Part III: Change Management

Bjørnar Solhaug

SECURWARE 2011-08-21

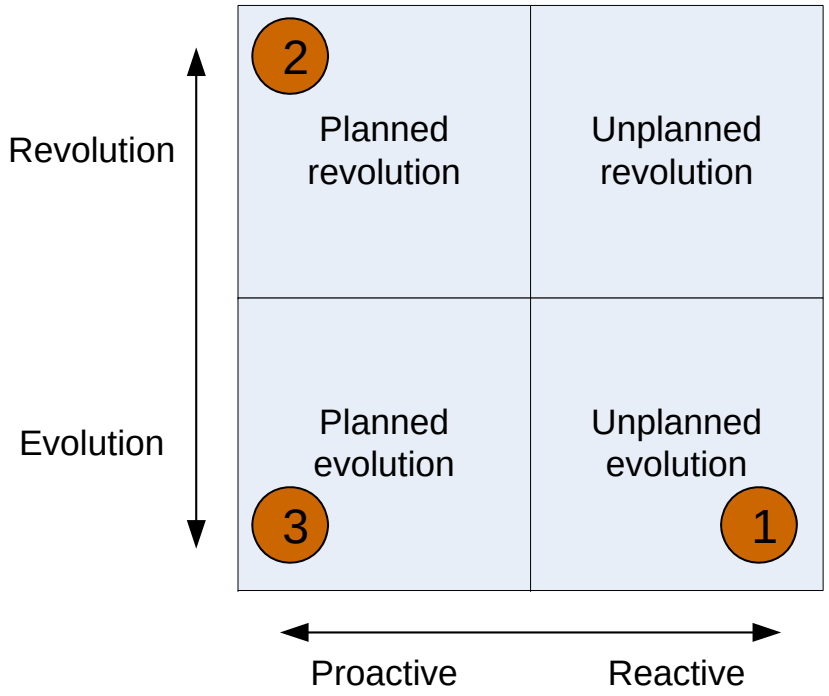
Overview of Part III

- Changing and evolving risk
- Three perspectives on change
- Formal foundation
- Risk graphs
- Risk graphs with change
- CORAS instantiation
- Practical example
- Summary

Changing and Evolving Risk

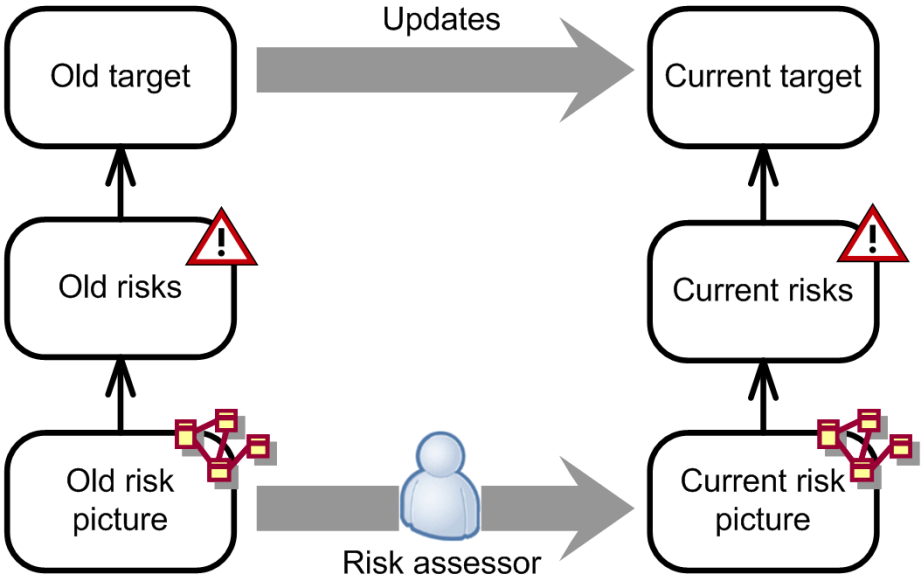
- Many risk assessments build on unrealistic assumptions
  - Particular configuration of the target
  - Particular point in time
  - Valid under the assumptions of the target description
- Reality change and evolve
  - The target and the environment change and evolve over time
  - The assumptions, context, scope, focus, assets and parties may change and evolve over time
  - As a result, risks change and evolve over time
  - Change and evolvement must be reflected in the risk picture

Three Perspectives on Change



1: The maintenance perspective
2: The before-after perspective
3: The continuous evolution perspective

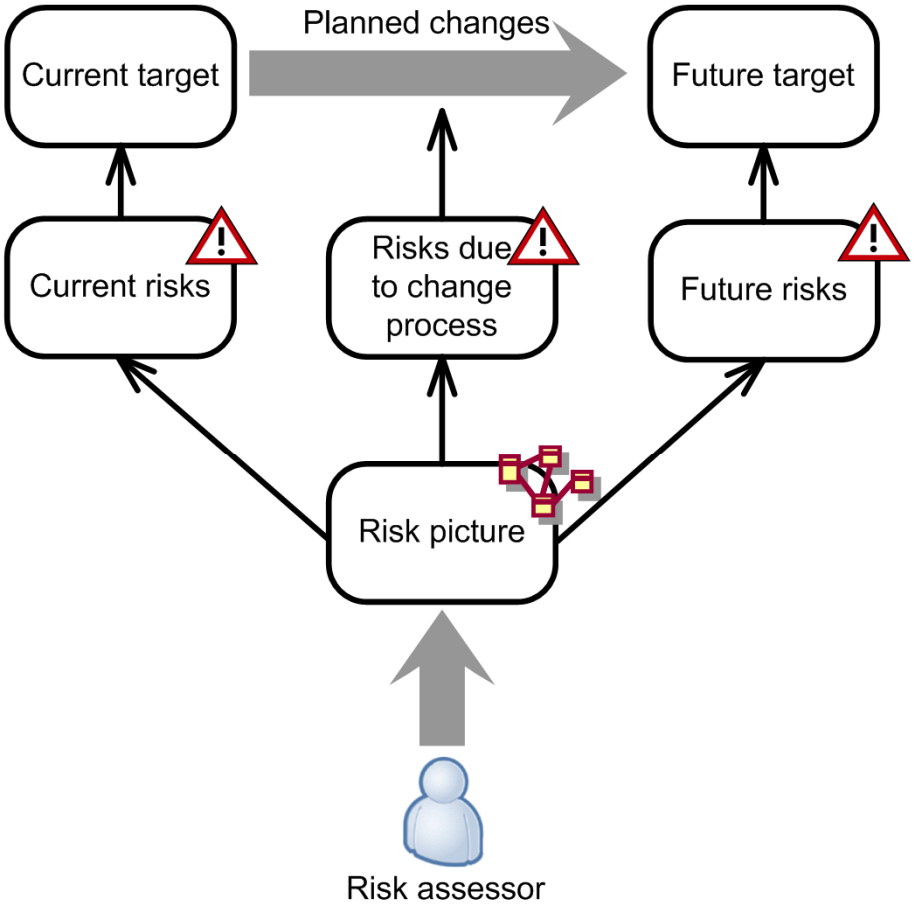
Maintenance Perspective



Methodological challenges

- Reuse the old risk assessment results
- Avoid having to start from scratch
- Requires
  - Identifying the updates made to the target and update the target description accordingly
  - Identifying which risks and parts of the risk picture/risk model are affected by the updates
  - Updating the risk picture/risk model without having to do changes in the unaffected parts

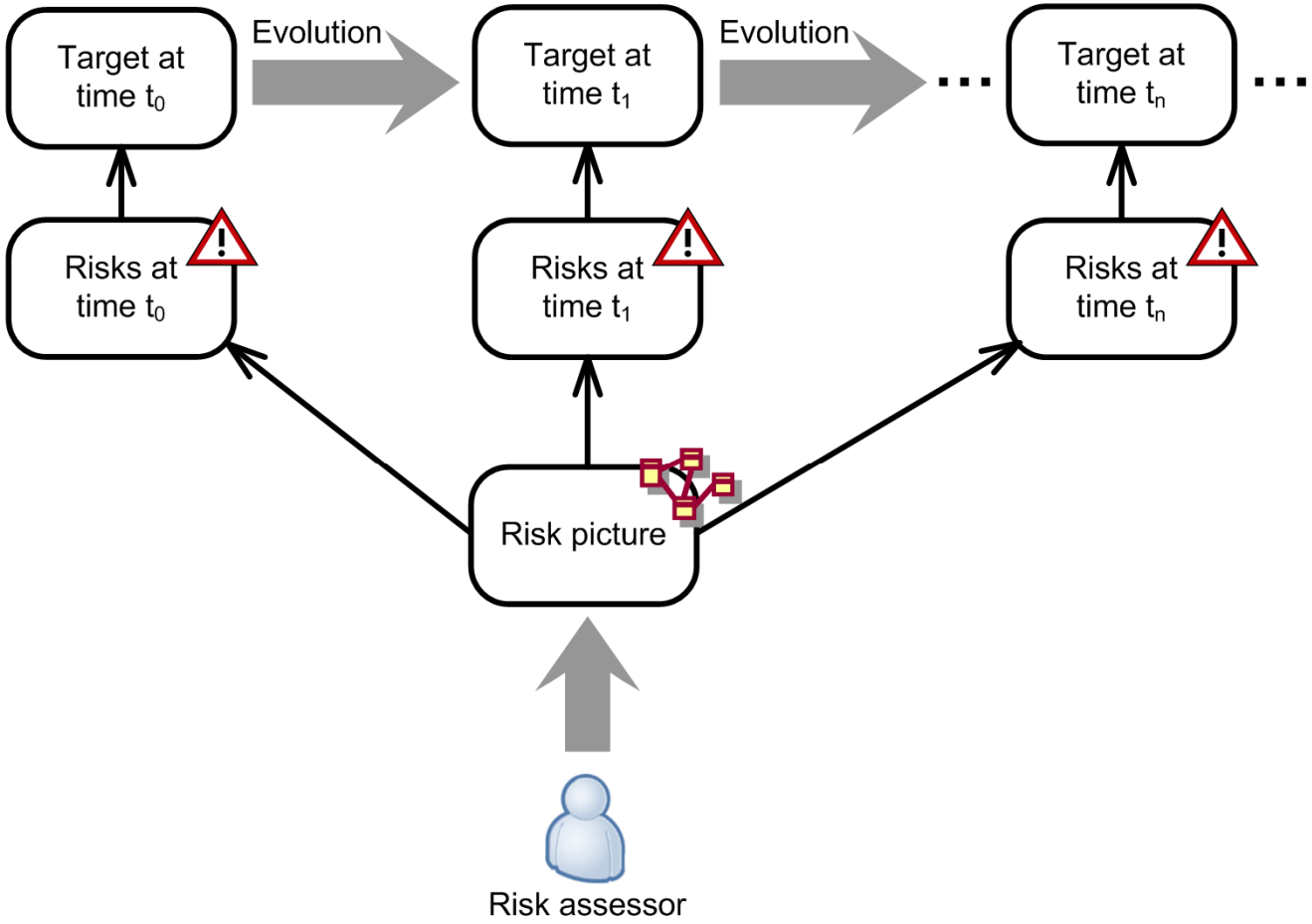
Before-After Perspective



Methodological Challenges

- Obtain and present a risk picture for the current risks, the future risks, and the risks to the change
- Requires:
  - A target description that characterizes the target “as-is” and the target “to-be“
  - A description of the process of change
  - Identifying current and future risk without doing double work
  - Identifying risks to the change process
  - Providing a risk picture that characterizes current risks, future risks and risks to the change process, and that relates these to the target description

Continuous Evolution Perspective



Continuous Evolution Perspective

Methodological challenges

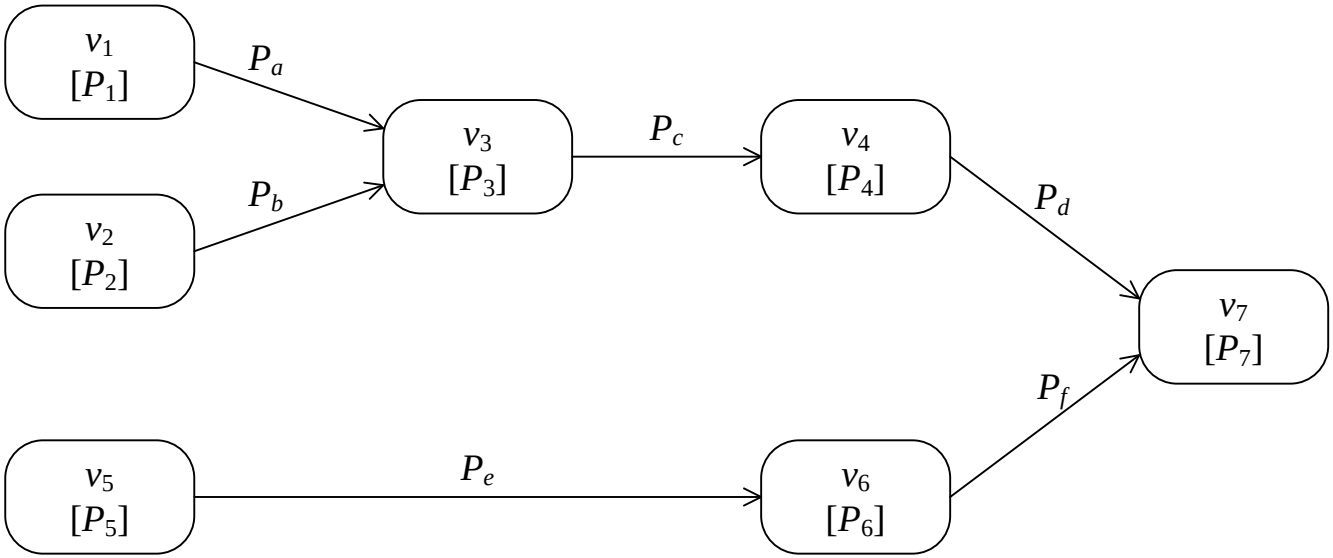
- Identify and present evolving risks in a dynamic risk picture/risk model
- Requires:
  - Generalizing a target description in such a way that it characterizes evolution of the target and its environment
  - Identifying and generalizing the risks affected by evolution in the target or its environment
  - Characterizing the evolution of risks and presenting it in a dynamic risk picture/risk model
  - Relating the evolution of risks described by the risk picture/risk model to the evolution of the target described in the target description

Formal Foundation

Risk Modeling

- **Risk analysis** involves the process of understanding the nature of risks and determining the risk level
- **Risk modeling** refers to techniques for risk identification, documentation and estimation
- A **risk model** is a structured way of representing unwanted incidents and its causes and consequences by means of graphs, trees or block diagrams
- **Risk graphs** are an aid for
  - structuring events and scenarios leading to incidents
  - estimating likelihoods of incidents

Risk Graph

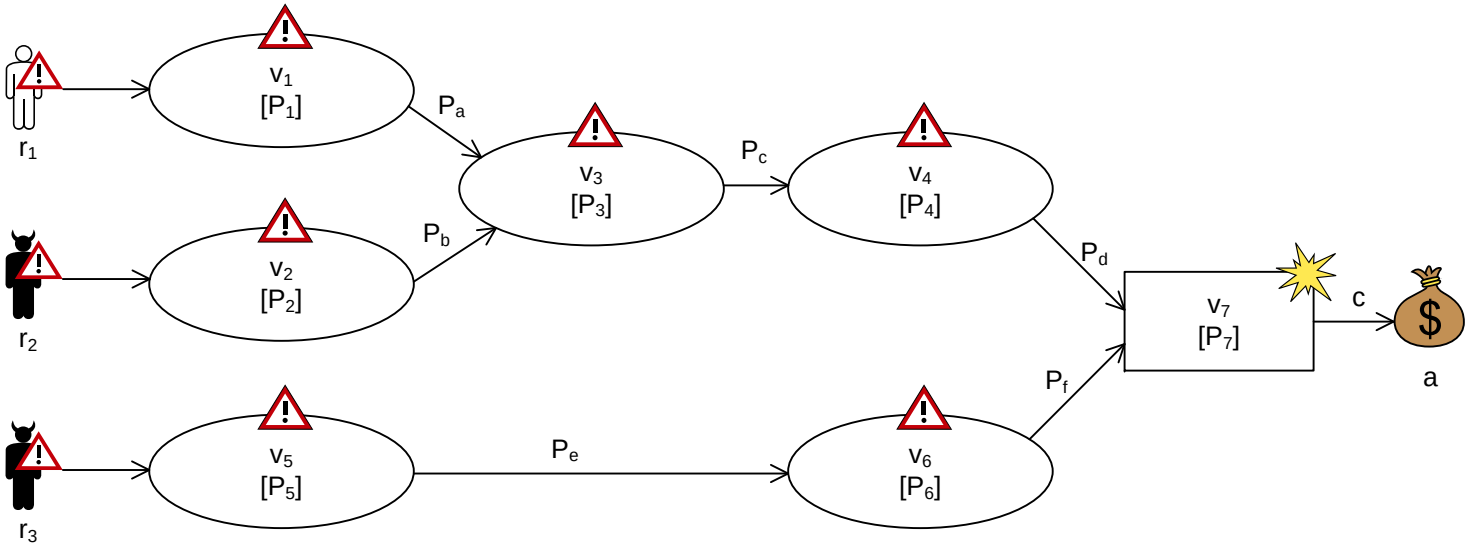


- Risk graphs can be understood as a common abstraction of several established risk modeling techniques
  - Fault trees, attack trees, cause-consequence diagrams, Bayesian networks, CORAS threat diagrams

Formalization of Risk Graphs

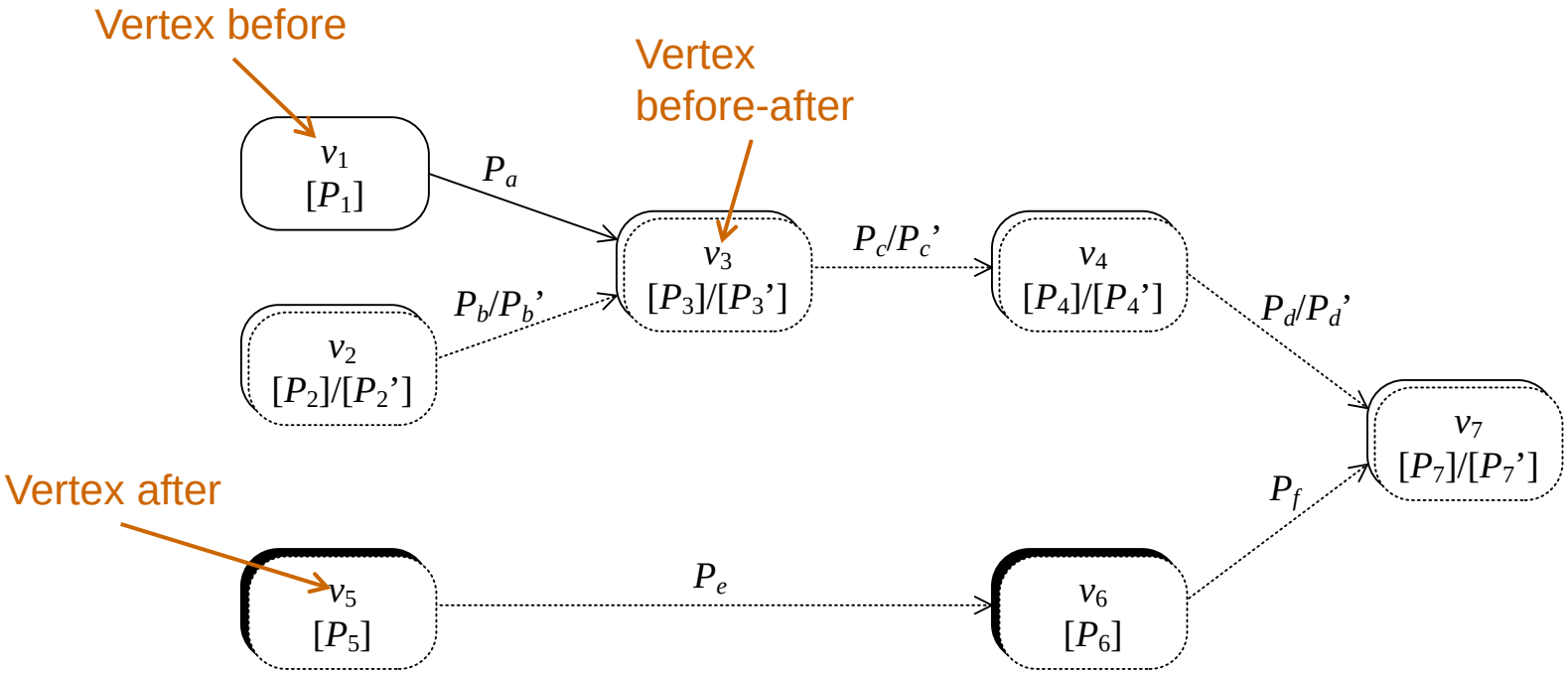
- Syntax
  - A risk graph is a set *D* of elements *e*
  - An element is a vertex *v* or a relation $v_1 \rightarrow v_2$
  - A probability set $P \subseteq [0,1]$ is assigned to the elements
- Semantics
  - Scenarios and probabilities are represented by a probability space on traces of events
- Calculus
  - Rules for reasoning about risk graphs
  - Soundness proofs with respect to the semantics

CORAS Instantiation



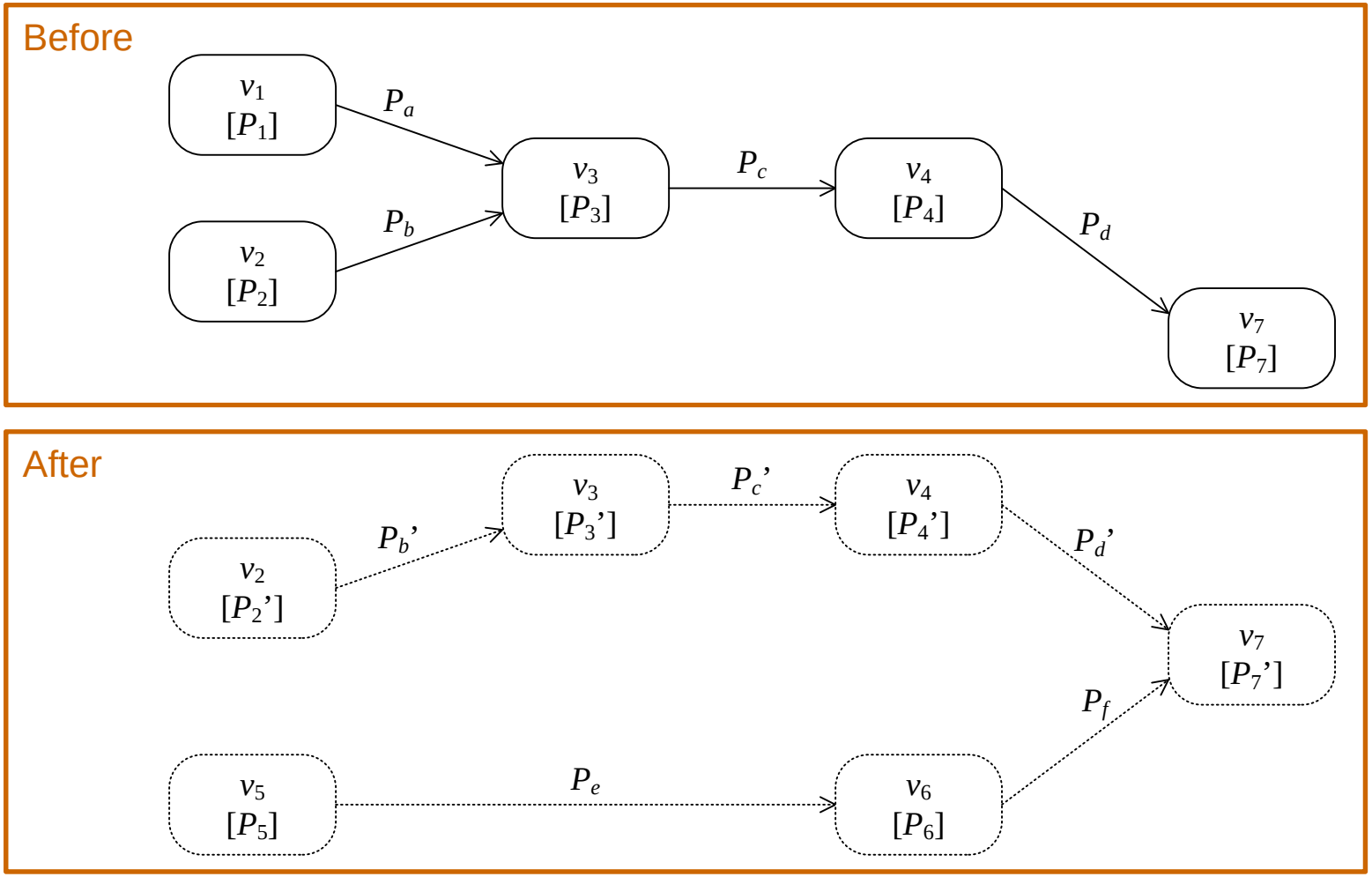
- CORAS vertices and relations can be interpreted in terms of risk graph vertices and relations
- The risk graph semantics and calculi carries over to CORAS

Risk Graphs with Change

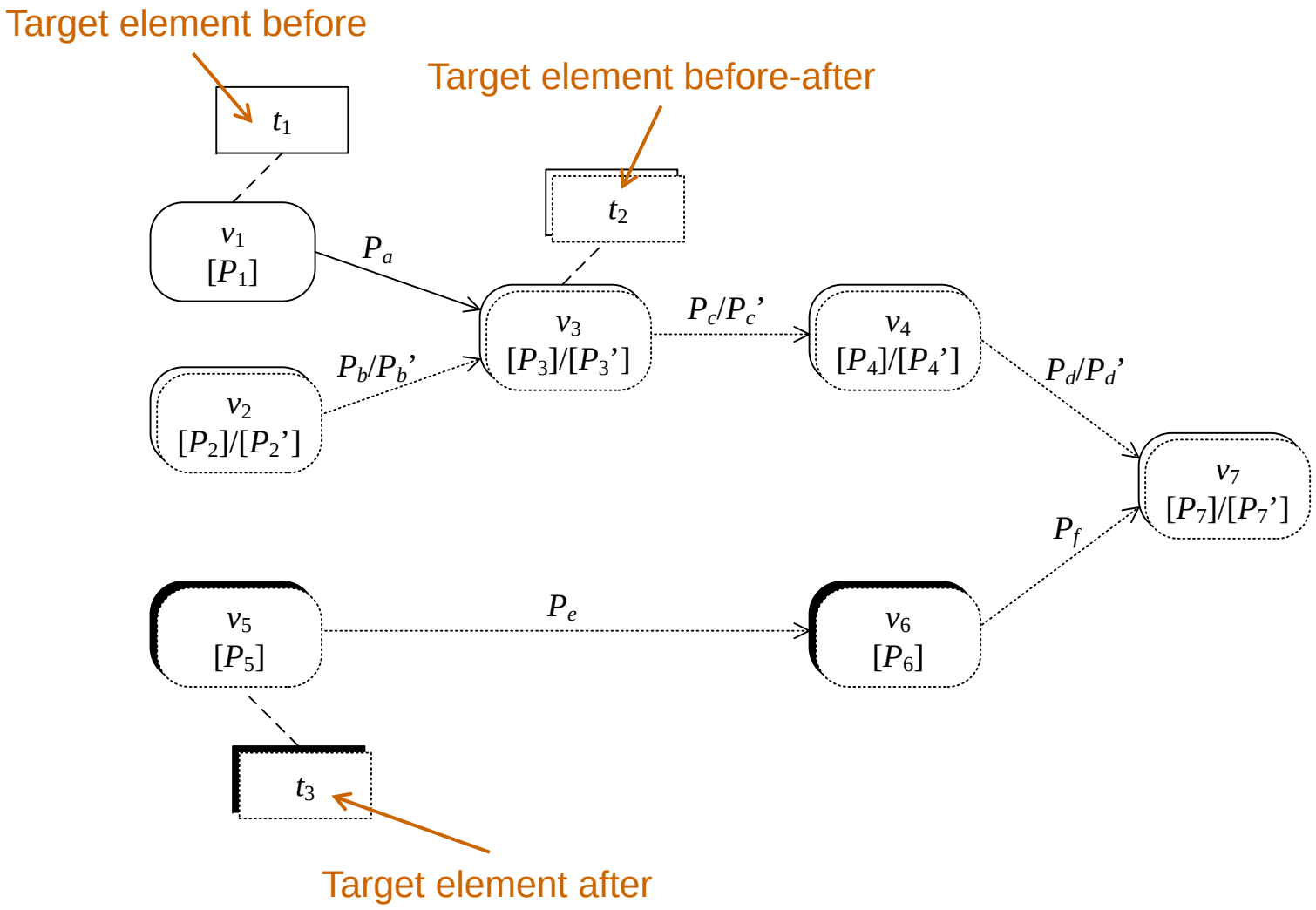


- Explicit modeling of
  - Elements before change
  - Elements after change
  - Changes in likelihood estimates

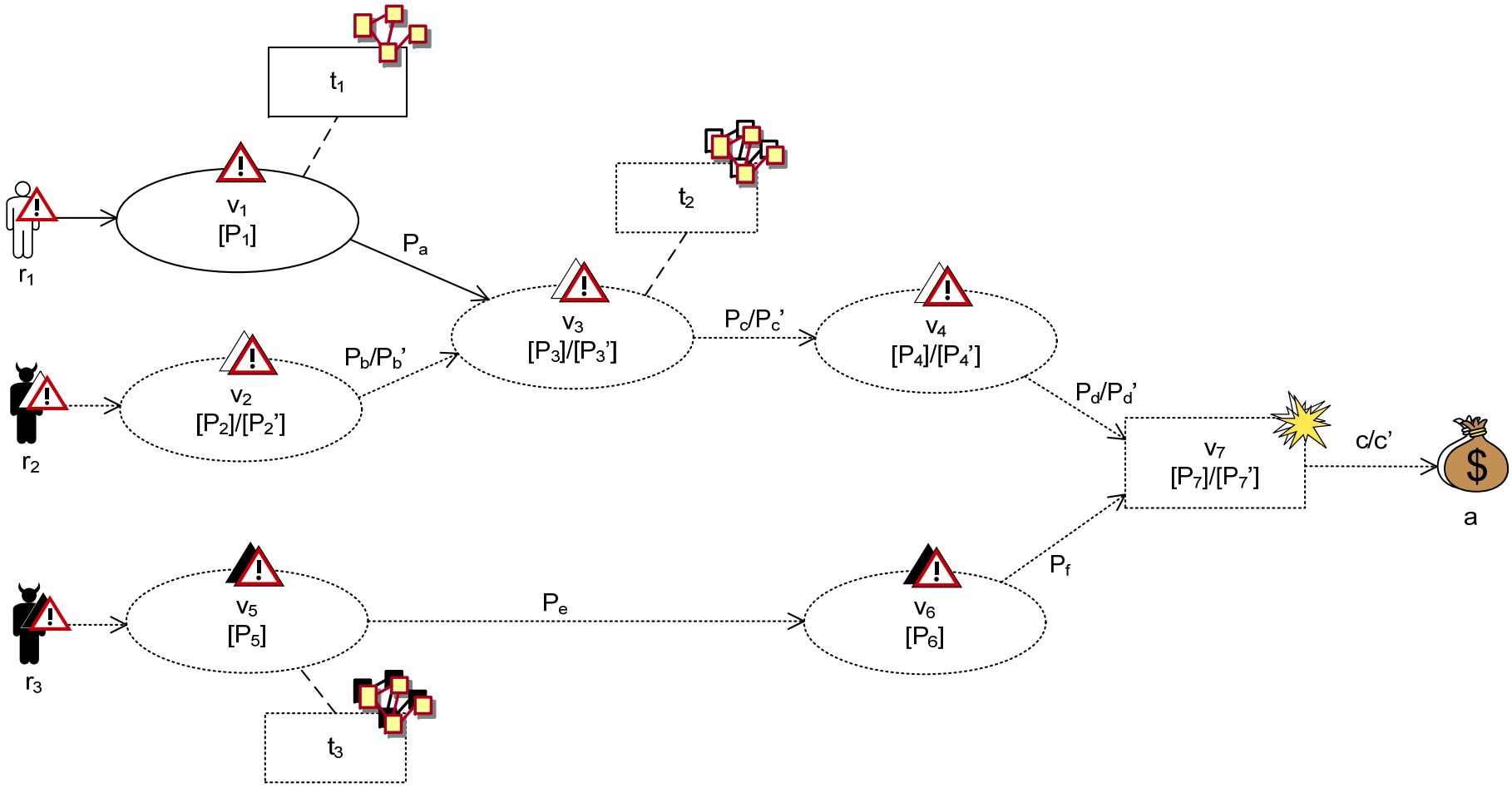
Two Views on Risk Graphs with Change



Trace Model


Target element before
Target element before-after
t_1
t_2
v_1
$[P_1]$
P_a
v_3
$[P_3]/[P_3']$
P_c/P_c'
v_4
$[P_4]/[P_4']$
P_d/P_d'
v_2
$[P_2]/[P_2']$
P_b/P_b'
v_7
$[P_7]/[P_7']$
P_f
v_5
$[P_5]$
P_e
v_6
$[P_6]$
t_3
Target element after

CORAS Instantiation



Practical Example: ATM

Process of Eight Steps

1. Preparations for the analysis 2. Customer presentation of the target 3. Refining the target description using asset diagrams 4. Approval of the target description	Establish context
5. Risk identification using threat diagrams 6. Risk estimation using threat diagrams 7. Risk evaluation using risk diagrams	Assess risk
8. Risk treatment using treatment diagrams	Treat risk

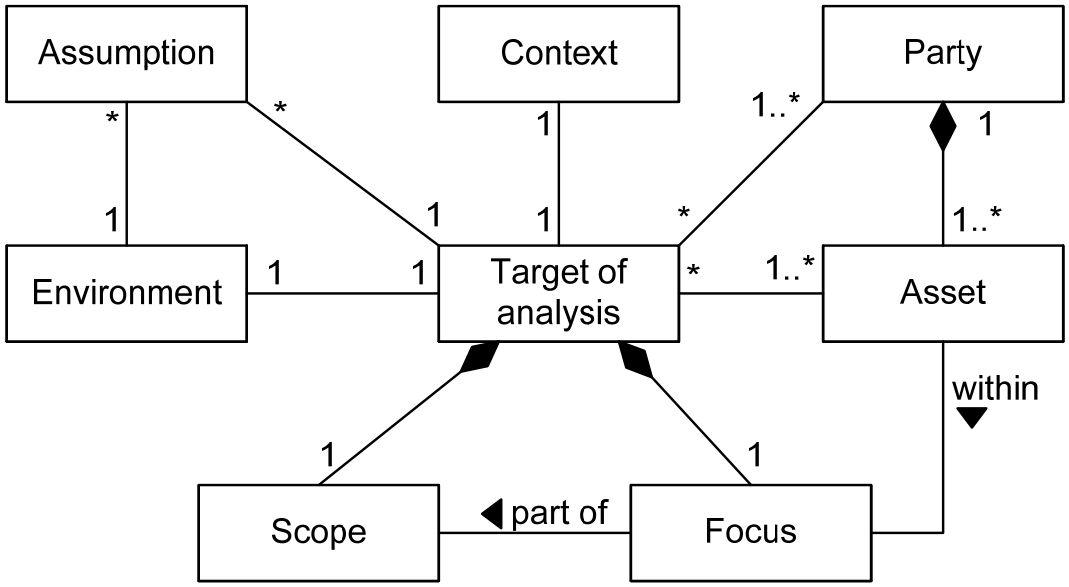
Need to address change in all steps

Establish Context

CORAS Steps 1-4

Establish Context

- Make a description of target as-is and target to-be
- Identify and document changes regarding target of analysis and risk evaluation criteria



Changes

- Current characteristic of ATM
  - Limited interaction with external world
    - Limited security problems in relation to information flow to and from the environment
  - Humans at the centre
    - Limited role of automated decision support systems and tools
- Changes in European ATM
  - Introduction of new information systems and decision support systems
  - Reorganization of services

Target of Analysis

- Arrival management and the role of air traffic controllers (ATCOs) in the area control centre (ACC)
- The introduction of AMAN and ADS-B
  - Arrival manager (AMAN) is a decision support tool for the automation of ATCO tasks in the arrival management
  - Automatic Dependent Surveillance-Broadcast (ADS-B) is a cooperative GPS-based surveillance technique where aircrafts constantly broadcast their position to the ground and to other aircrafts

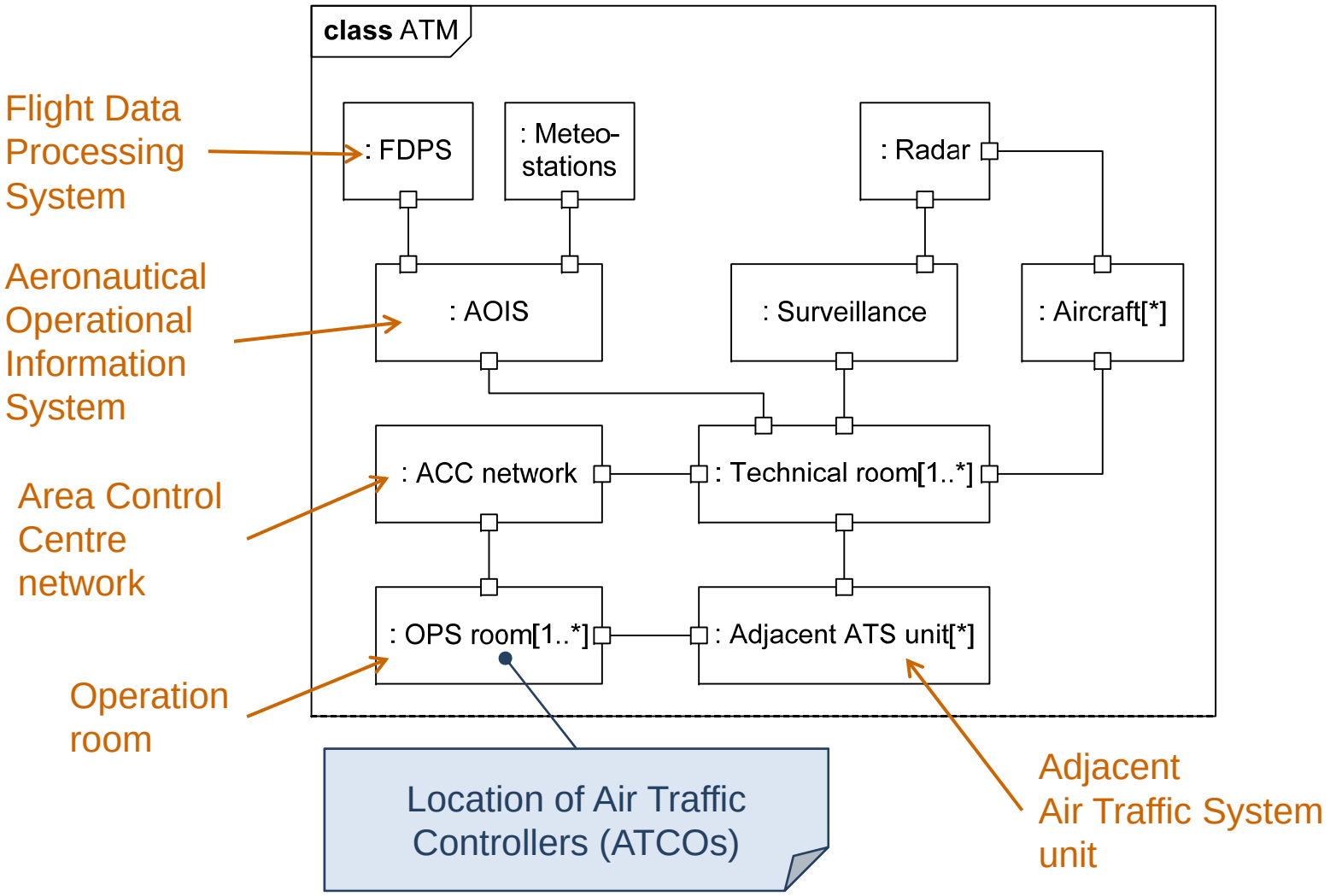
Focus of Analysis

- Before changes:
  - Information provision (availability)
  - Compliance with regulation
- Additional concerns after changes:
  - Information protection (confidentiality)

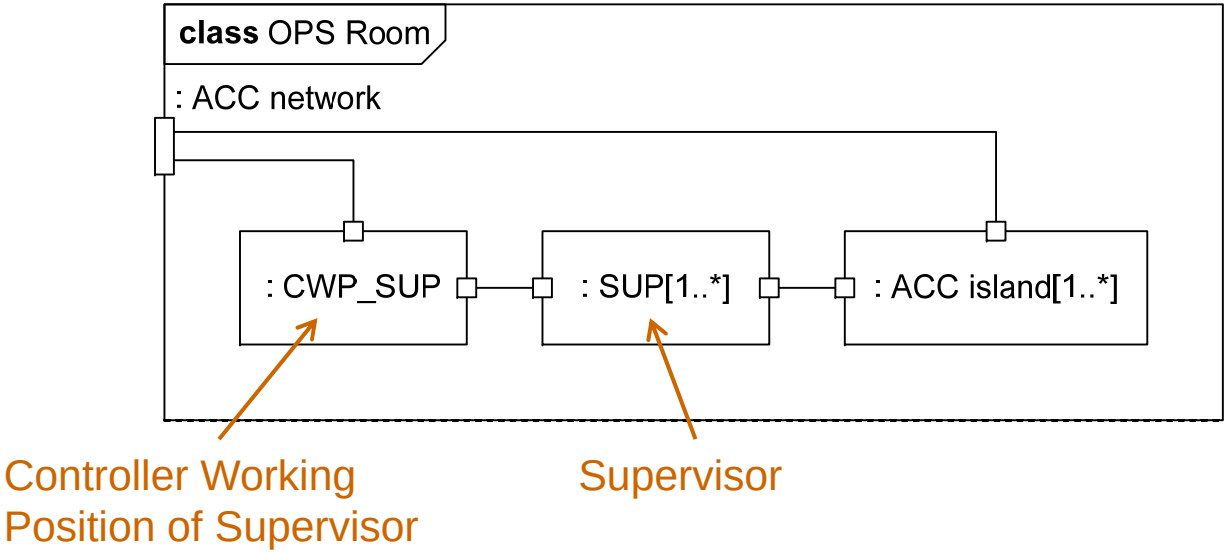
Target Description

- 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)
- One set of diagrams for target as-is
- One set of diagrams for target to-be

Target Before

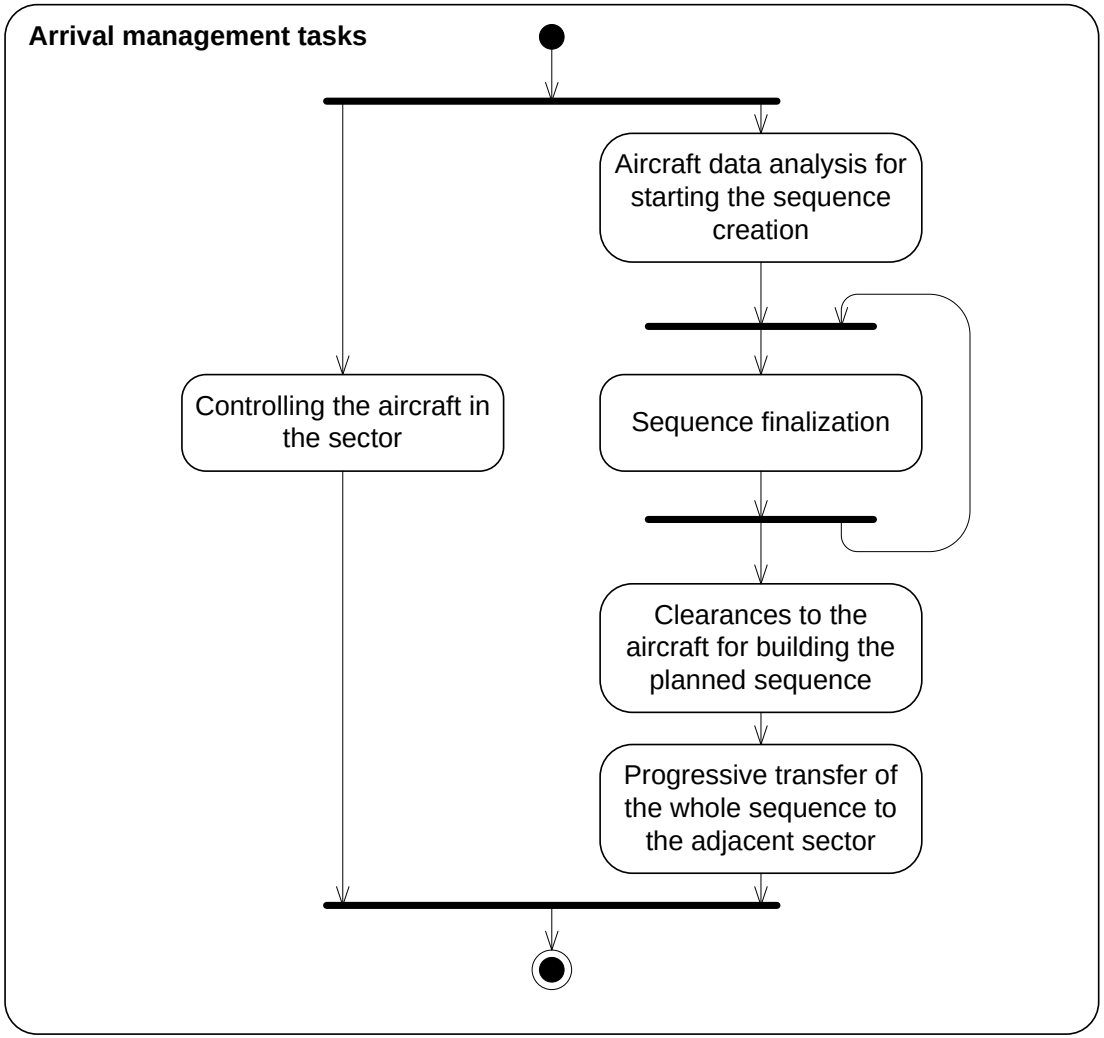


Target Before

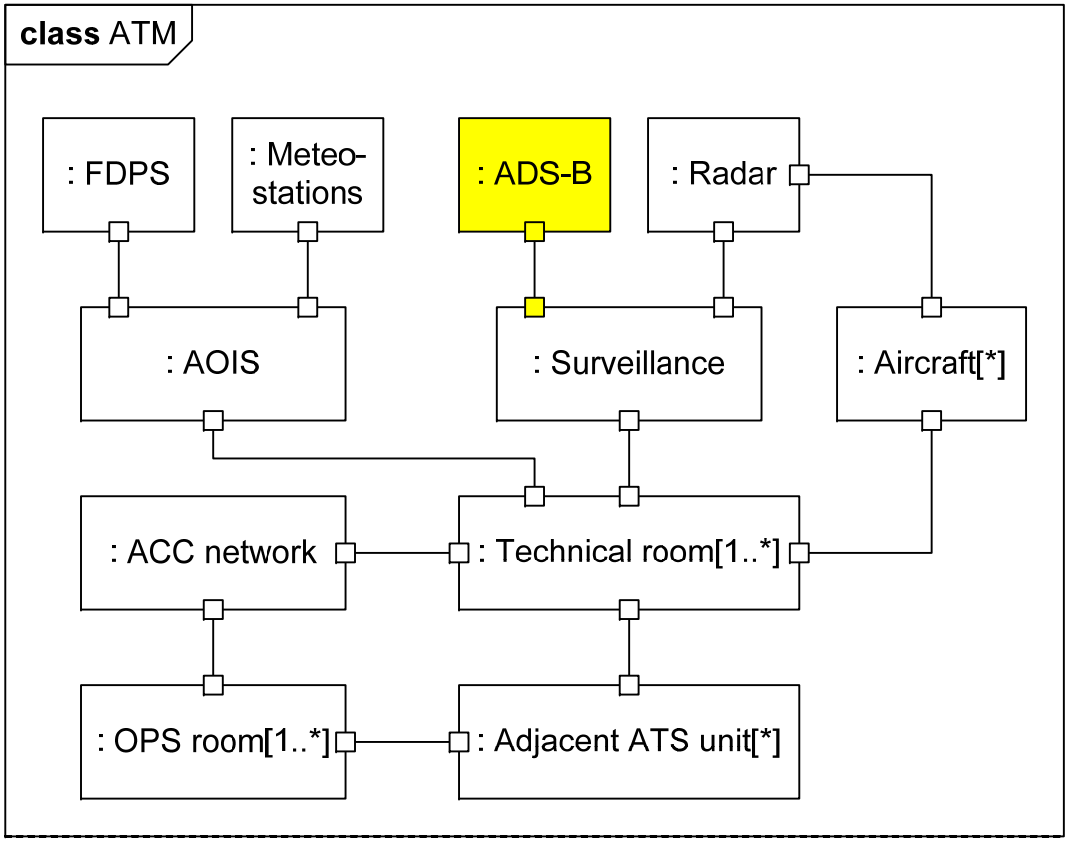


- SUP is an air traffic controller (ATCO) supervising the traffic management of an ACC island
- ATCOs in the ACC island work in teams of two

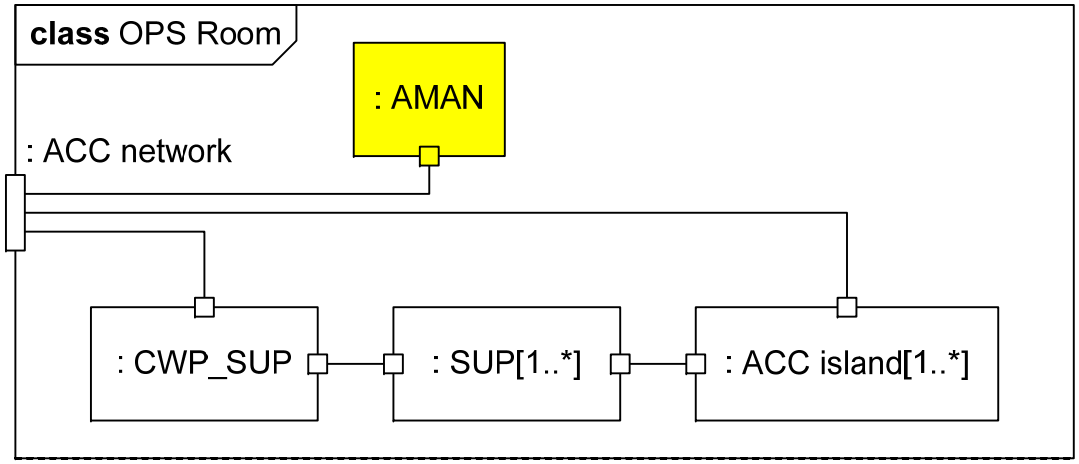
Target Before



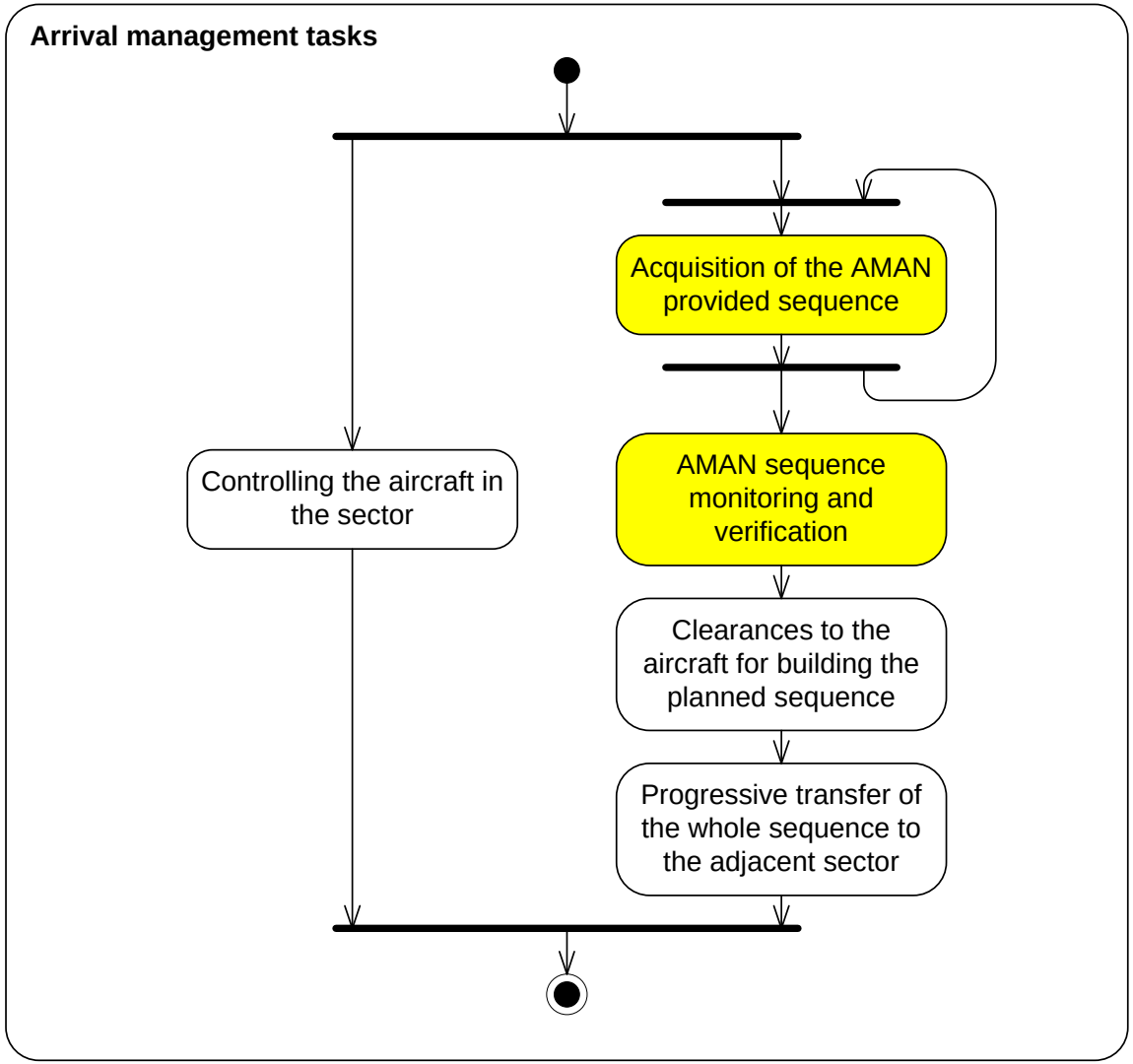
Target After



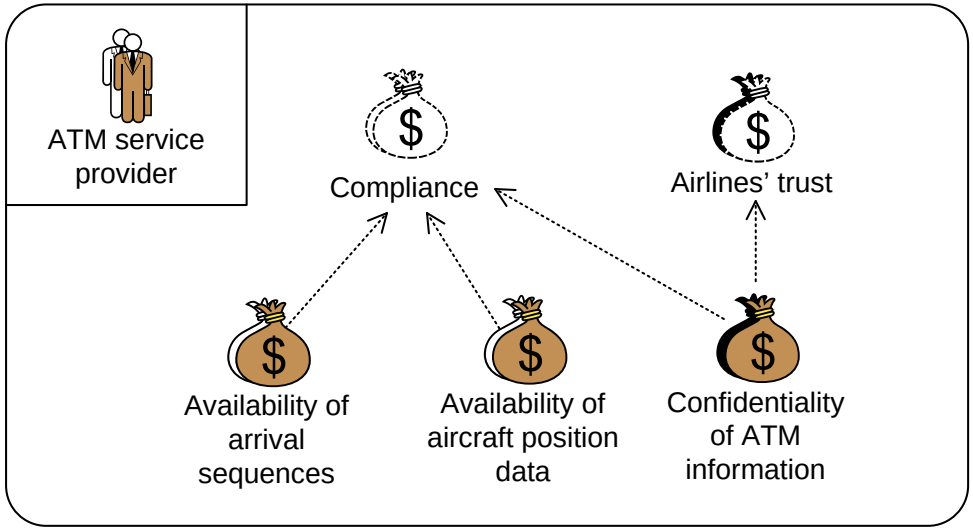
Target After



Target After



Assets Before-After



- Party remains the same under change
- Direct asset Confidentiality of ATM information is considered only after changes
- Indirect asset Airlines' trust is considered only after changes

Consequence Scales

Confidentiality

Consequence	Description
Catastrophic	Loss of data that can be utilized in terror
Major	Data loss of legal implications
Moderate	Distortion of air company competition
Minor	Loss of aircraft information data
Insignificant	Loss of publically available data

Availability

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

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

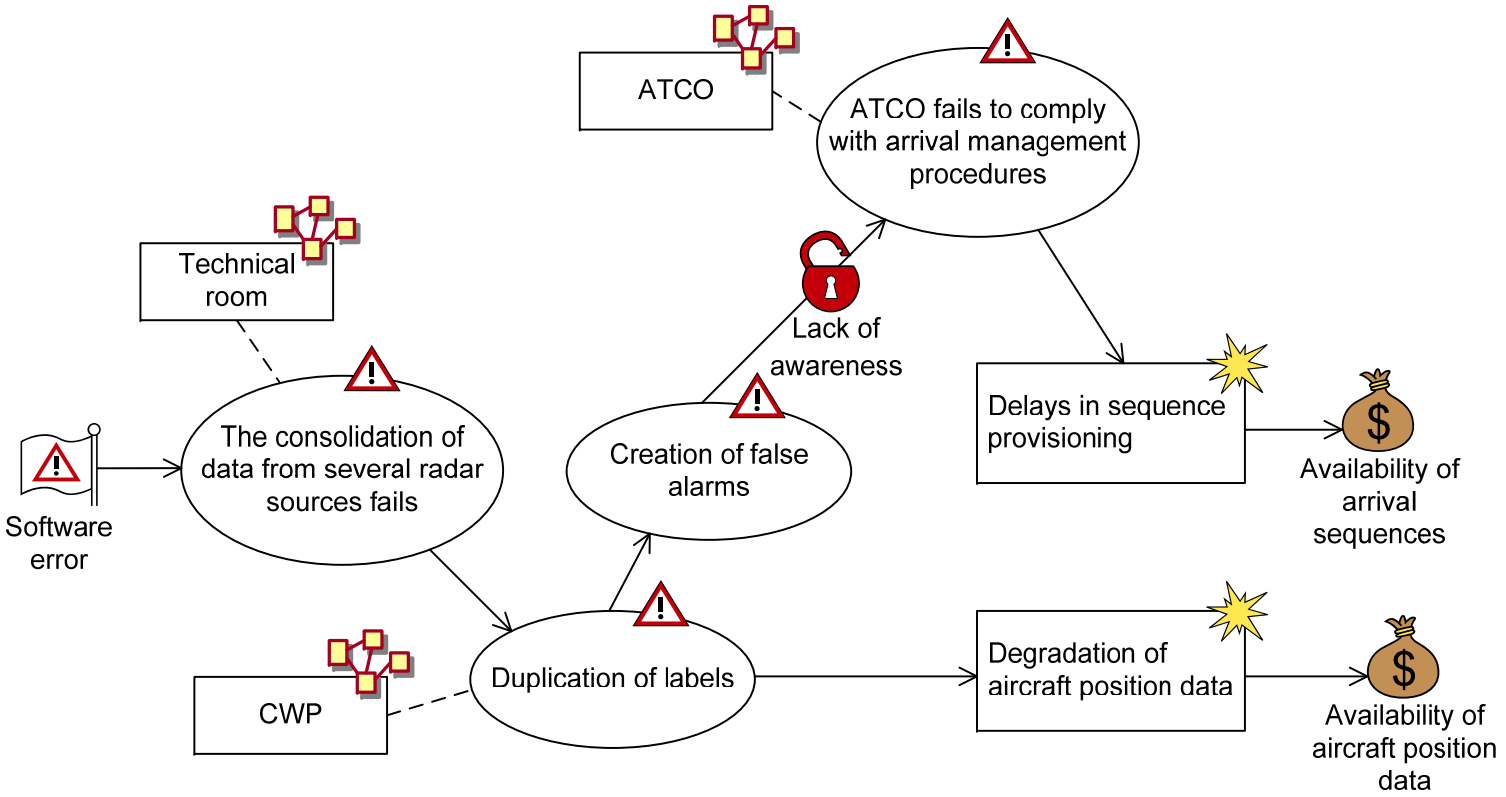
Likelihood	Insignificant	Minor	Moderate	Major	Catastrophic
Rare					
Unlikely					
Possible					
Likely					
Certain					

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

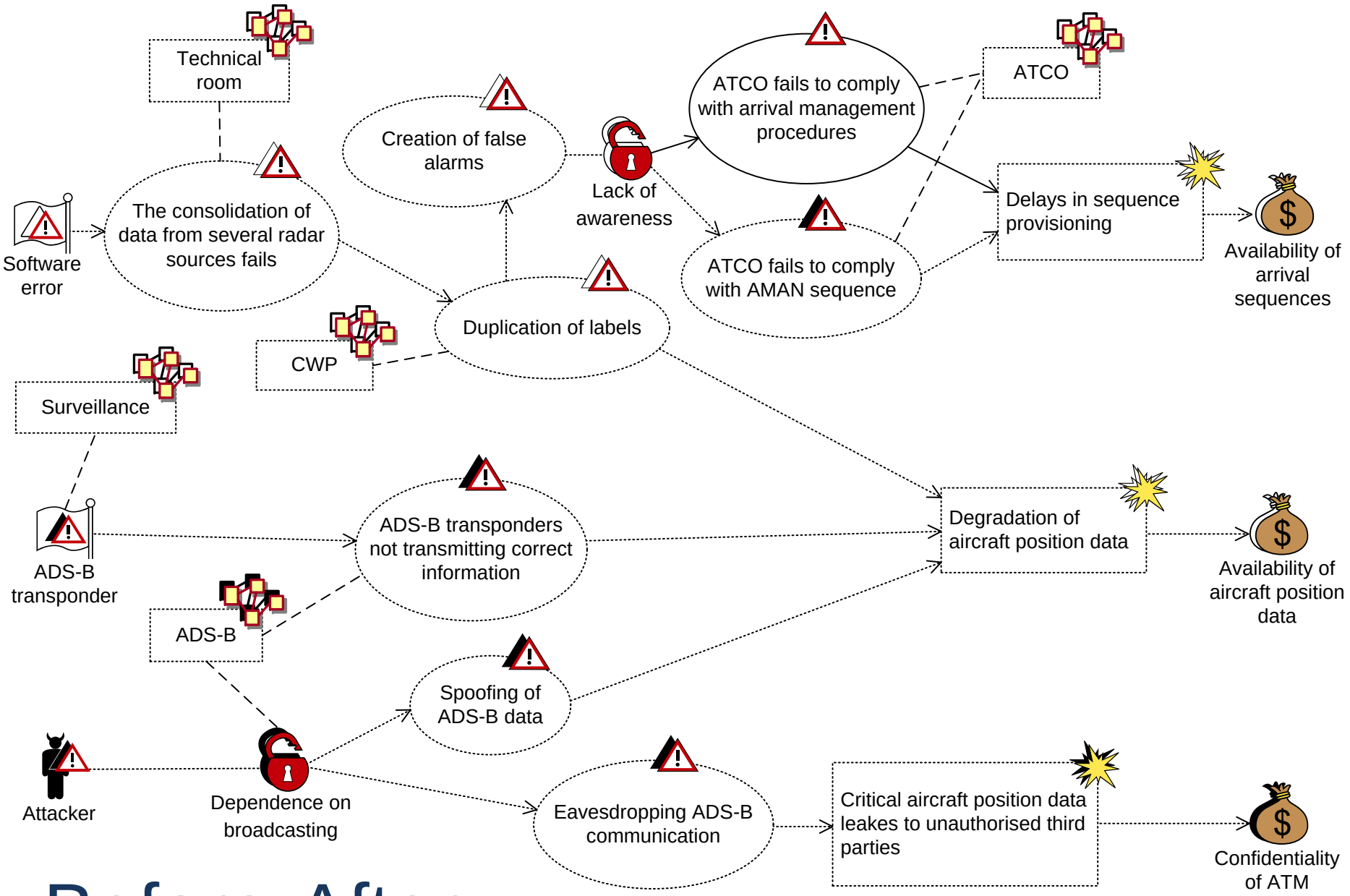
Note: Also the evaluation criteria may change

Risk Identification

CORAS Step 5


ATCO
ATCO fails to comply with arrival management procedures
Technical room
Lack of awareness
Delays in sequence provisioning
Availability of arrival sequences
Software error
The consolidation of data from several radar sources fails
Creation of false alarms
CWP
Duplication of labels
Degradation of aircraft position data
Availability of aircraft position data

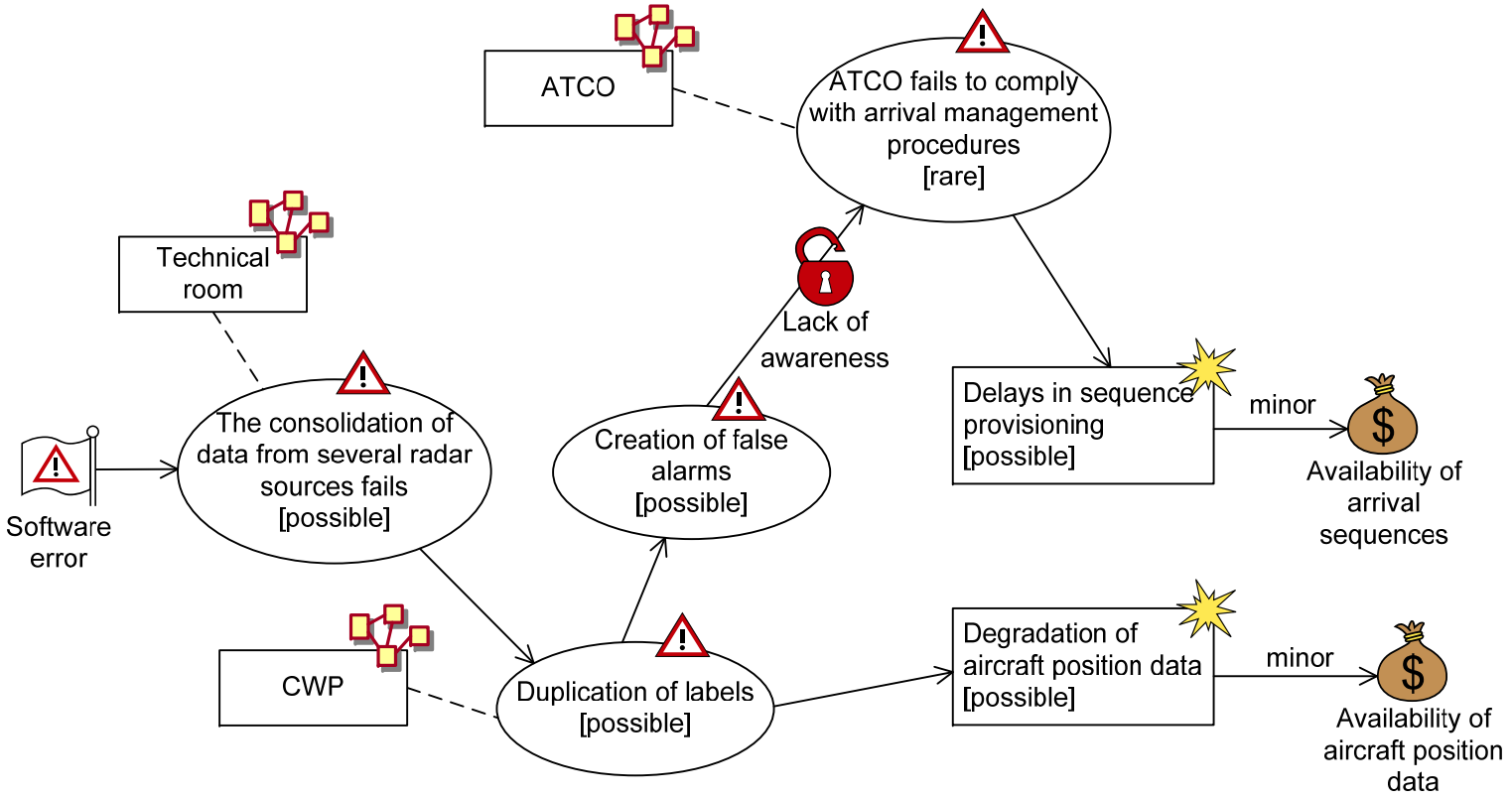
Before



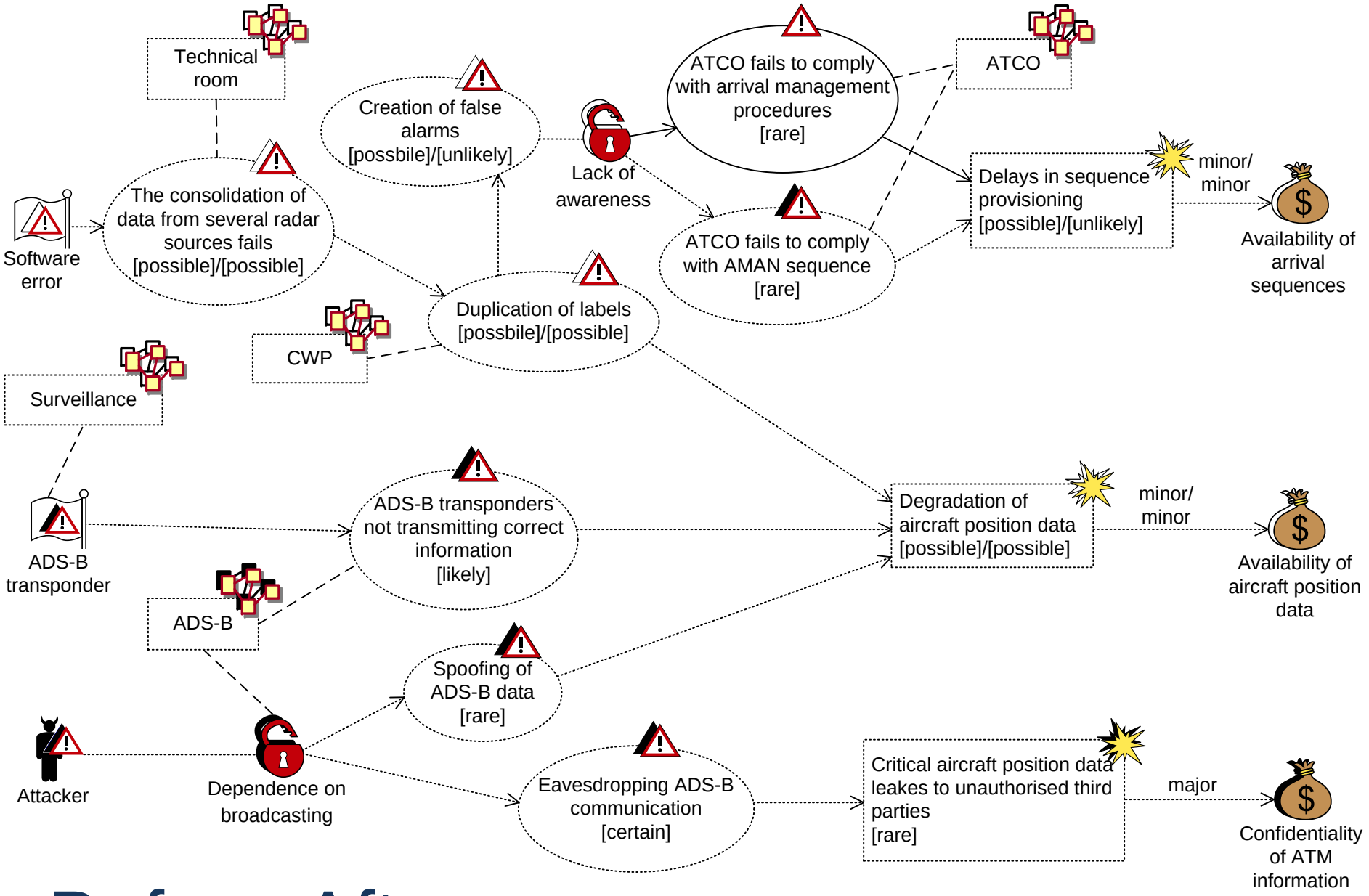
Before-After

Risk Estimation

CORAS Step 6


ATCO
ATCO fails to comply with arrival management procedures [rare]
Technical room
Lack of awareness
Delays in sequence provisioning [possible]
minor
Availability of arrival sequences
The consolidation of data from several radar sources fails [possible]
Creation of false alarms [possible]
Software error
CWP
Duplication of labels [possible]
Degradation of aircraft position data [possible]
minor
Availability of aircraft position data

Before



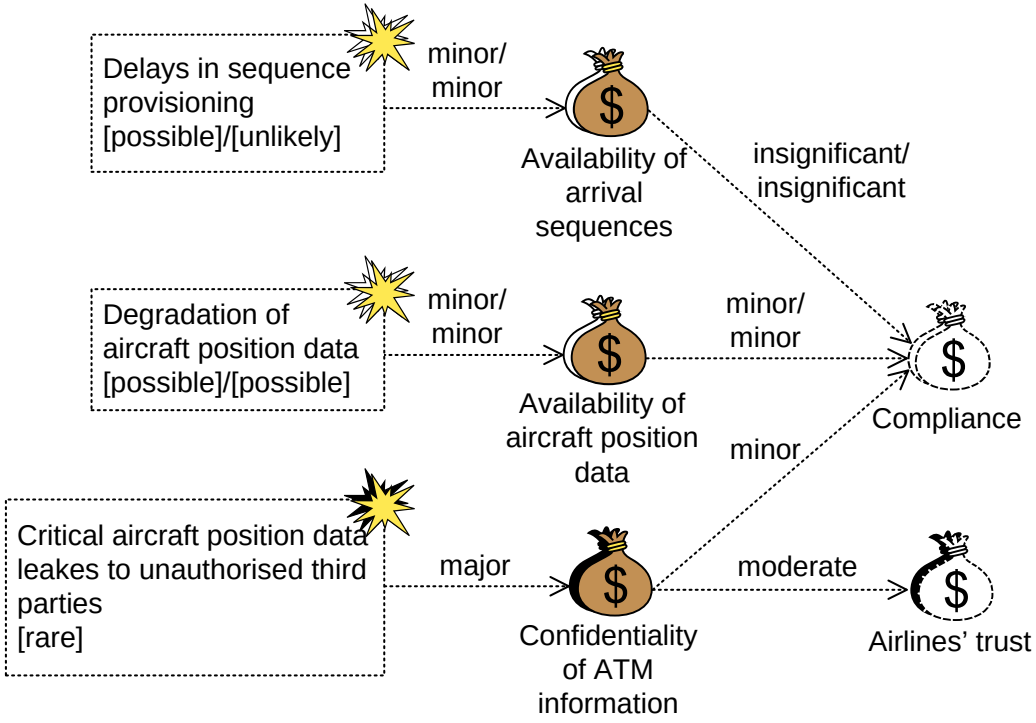
Before-After

Risk Evaluation

CORAS Step 7

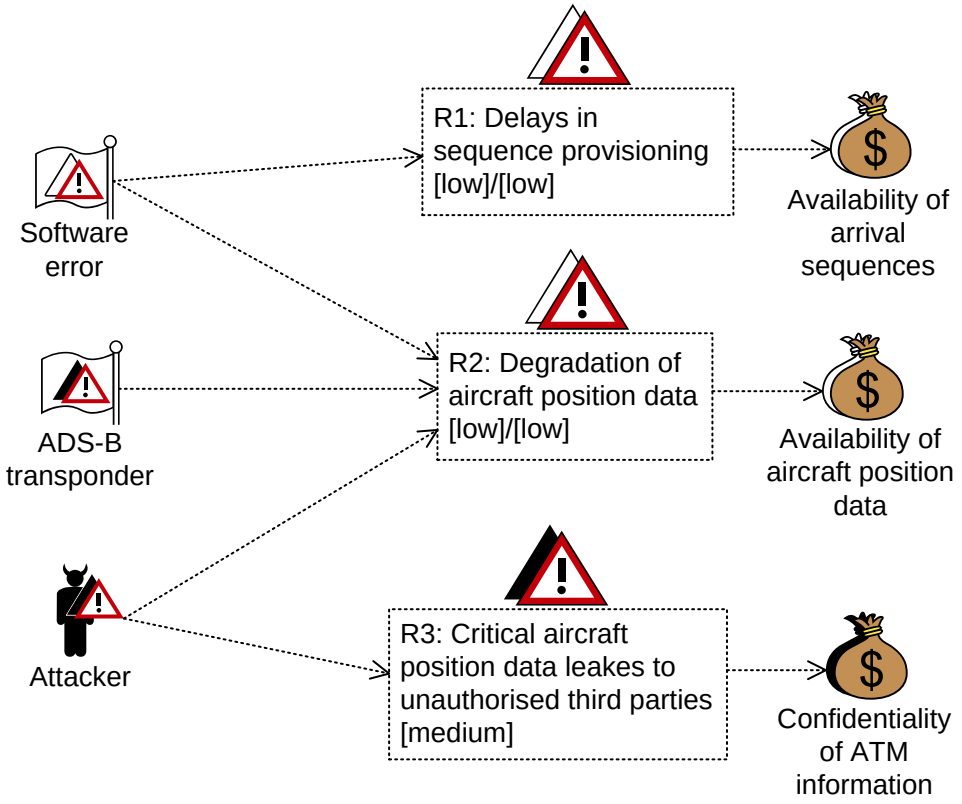
Indirect Assets

- Before-After



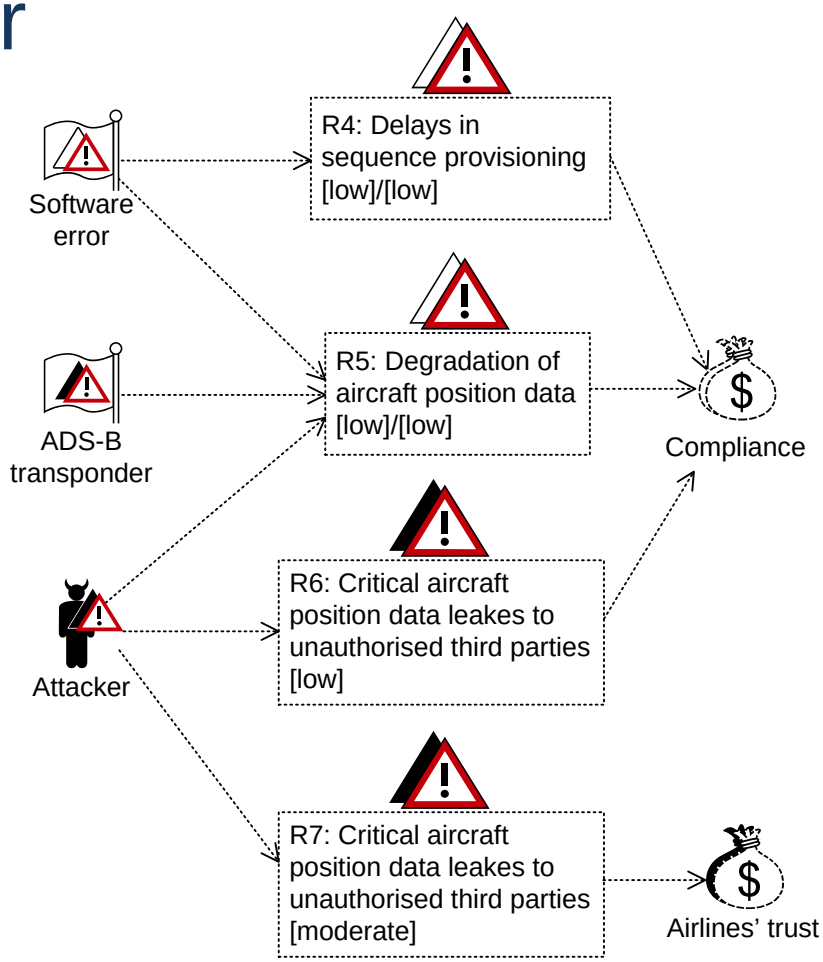
Risk Diagram

- Before-After



Risk Diagram

- Before-After



Risk Evaluation

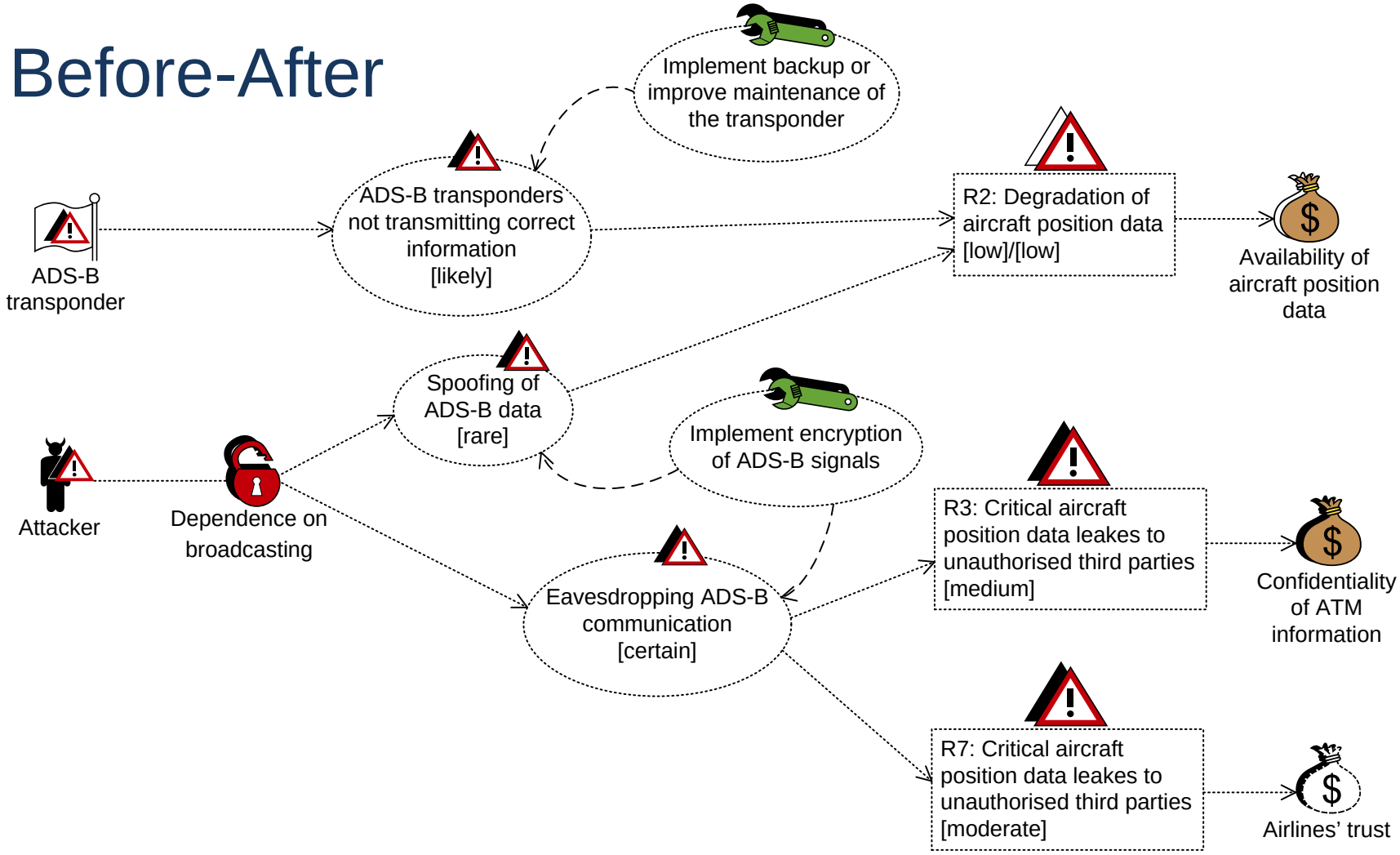
Consequence

Likelihood	Insignificant	Minor	Moderate	Major	Catastrophic
Rare		**R6**	**R7**	**R3**	
Unlikely	**R4**	**R1**			
Possible	*R4*	*R1*, ***R2***, ***R5***			
Likely					
Certain					

- Legend:
  - *Italic* denotes risk before
  - **Bold** denotes risk after

Treatment Diagram

- Before-After



Summary

- For systems that change, also the risks change and should be analyzed as such
- Only the parts of the risk picture affected by changes should be analyzed anew
- CORAS supports
  - Traceability of changes from target system to risk models
  - The explicit modeling of changes to risk
- All artifacts of CORAS are generalized to handle change
  - The CORAS language
  - The CORAS tool
  - The CORAS method
- Further reading:
  - Mass Soldal Lund, Bjørnar Solhaug, Ketil Stølen. Risk analysis of changing and evolving systems using CORAS. To appear in Proc. of Foundations of Security Analysis and Design (FOSAD'11), LCNS, Springer, 2011