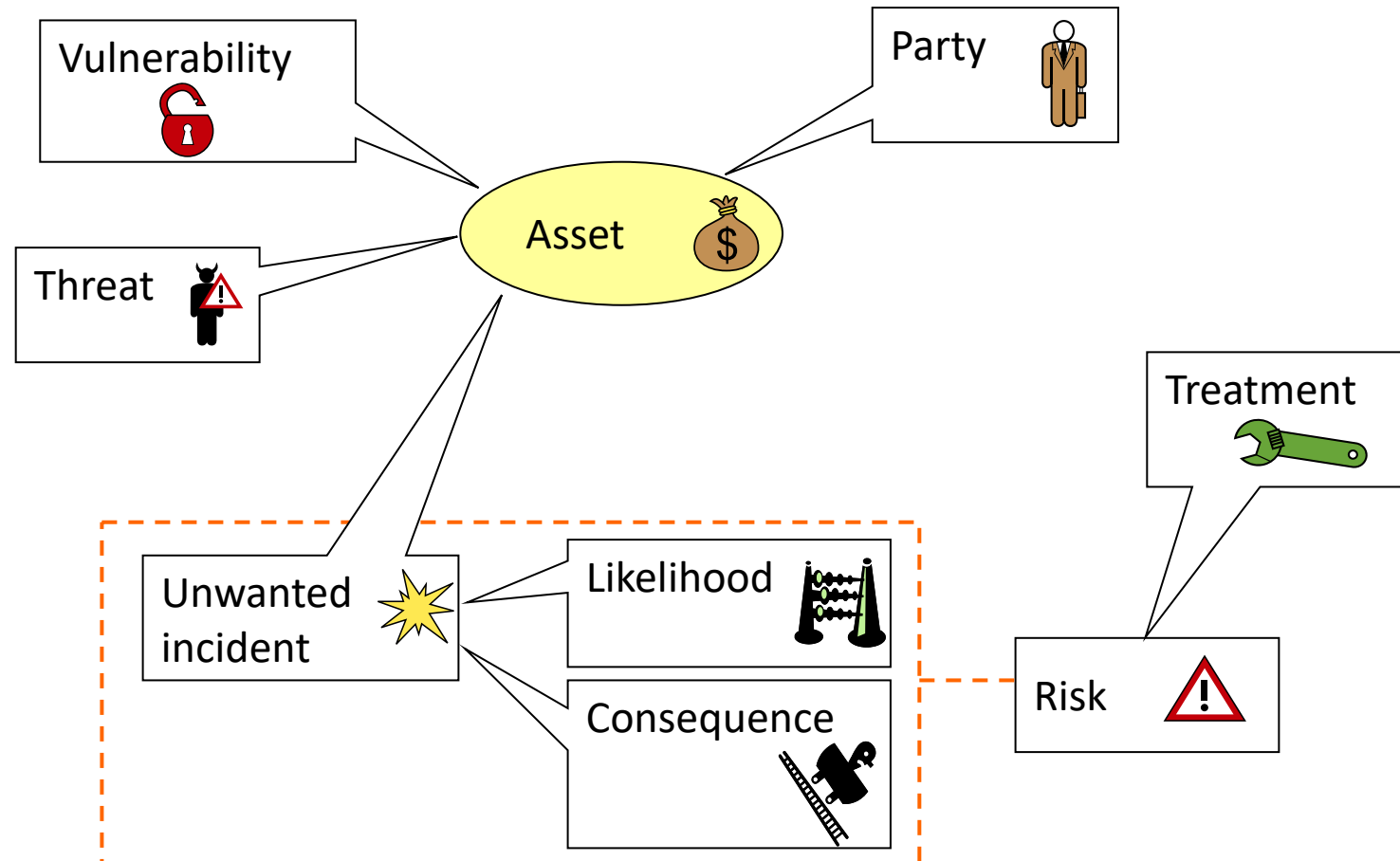
<http://heim.ifi.uio.no/~ketils/kst/Articles/2011.FOSAD.pdf>

# The CORAS Method

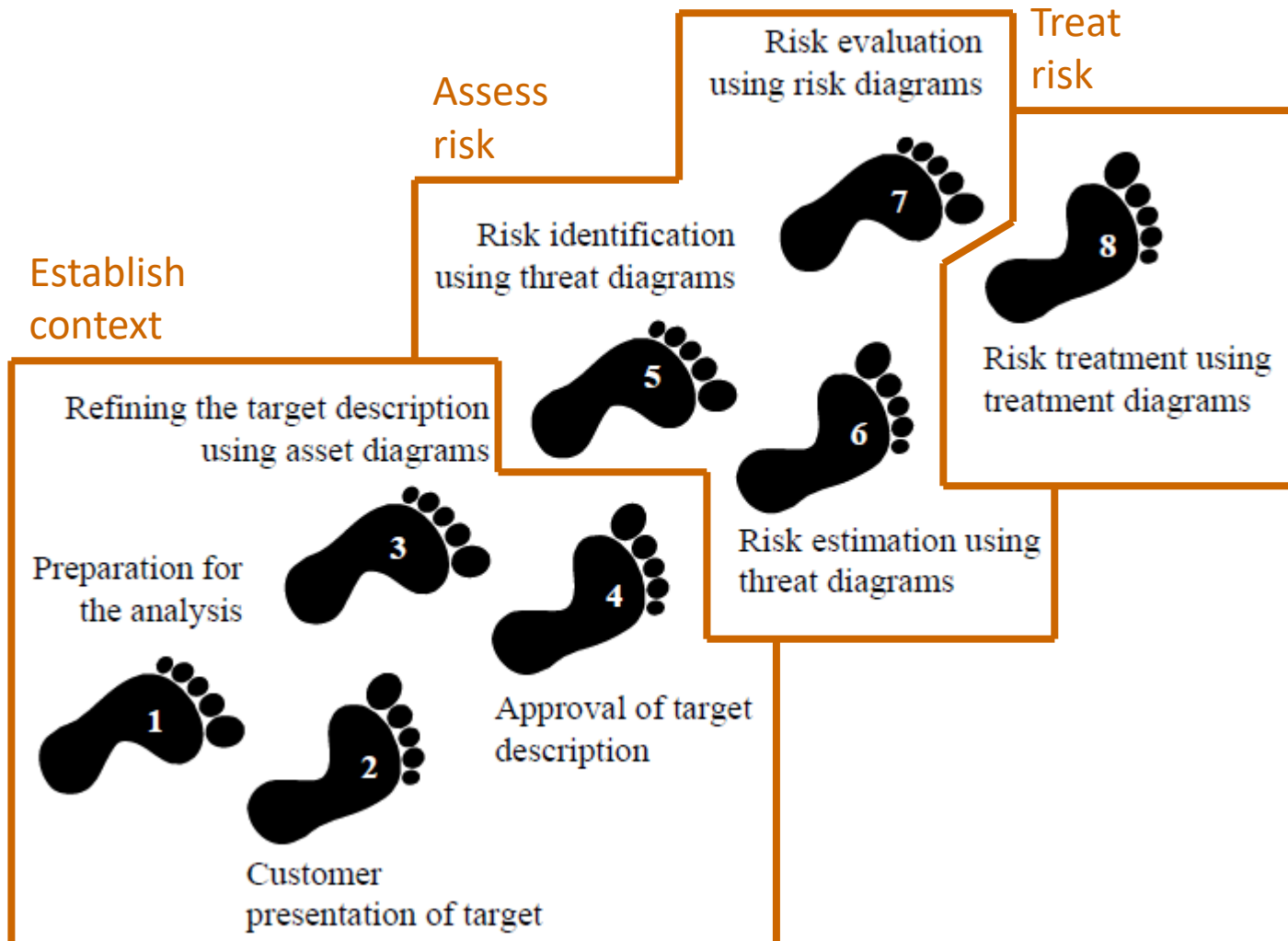
---

- Asset-driven defensive risk analysis method
- Operationalization of ISO 31000 and ISO 27005 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

# Main Concepts



# The 8 Steps of the CORAS Method



# Risk Modeling

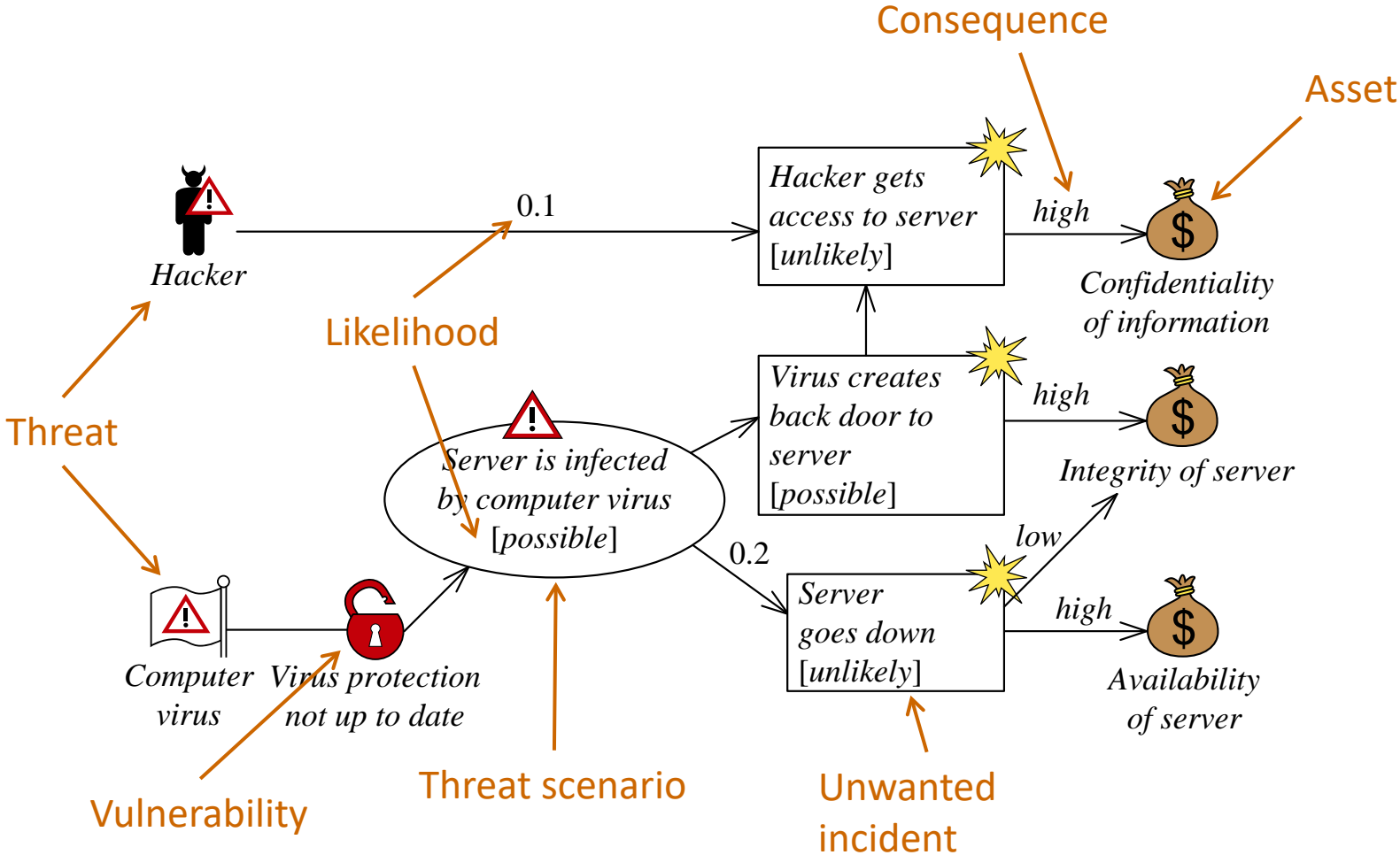
---

The CORAS language consists of five kinds of diagrams

- Asset diagrams
- Threat diagrams
- Risk diagrams
- Treatment diagrams
- Treatment overview diagrams

Each kind supports concrete steps in the risk analysis process

# CORAS Example: Threat Diagram





# Example Case

---

- Customer is a national air navigation service provider
- The customer decides on an assessment of 250 person-hours on behalf of the external assessment team
- Focus should be on the role of the Air Traffic Controllers (ATCOs) in the process of arrival management
- Main concerns
  - 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 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

# Step 2: Customer presentation of target

---

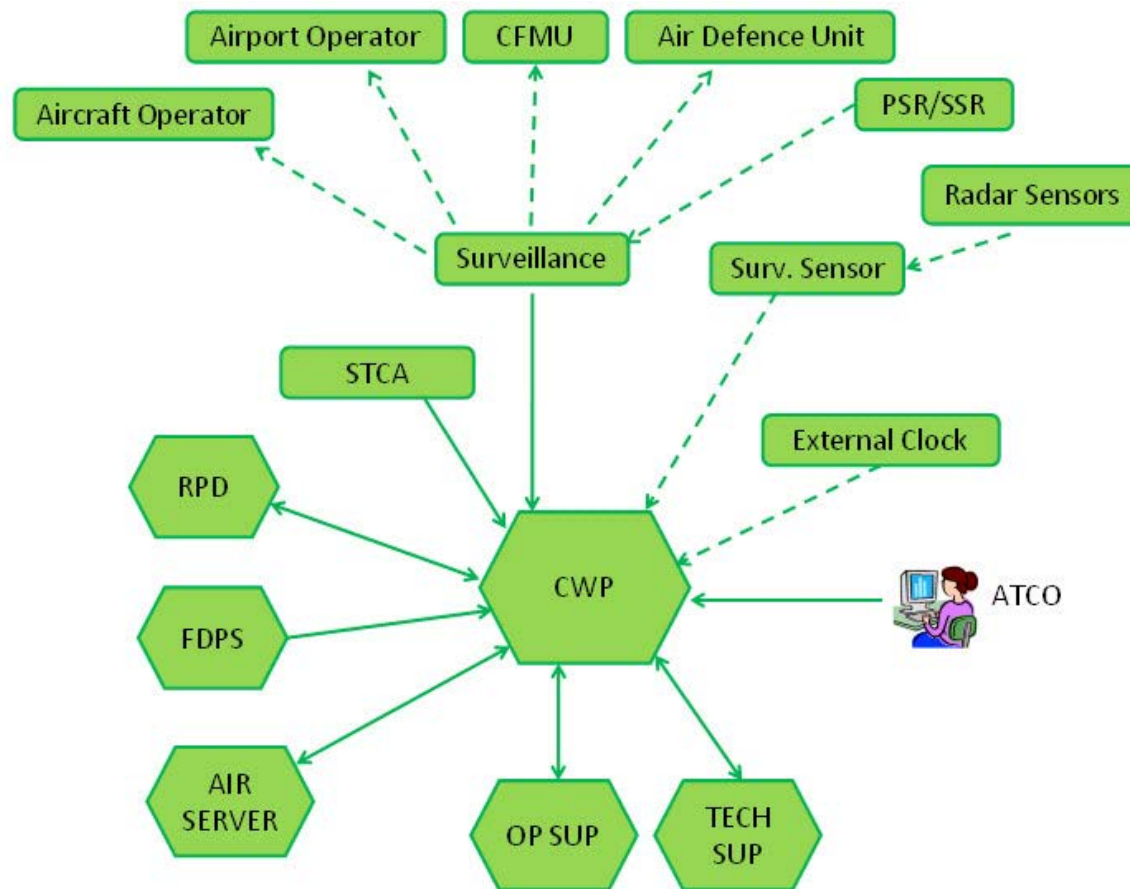
## Objectives

- 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

# Typical documentation provided by customer



Problem:

- Difficult to comprehend
- No clear semantics

# Step 3: Refine target description using asset diagrams

---

## Objectives

- Ensure common understanding of target including scope, focus and assets

## Face-to-face meeting

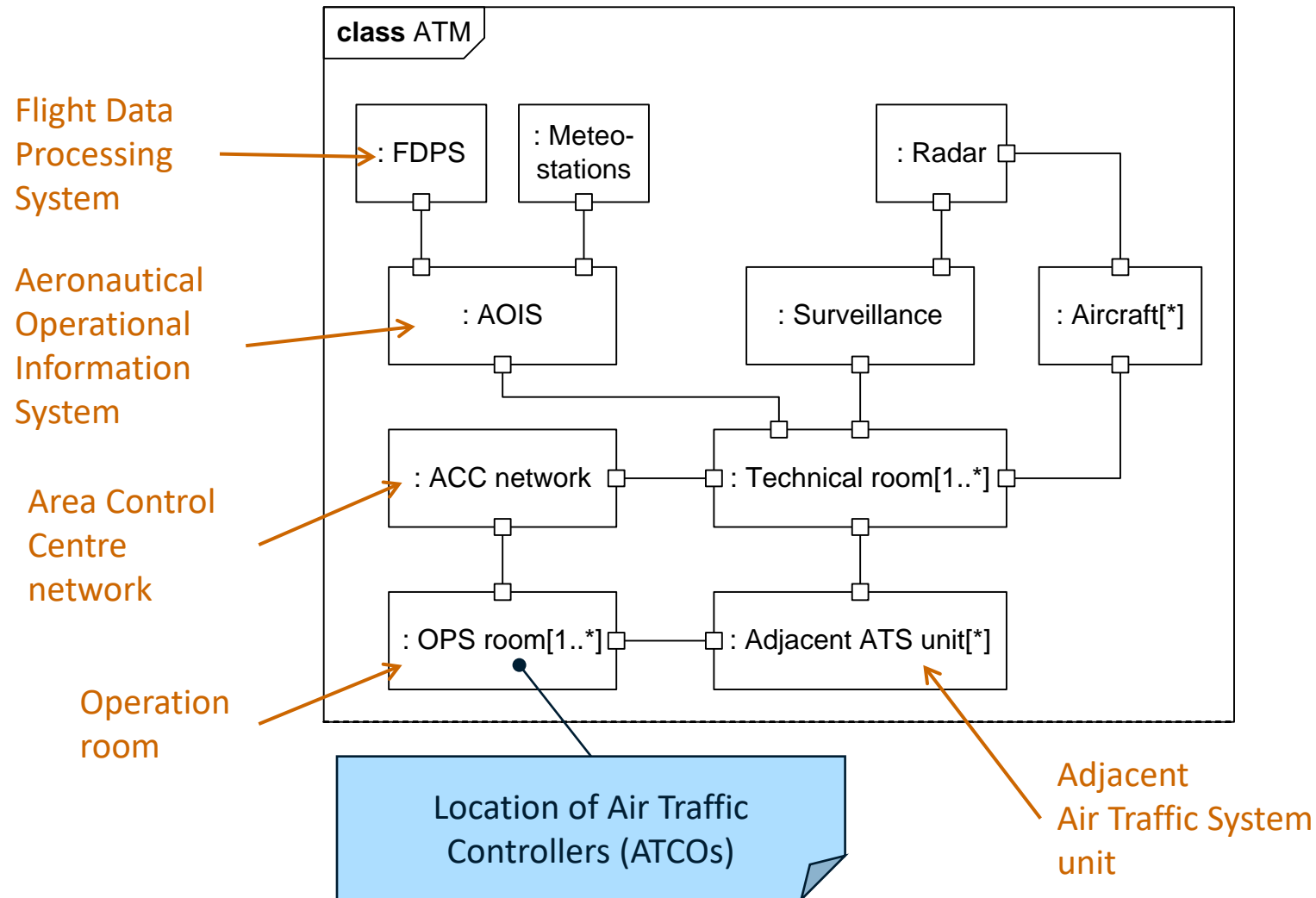
- Assessment team presents their understanding of the target
- Assets are identified
- High-level assessment

# Target description made by external assessment team

---

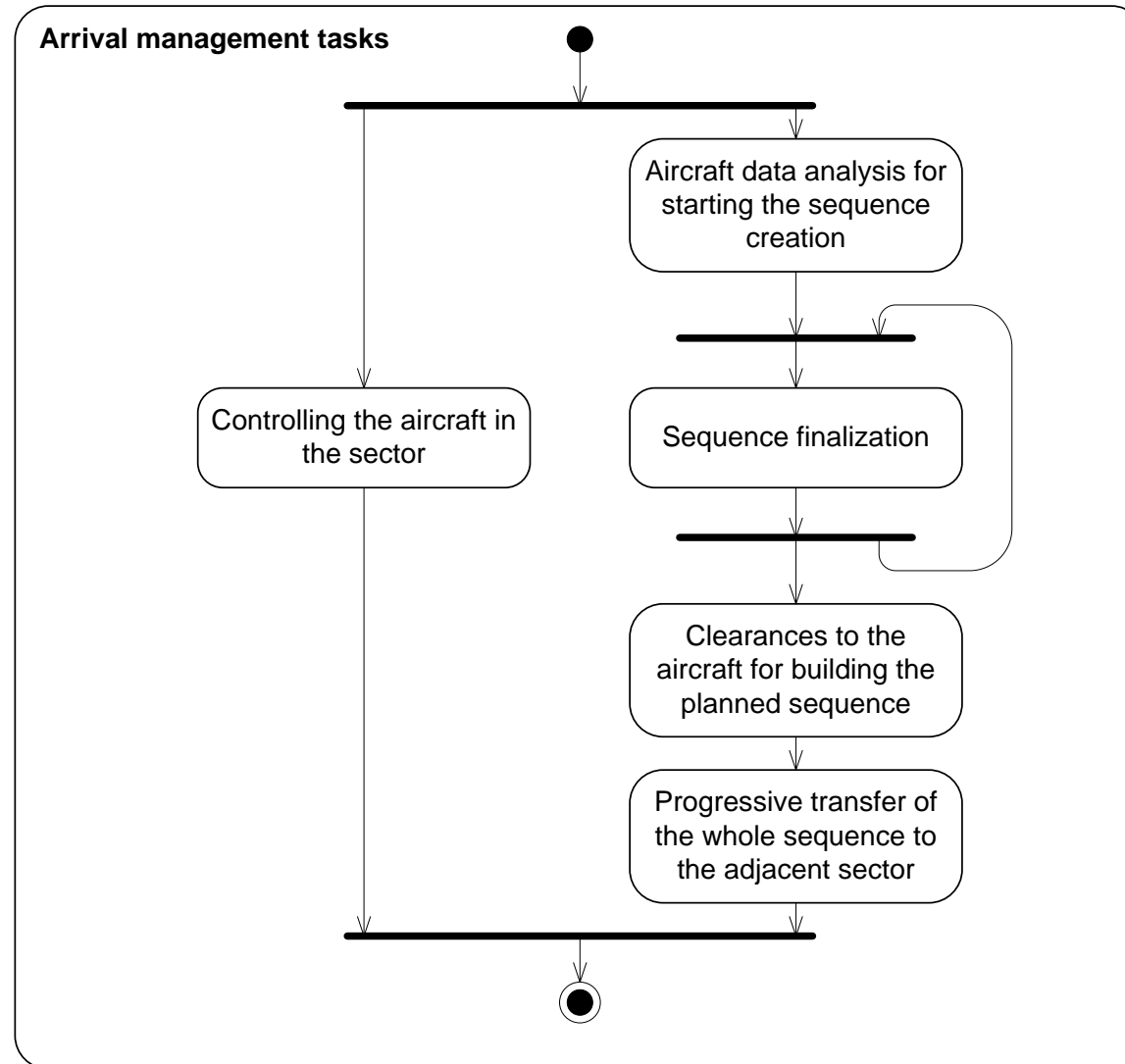
- Conceptual overview specified in UML class diagrams
- Activities specified using UML internal structure and activity diagrams

# Example of Internal Structure Diagram



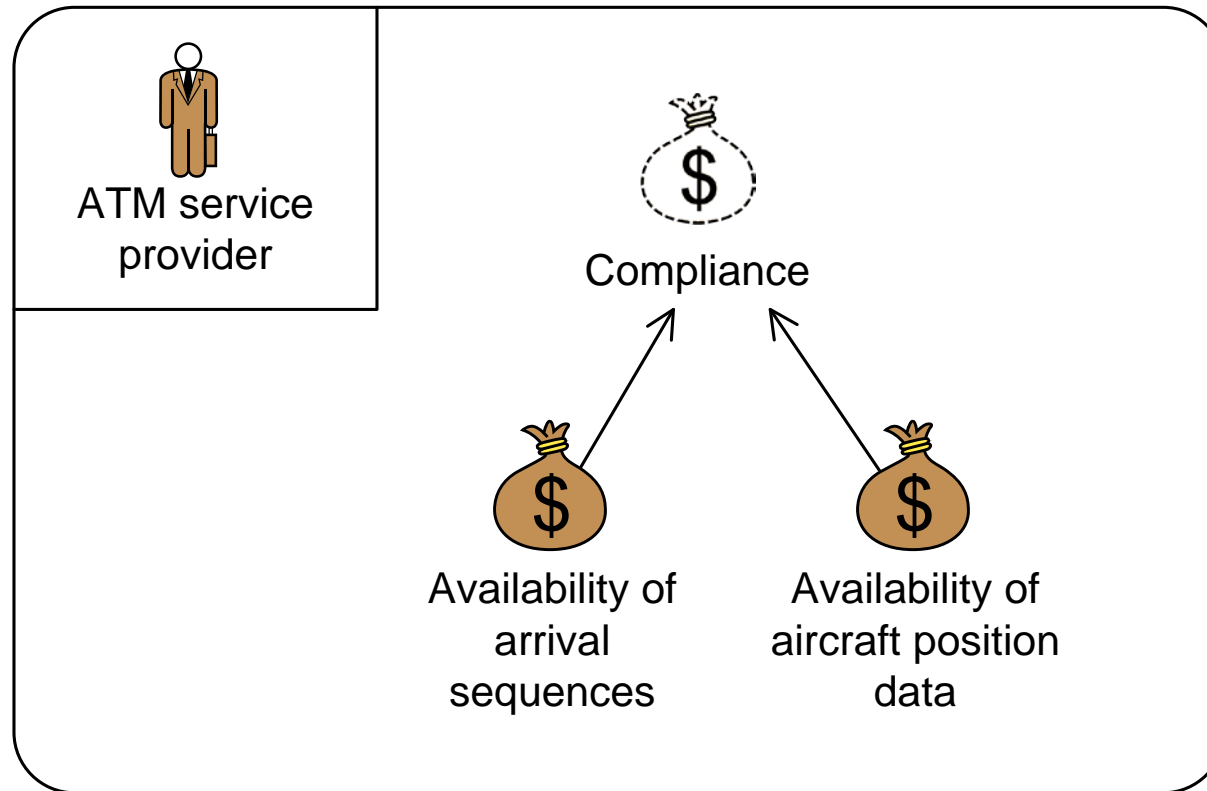


# Example of Activity Diagram



# Asset Identification Using Asset Diagrams

- Assets are the values the party of the assessment wants to protect






# High-level assessment

---

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

# Results from High-level Assessment

		
<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

---

## Objectives

- 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

# Qualitative 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



# Qualitative 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

# Risk Evaluation Criteria

---

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Rare	Low	Low	Medium	High	Critical
	Unlikely	Low	Low	Medium	High	Critical
	Possible	Low	Low	Medium	High	Critical
	Likely	Low	Medium	High	Critical	Critical
	Certain	Low	Medium	High	Critical	Critical

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



**CYBERWISER.eu**

Cyber Range & Capacity Building in Cybersecurity