Security Risk Assessment III

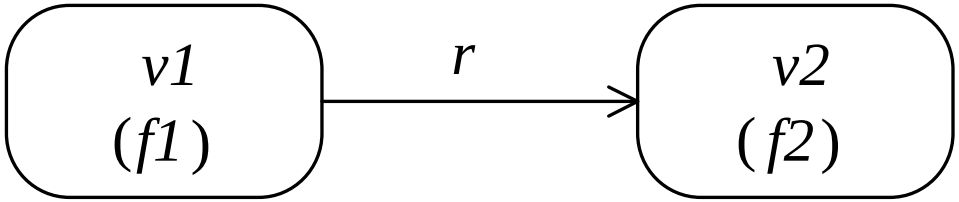
Ketil Stølen, SINTEF & UiO

Overview of Part III

- Frequency calculation
- Consequence calculation
- Three perspectives on change
- Risk graphs with change
- CORAS instantiation
- Practical example

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

$$v_1 \sqcap\!| \; v_2$$

the vertex representing occurrences of vertex v2 that are due to an occurrence of vertex v1

Aggregation

$$v_1 \sqcup v_2$$

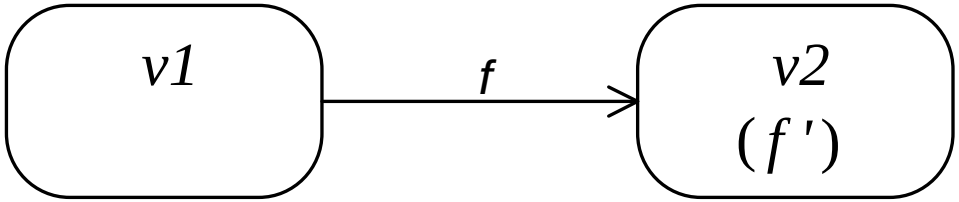
the vertex representing an occurrence of vertex v1 or an occurrence of vertex v2

Leads-to rule

If v1 occurs with frequence f and v1 leads-to v2 with consitional ratio r, then the number of occurrences of v2 due to v1 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 v1 initiates v2 with frequency f, then the number of occurrences of v2 due to v1 is f

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

Aggregation rule

If

v1 occurs with frequence f1
v2 occurs with frequence f2
an occurrence of v1 cannot be an occurrence of v2
an occurrence of v2 cannot be an occurrence of v1

then

v1 or v2 occurs with frequency f1+f2

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

Consequence calculation

Pre-requisite

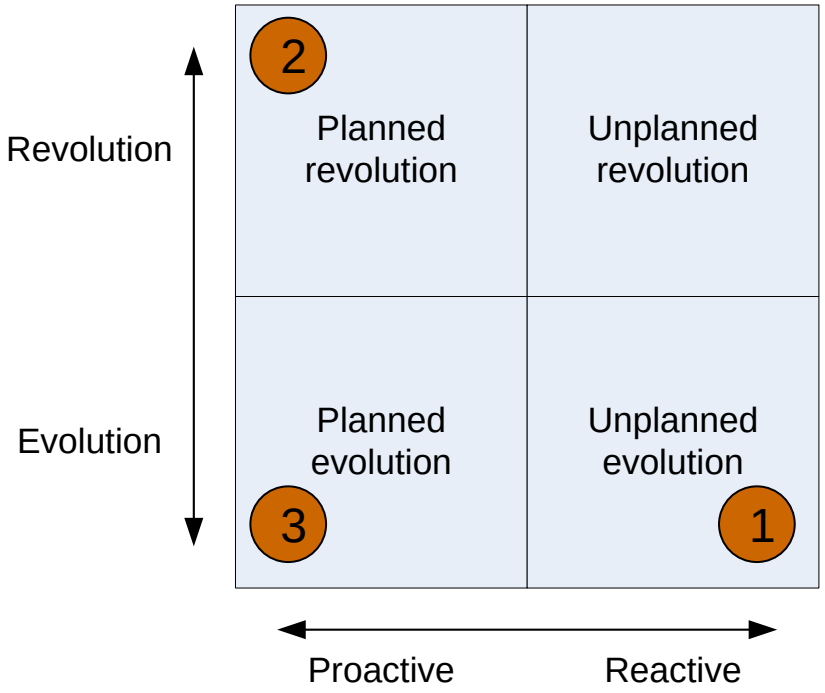
- Not possible unless the relevant consequence scales have been concerted into a common scale
- In the following we assume consequence is measured in terms of

Average loss in EURO per occurrence

Rule for aggregation of consequence

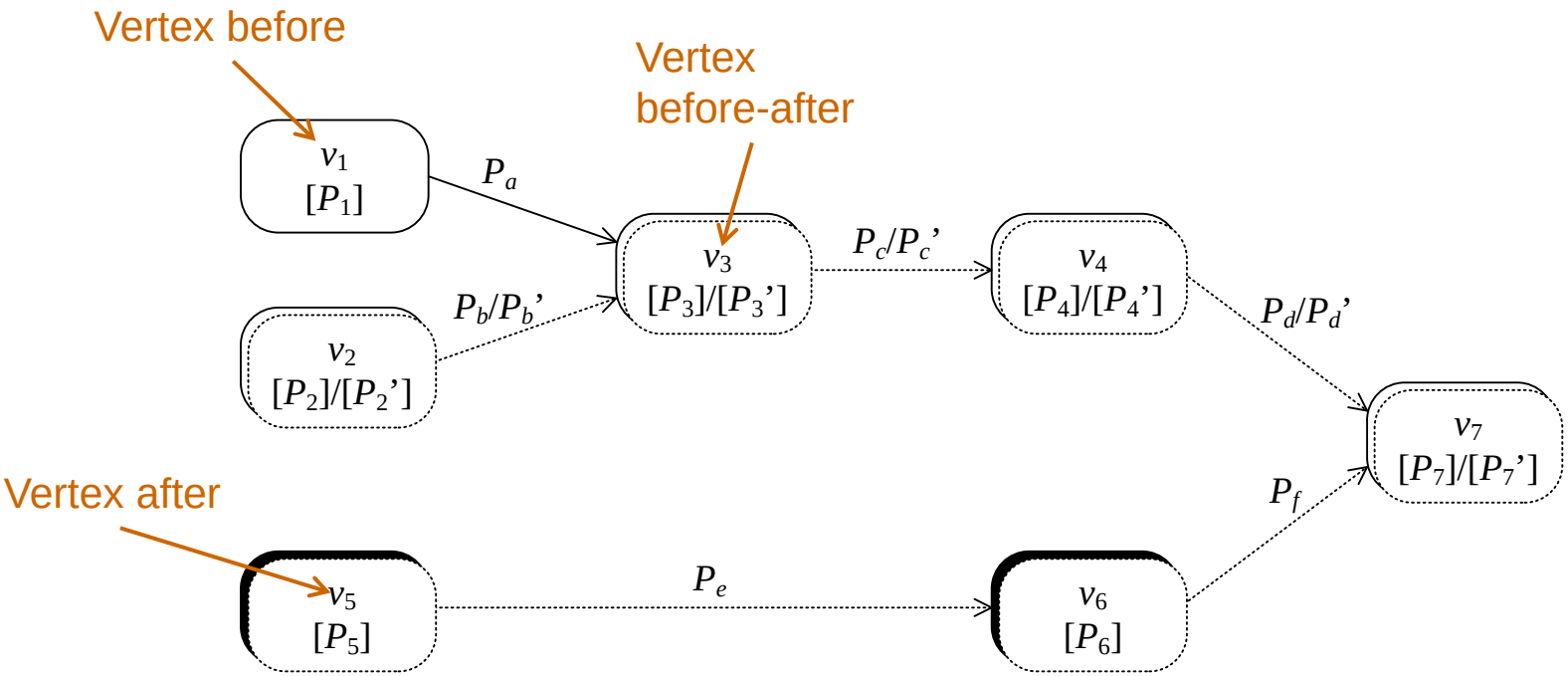
- IF
  - incident v1 occurs with frequency f1 and consequence c1
  - incident v2 occurs with frequency f2 and consequence c1
  - incident v1 and incident v2 are separate
- THEN
  - the aggregated incident occurs with consequence (f1*c1+f2*c2)/(f1+f2)

Three Perspectives on Change



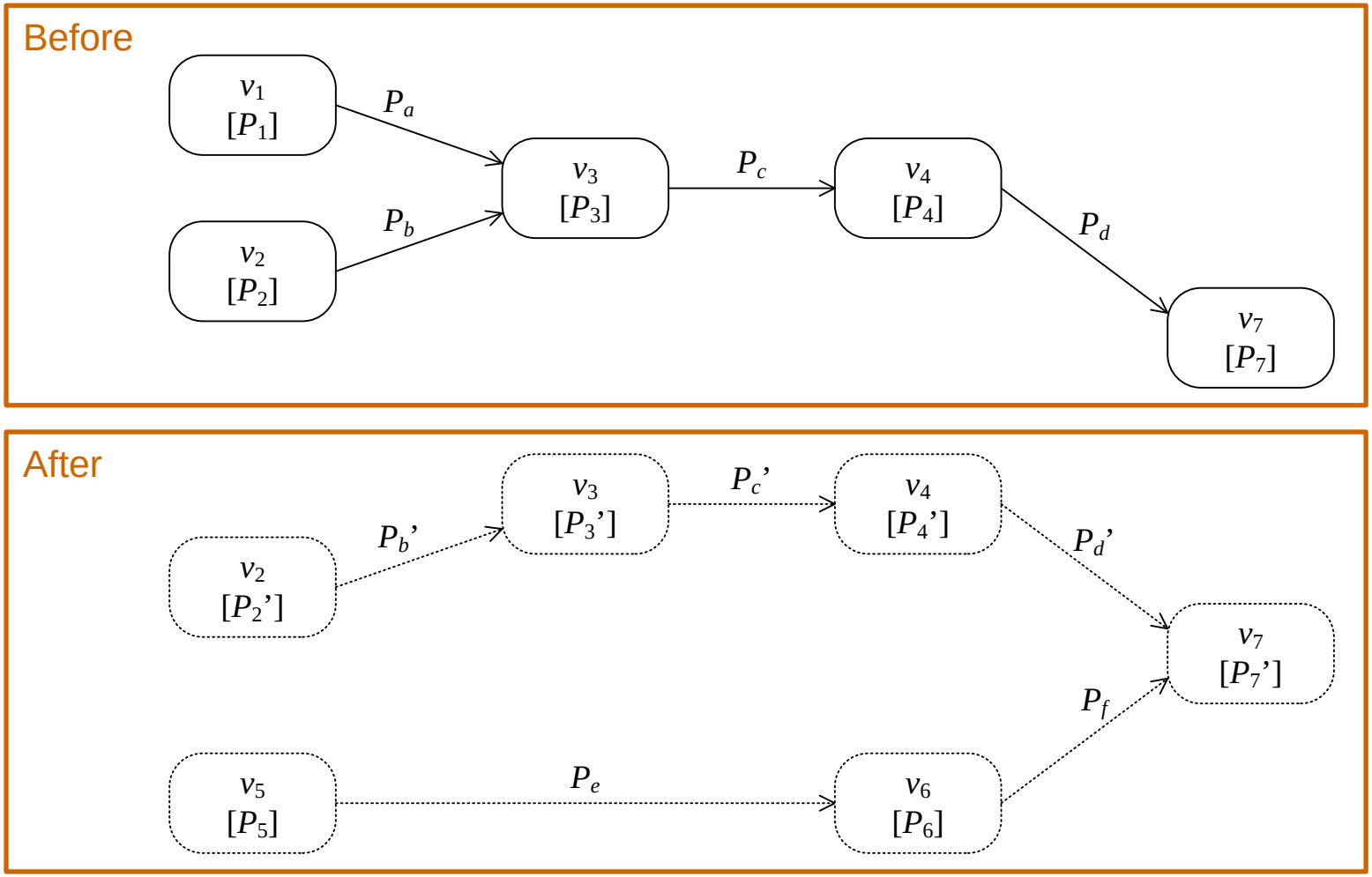
1: The maintenance (a posteriori) perspective
2: The before-after (a priori) perspective
3: The continuous evolution perspective

Risk Graphs with Change

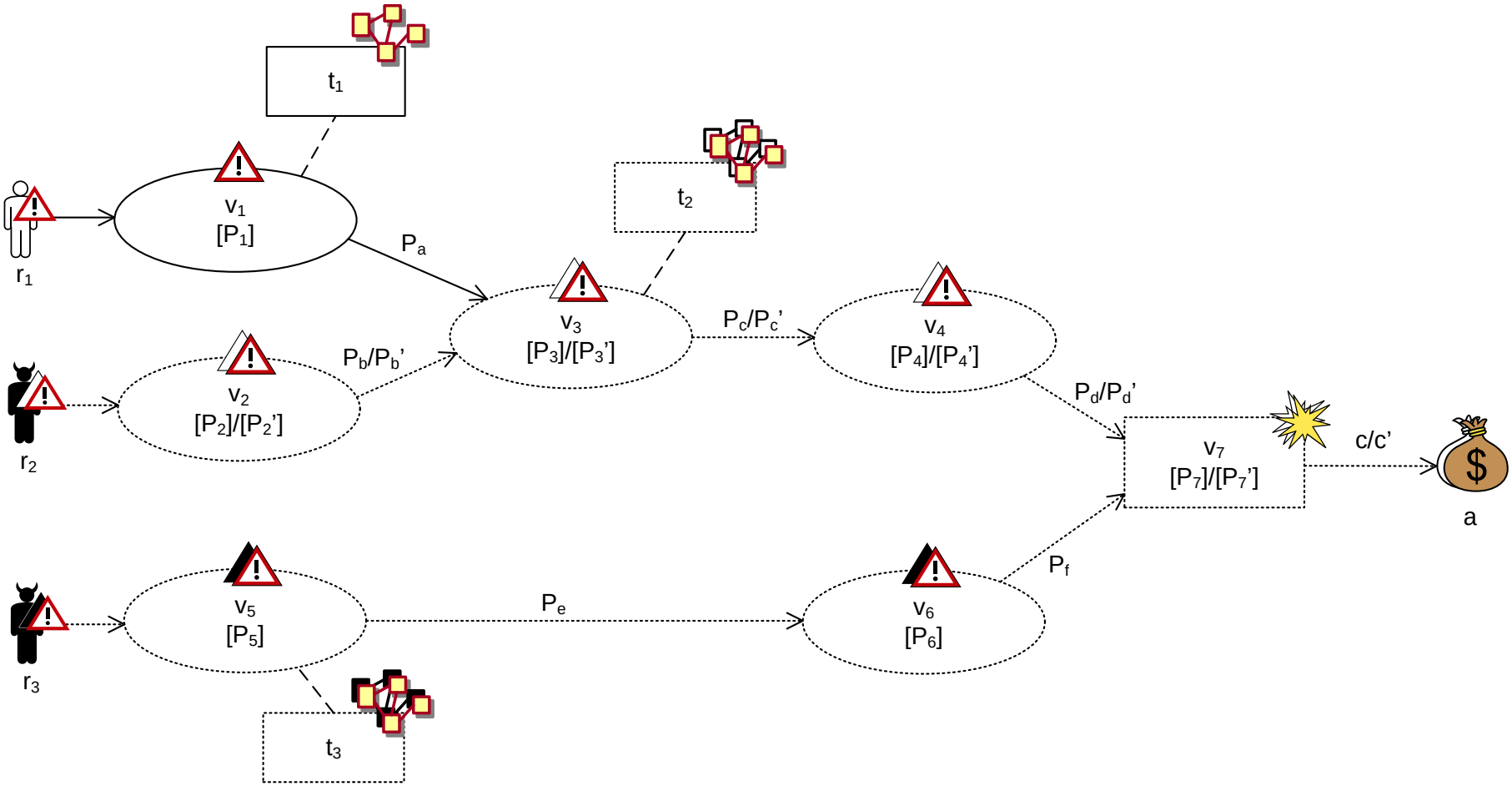


- Explicit modeling of
  - Elements before change
  - Elements after change
  - Changes in likelihood estimates

Two Views on Risk Graphs with Change



CORAS Instantiation



Practical Example: ATM

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

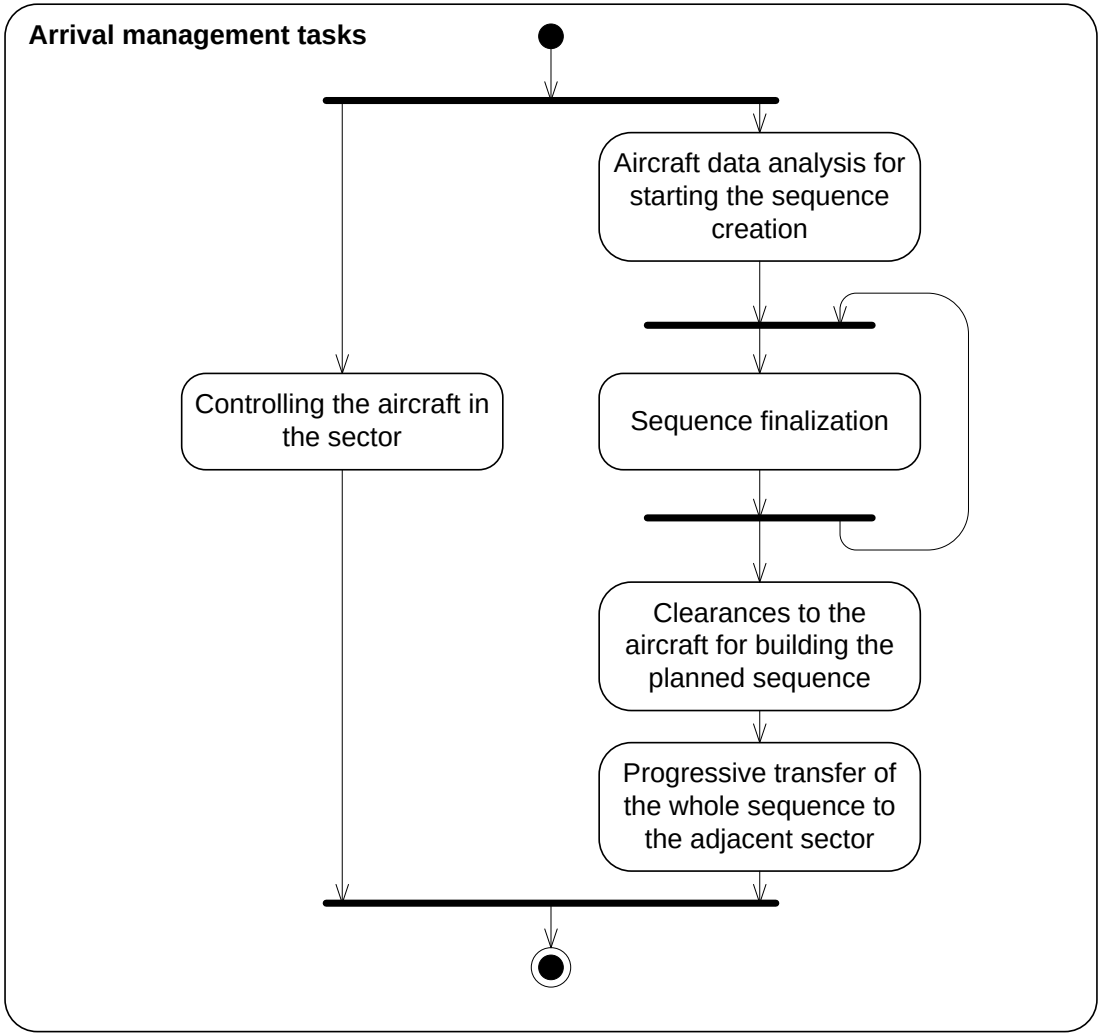
Target of Analysis

- 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

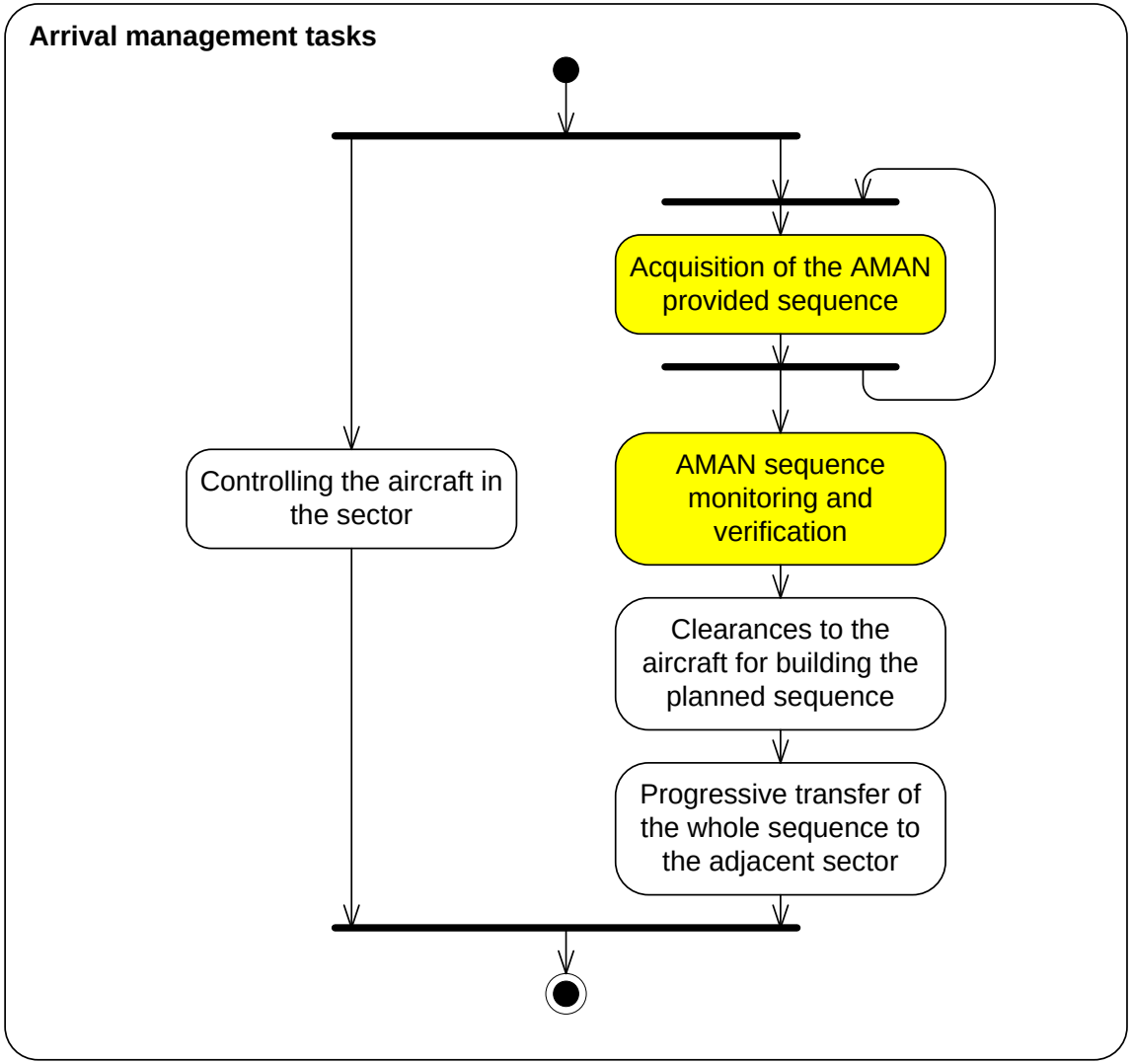
Focus of Analysis

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

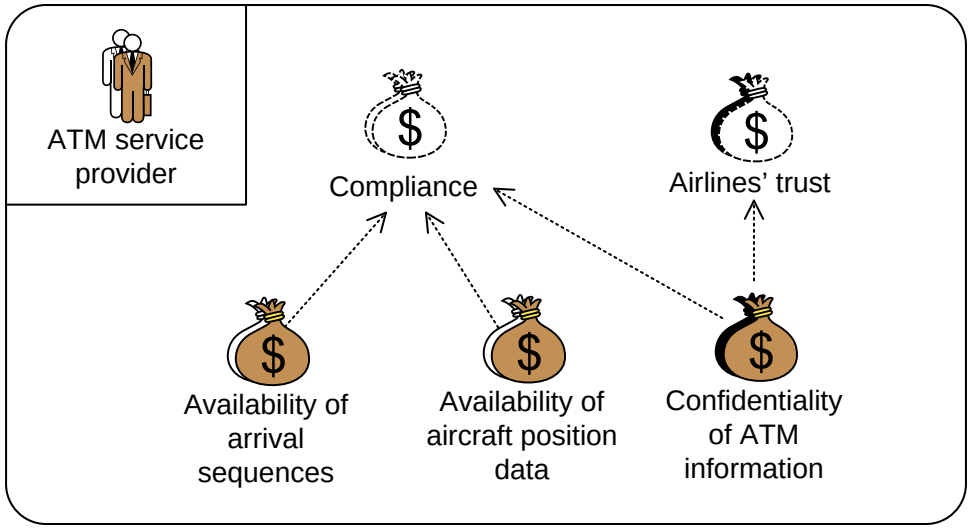
Target Before



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

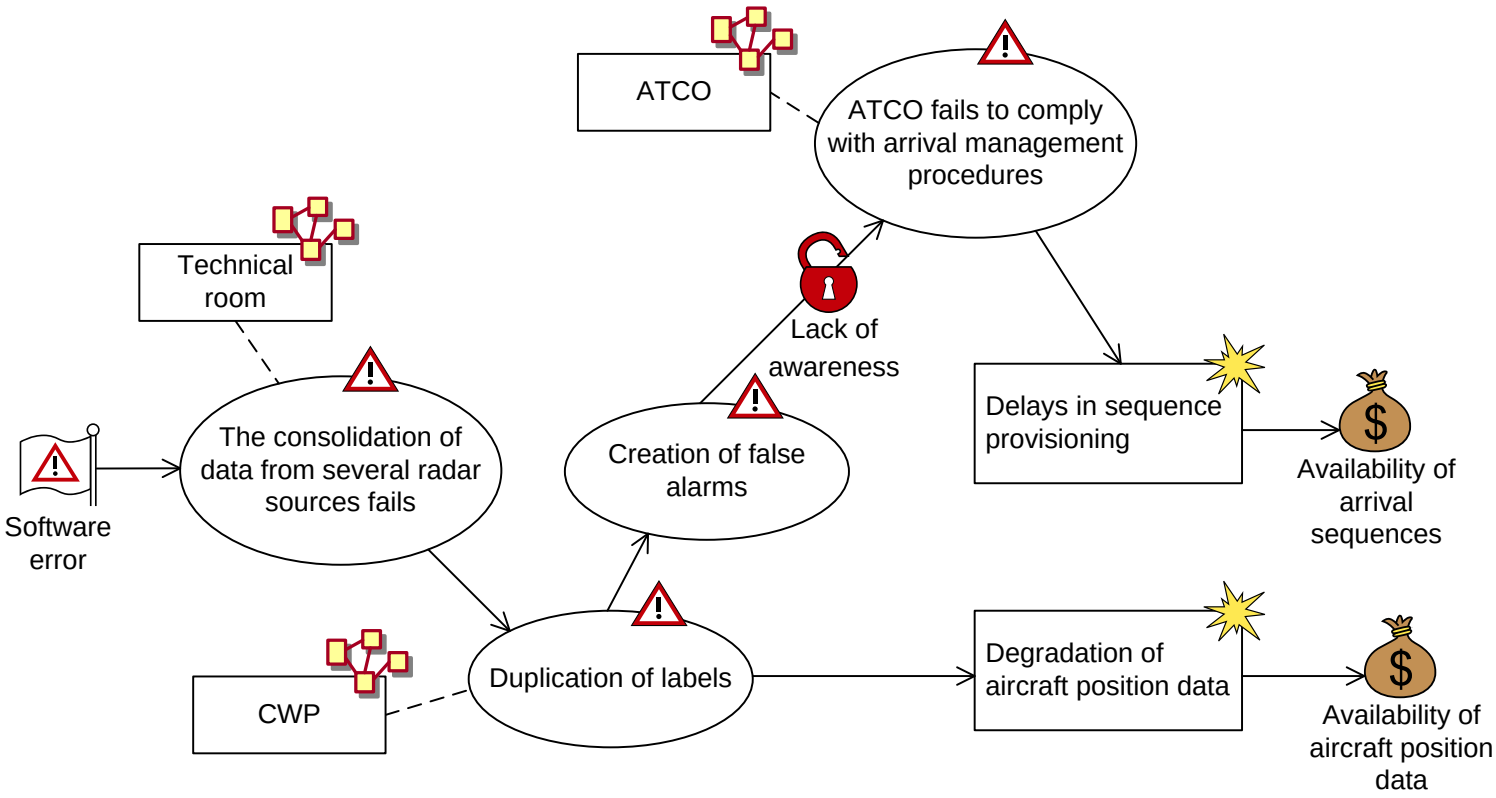
Likelihood	Consequence				
	Insignificant	Minor	Moderate	Major	Catastrophic
Rare					
Unlikely					
Possible					
Likely					
Certain					

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

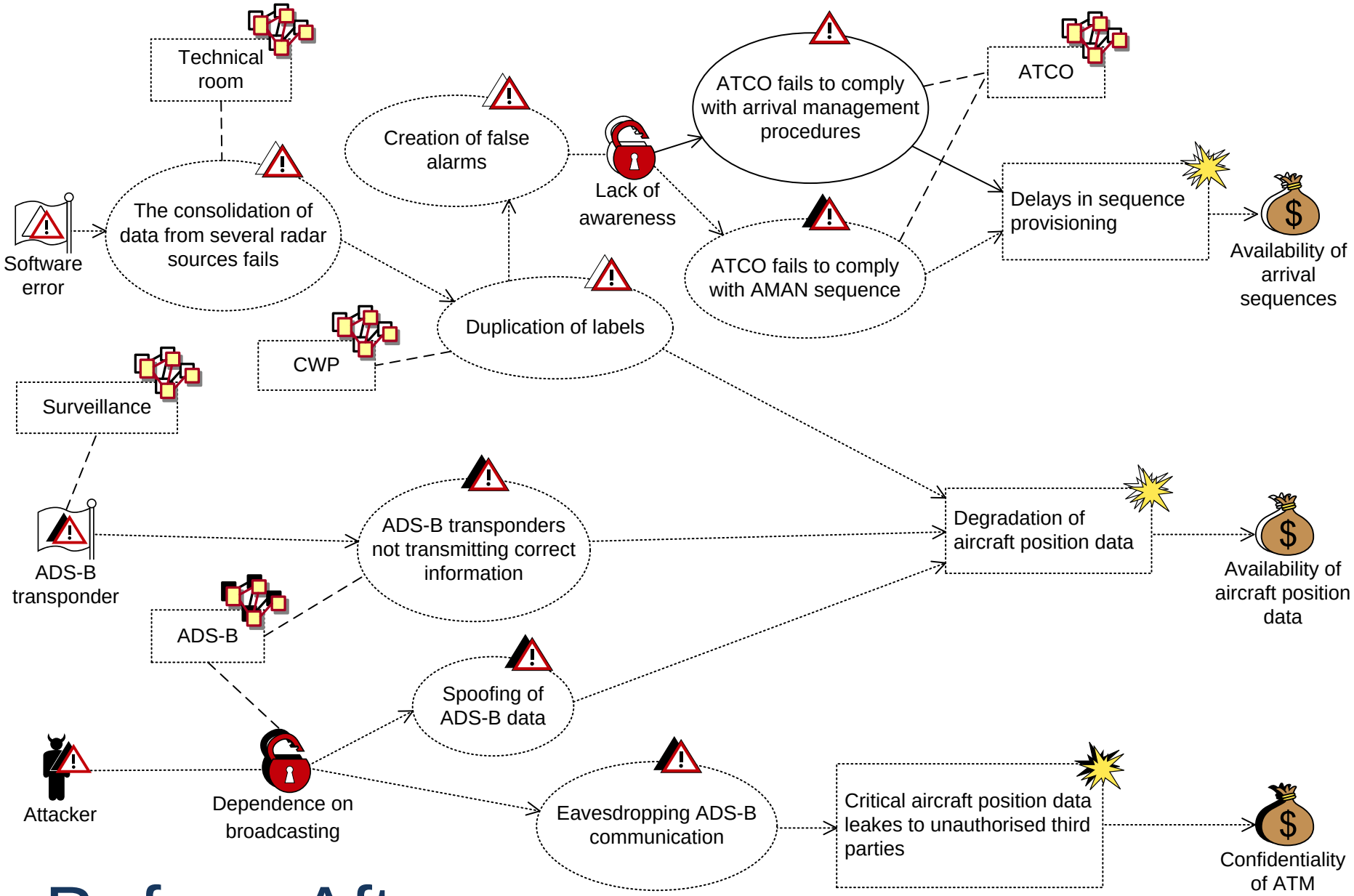
Note: Also the evaluation criteria may change

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

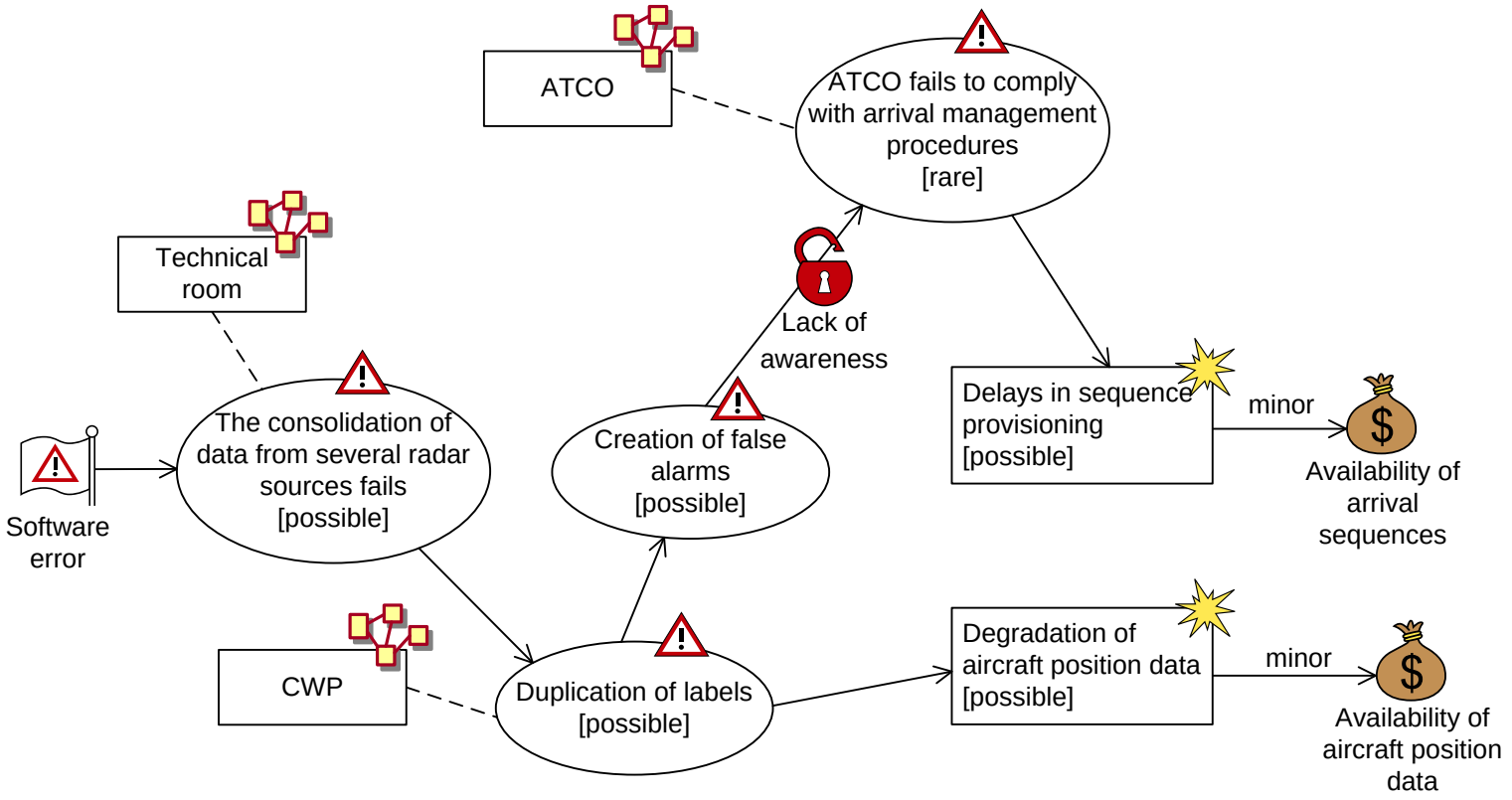
Before



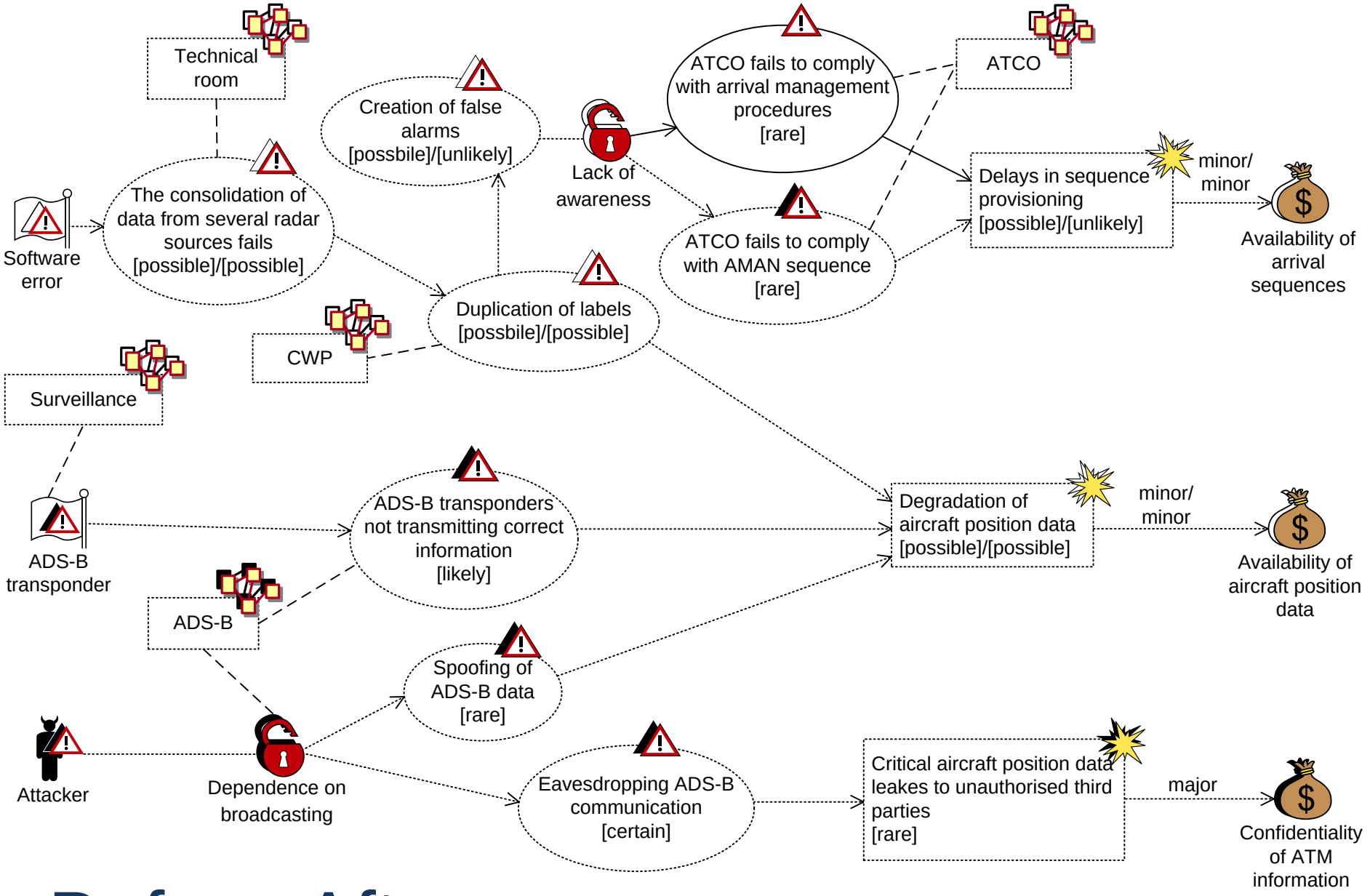
Before-After

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
Software error
The consolidation of data from several radar sources fails [possible]
Creation of false alarms [possible]
CWP
Duplication of labels [possible]
Degradation of aircraft position data [possible]
minor
Availability of aircraft position data

Before



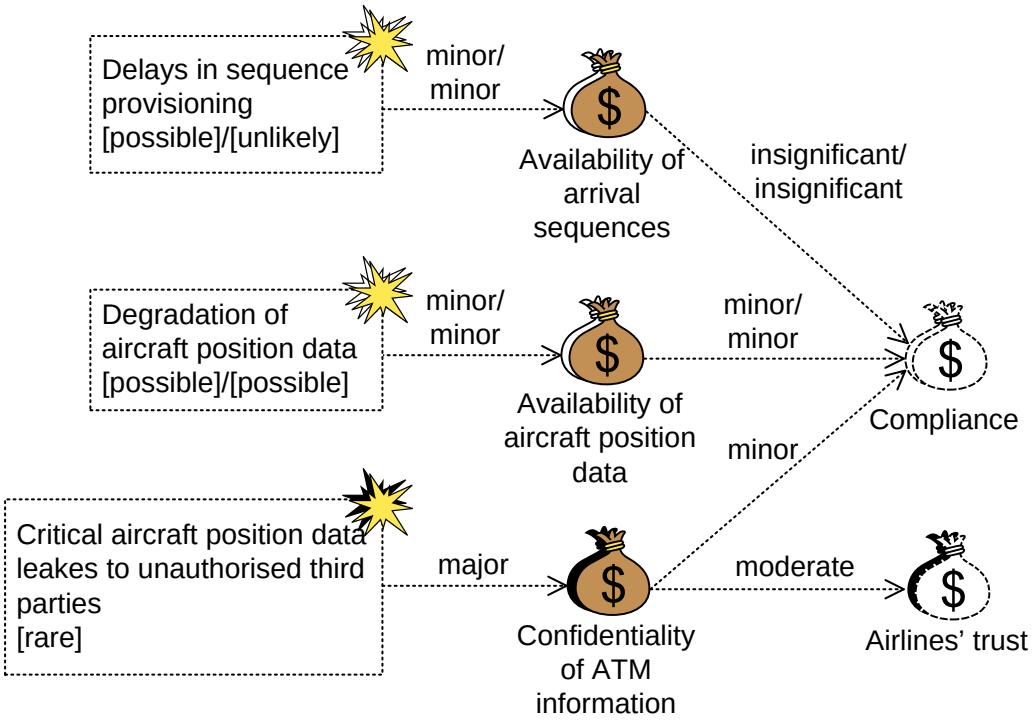
Before-After

Risk Evaluation

CORAS Step 7

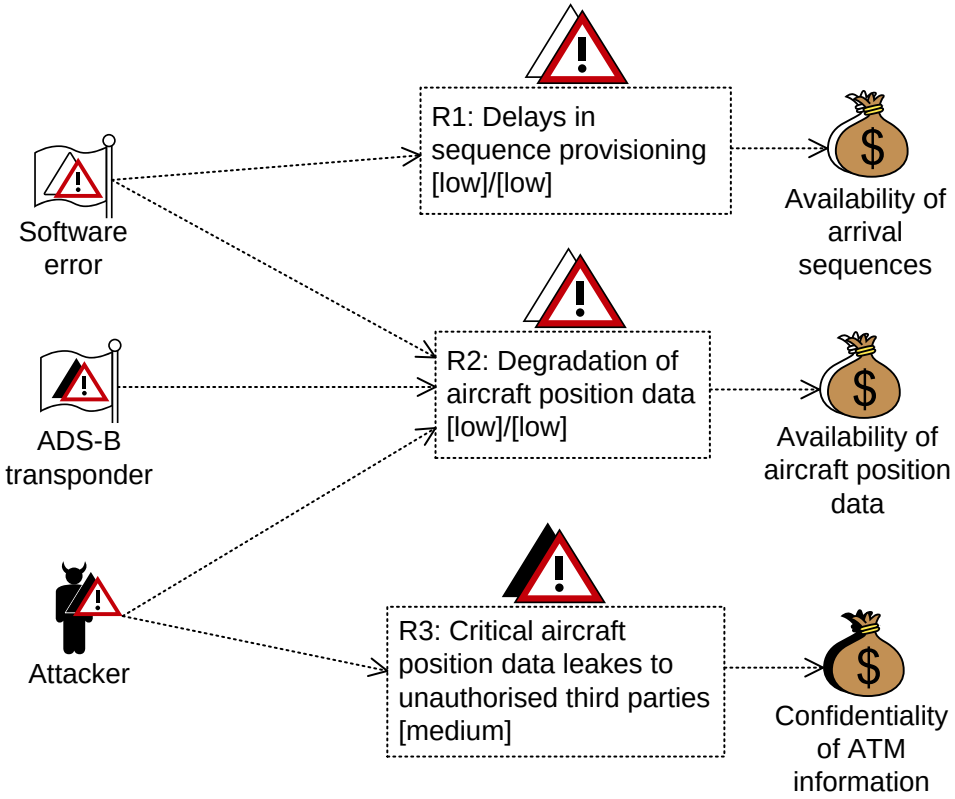
Indirect Assets

- Before-After



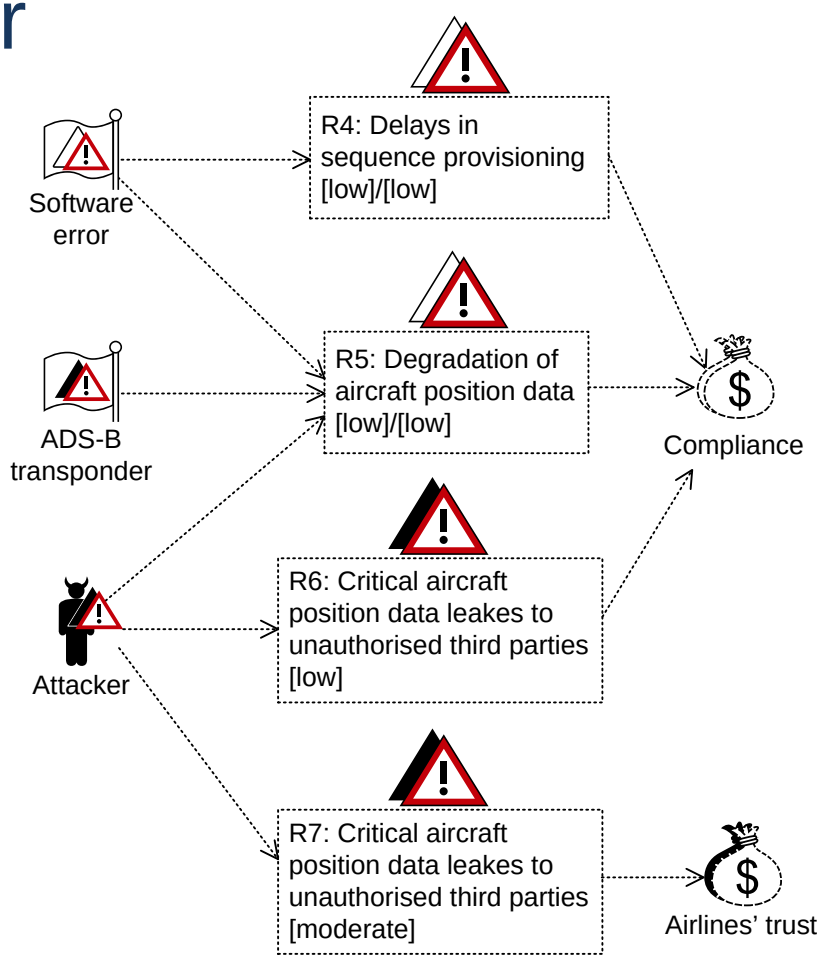
Risk Diagram

- 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