Security Risk Assessment III

Ketil Stølen, SINTEF & UiO

Overview of Part III

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

Consequence calculation

Pre-requisite

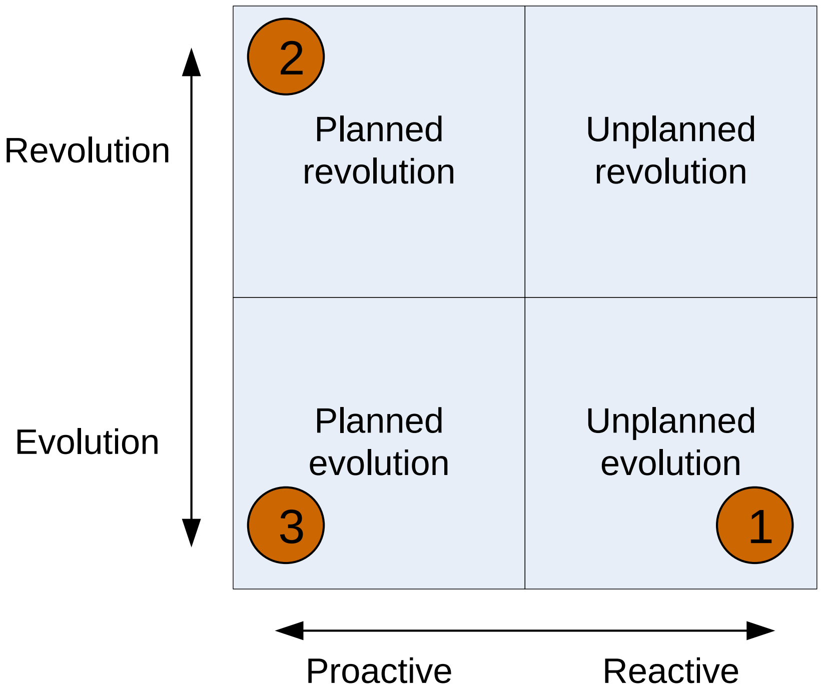
- Not possible unless the relevant consequence scales have been concerted into a common scale
- In the following we assume consequence is measured in terms of

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)

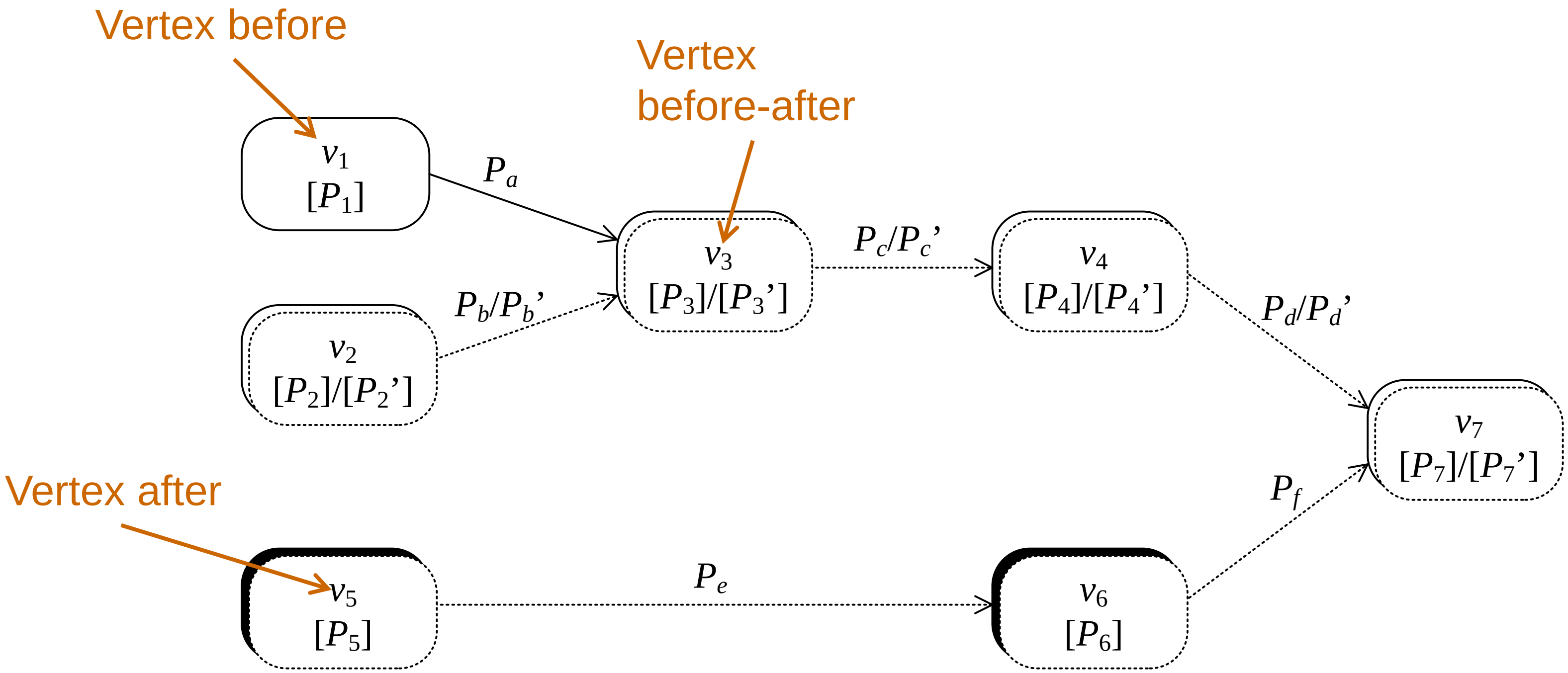
Three Perspectives on Change



	Proactive	Reactive
Revolution	2 Planned revolution	Unplanned revolution
Evolution	Planned evolution 3	Unplanned evolution 1

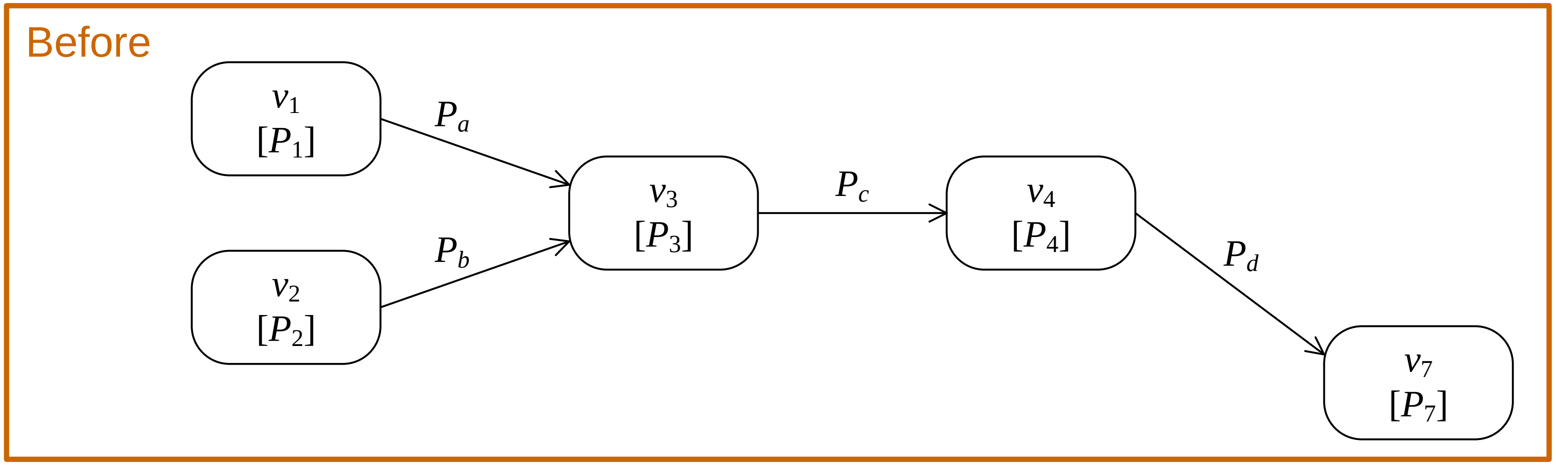
1: The maintenance (a posteriori) perspective
2: The before-after (a priori) perspective
3: The continuous evolution perspective

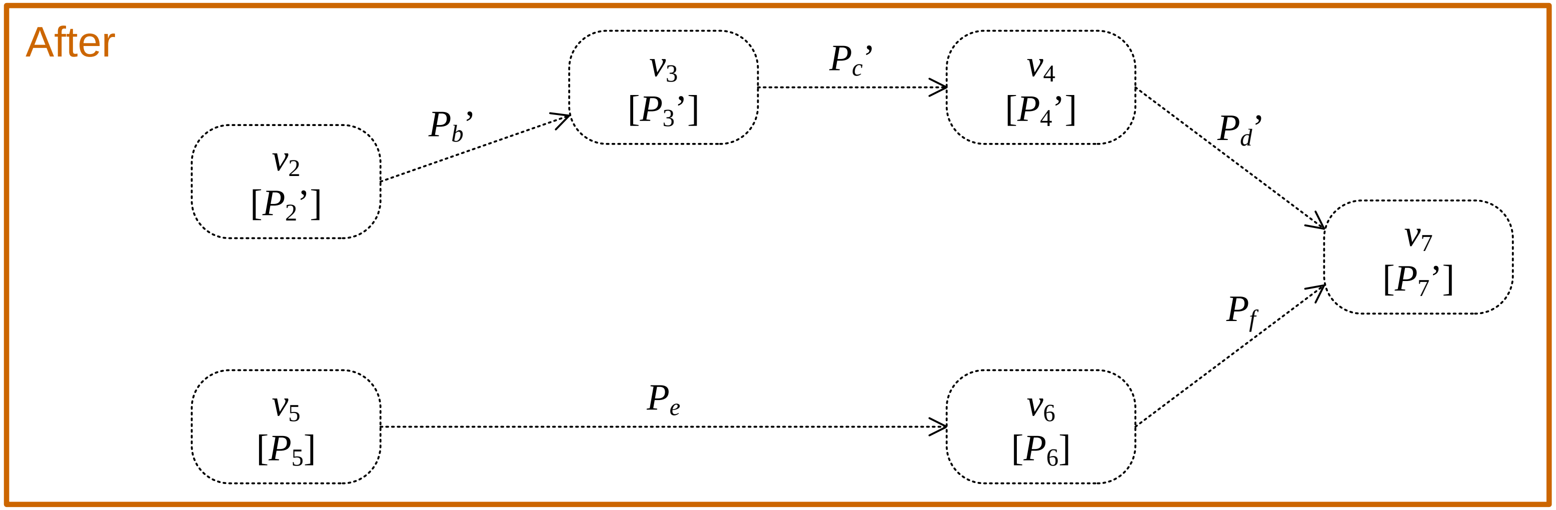
Risk Graphs with Change



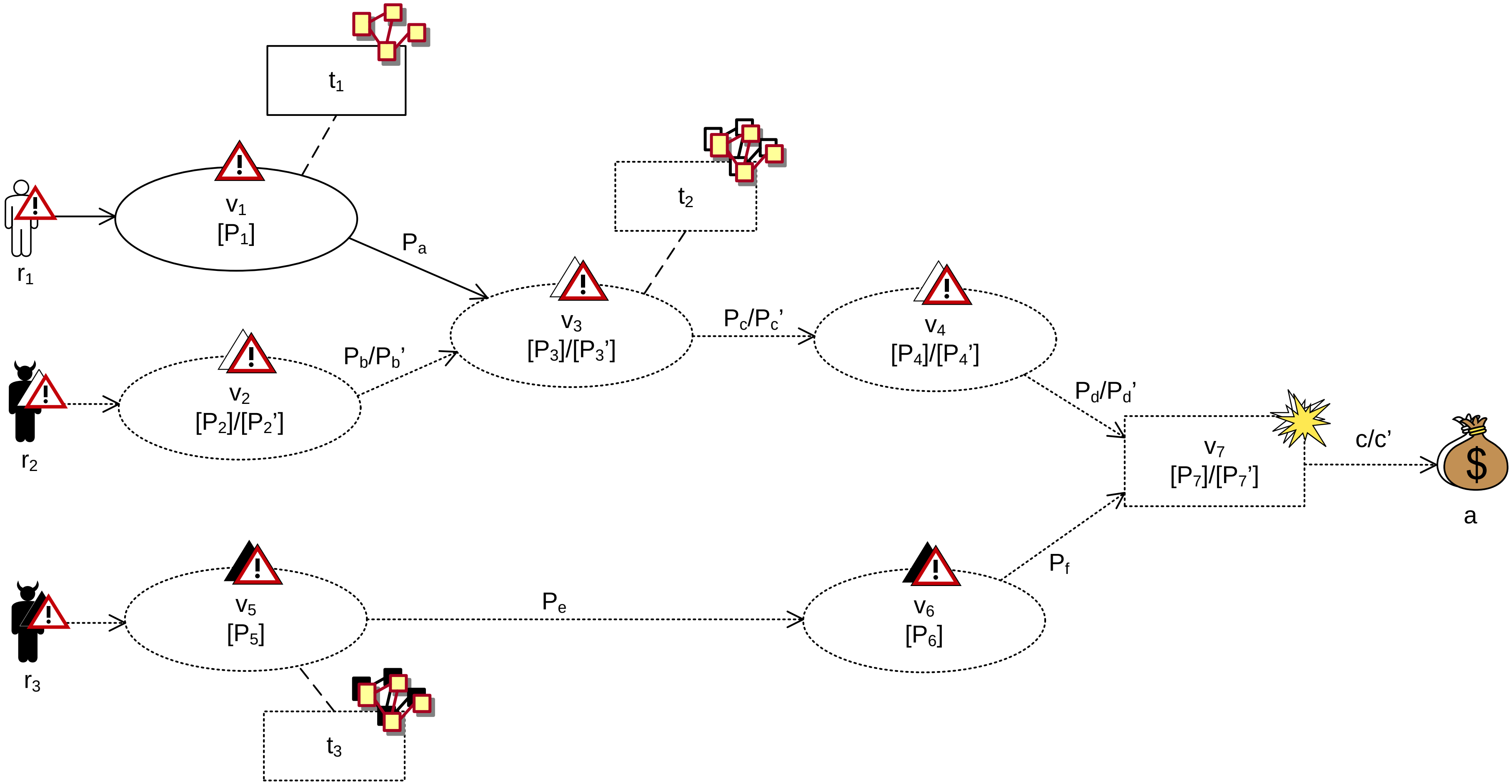
- Explicit modeling of
  - Elements before change
  - Elements after change
  - Changes in likelihood estimates

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

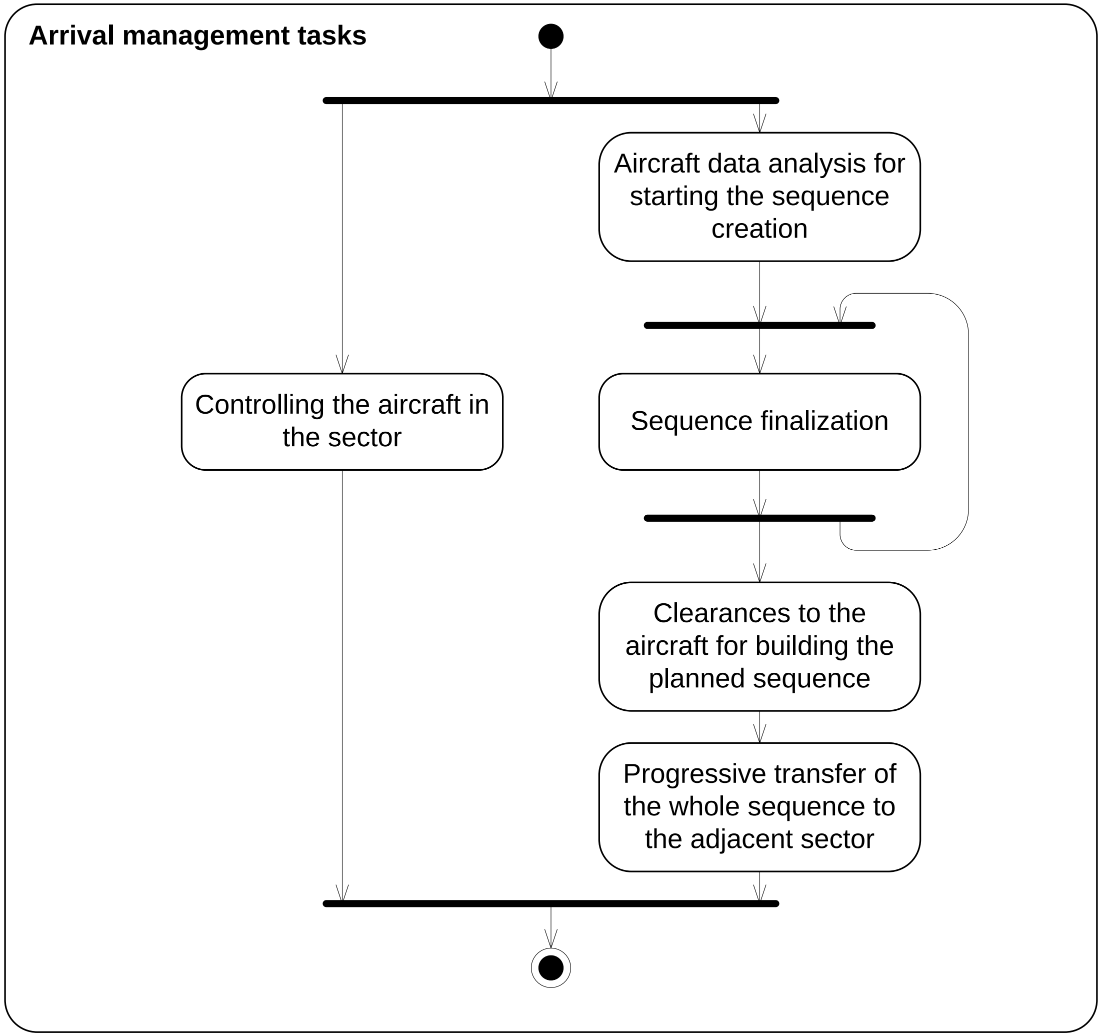
Target of Analysis

- 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

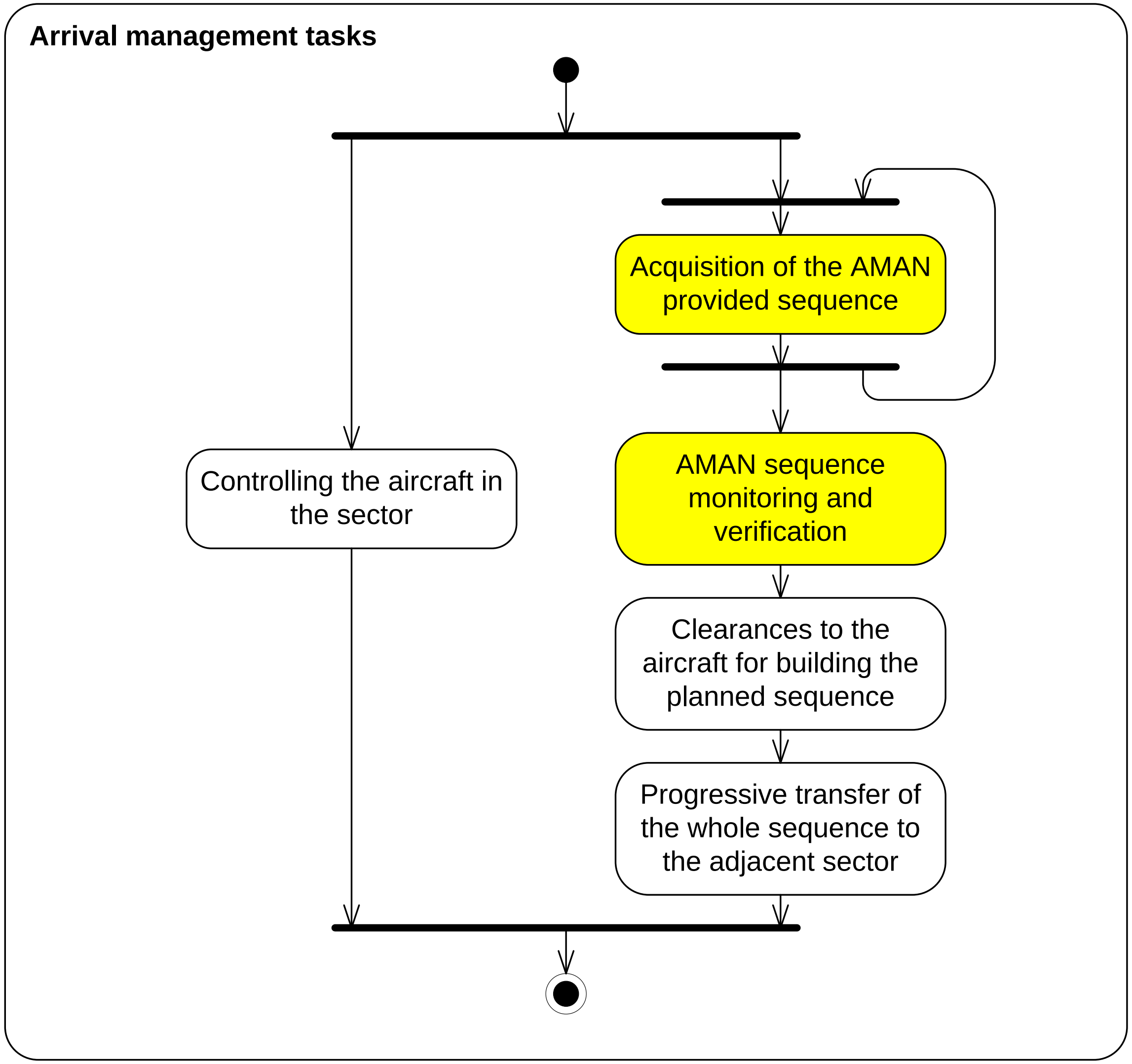
Focus of Analysis

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

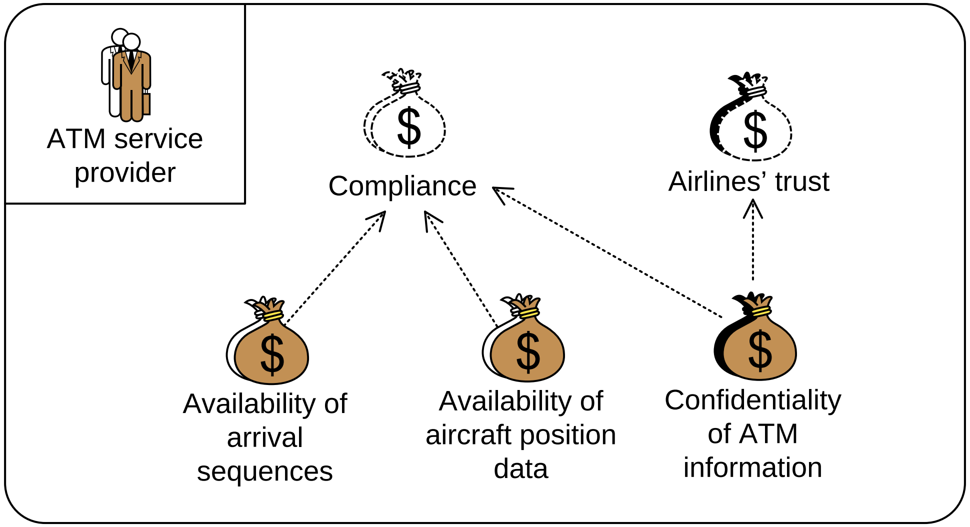
Target Before


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

Target After


Arrival management tasks
Acquisition of the AMAN provided sequence
Controlling the aircraft in the sector
AMAN sequence monitoring and verification
Clearances to the aircraft for building the planned sequence
Progressive transfer of the whole sequence to the adjacent sector

Assets Before-After


ATM service provider
Compliance
Airlines’ trust
Availability of arrival sequences
Availability of aircraft position data
Confidentiality of ATM information

- 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

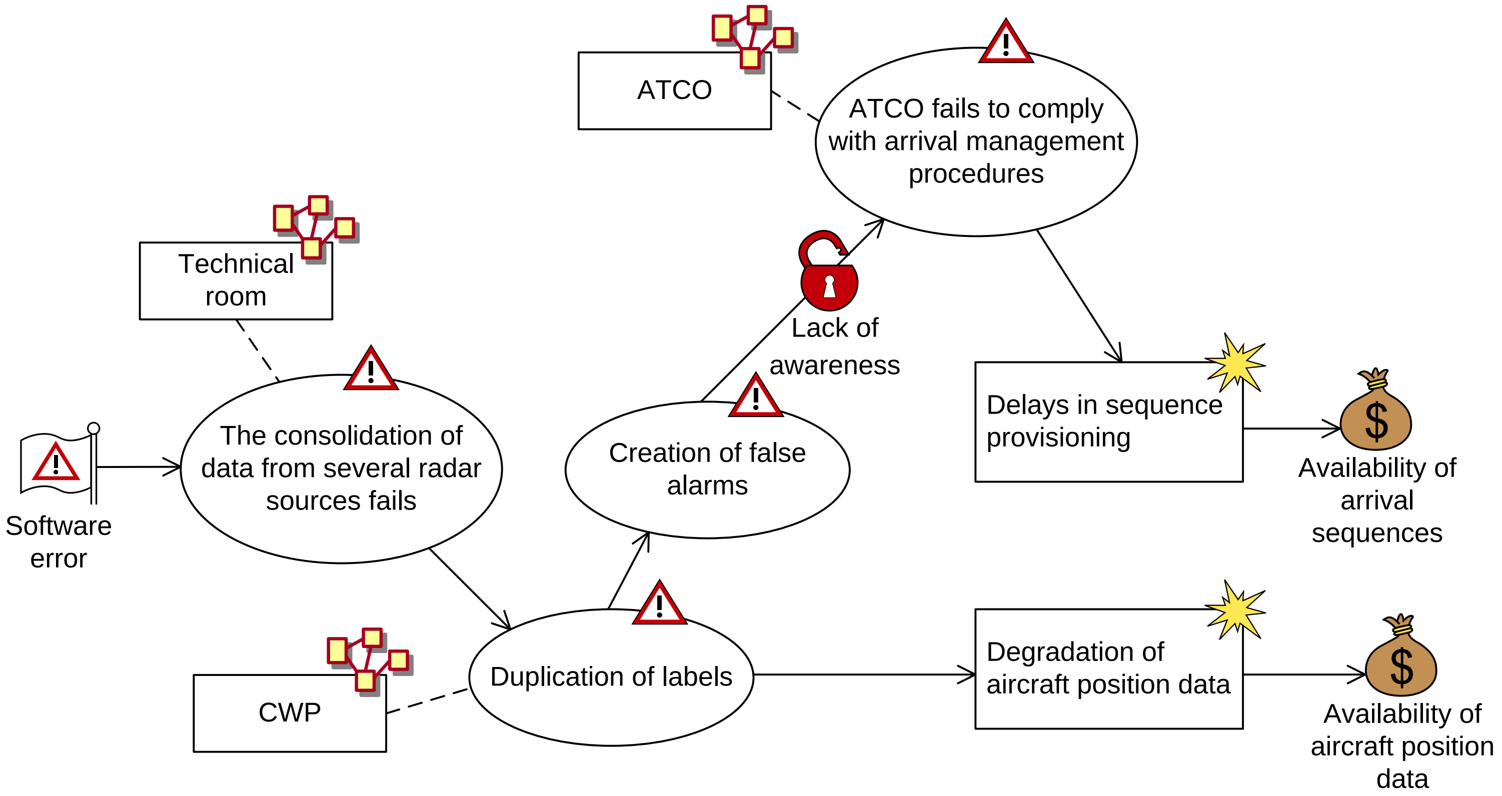
		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Rare	🟩	🟩	🟨	🟨	🟥
	Unlikely	🟩	🟩	🟨	🟨	🟥
	Possible	🟩	🟩	🟨	🟥	🟥
	Likely	🟩	🟨	🟨	🟥	🟥
	Certain	🟩	🟨	🟨	🟥	🟥

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

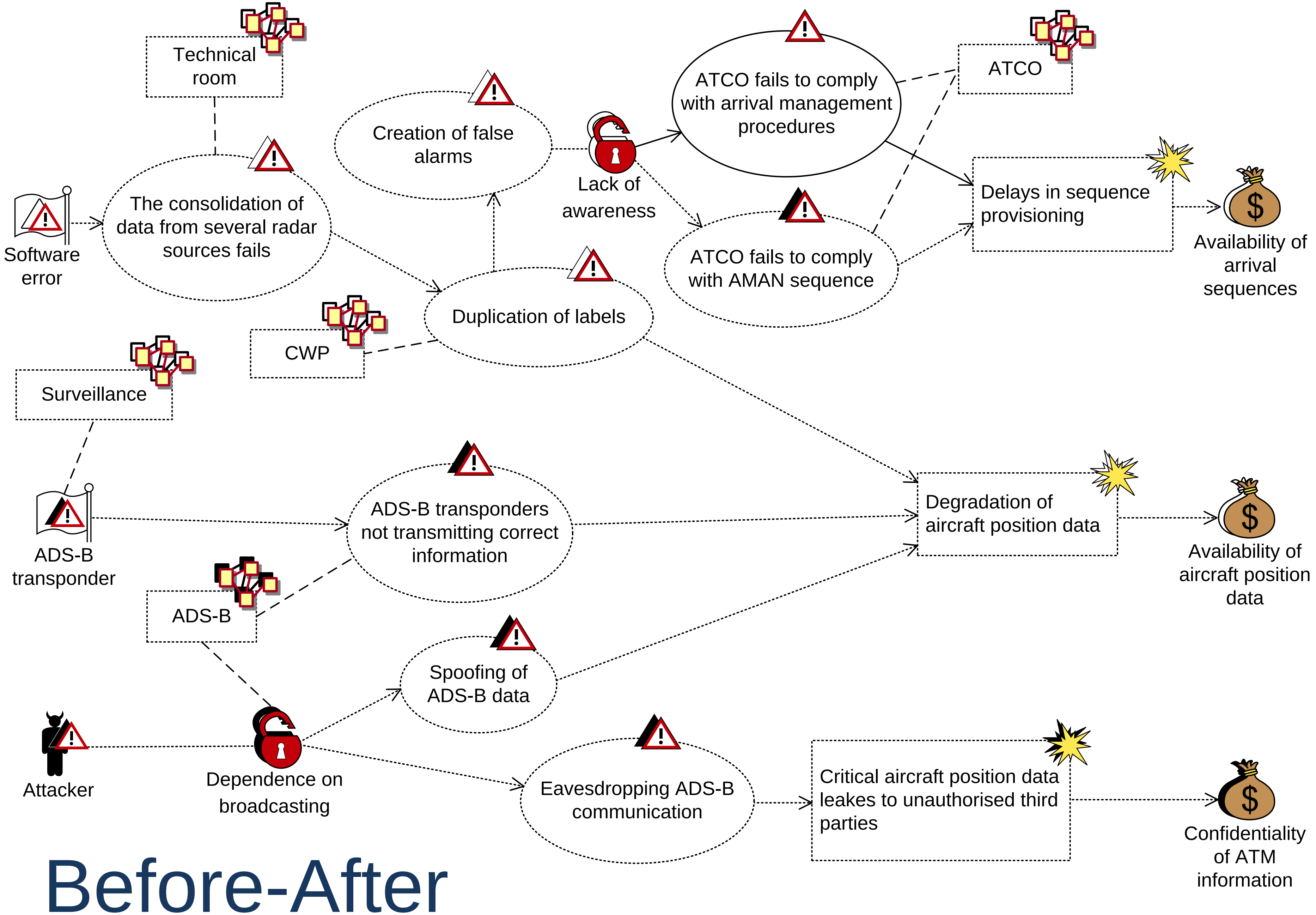
Note: Also the evaluation criteria may change

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
Duplication of labels
CWP
Degradation of aircraft position data
Availability of aircraft position data

Before



Technical room

Software error

The consolidation of data from several radar sources fails

Creation of false alarms

Lack of awareness

ATCO fails to comply with arrival management procedures

ATCO

ATCO fails to comply with AMAN sequence

Delays in sequence provisioning

Availability of arrival sequences

CWP

Duplication of labels

Surveillance

ADS-B transponder

ADS-B transponders not transmitting correct information

Degradation of aircraft position data

Availability of aircraft position data

ADS-B

Spoofing of ADS-B data

Attacker

Dependence on broadcasting

Eavesdropping ADS-B communication

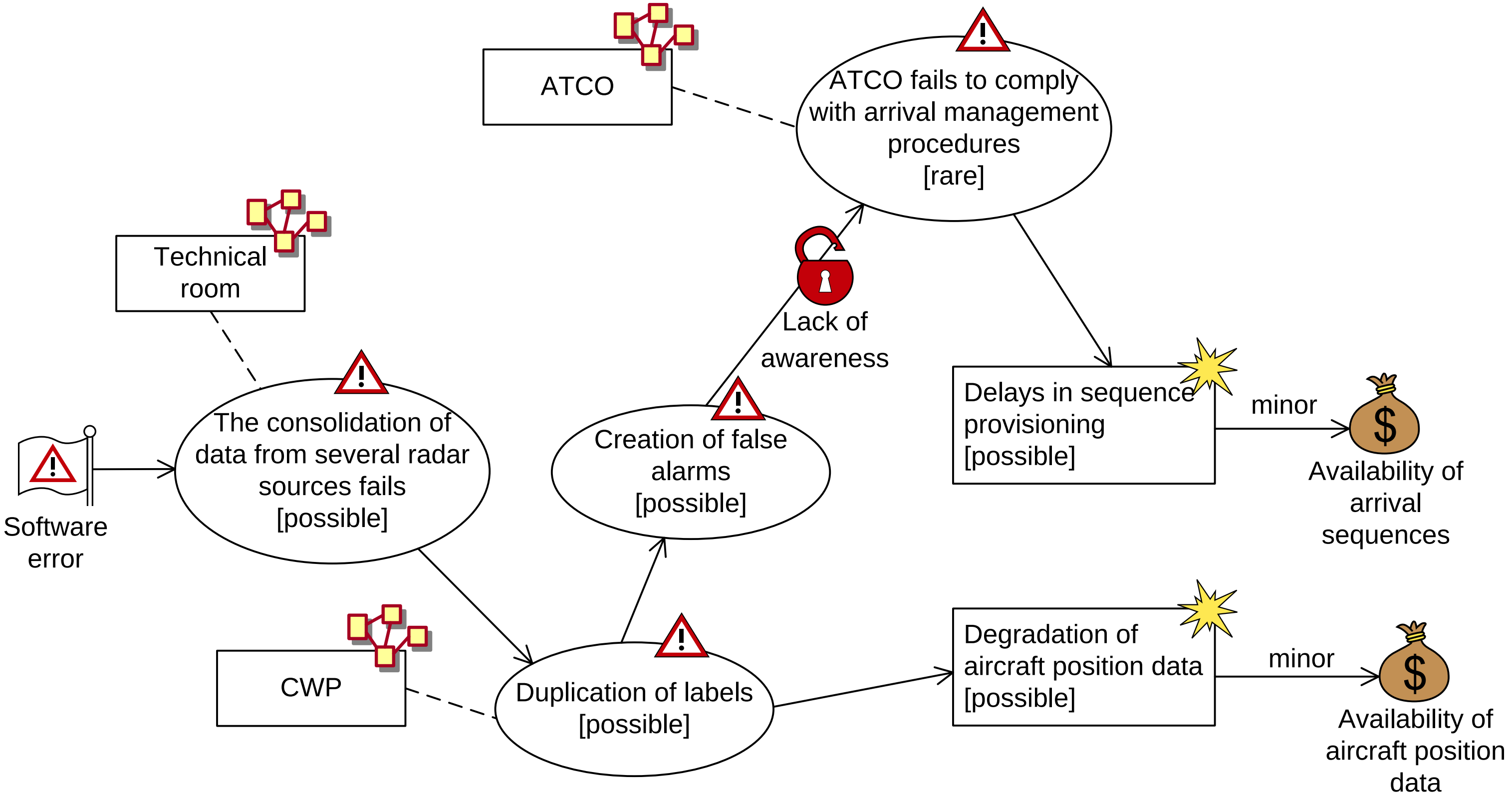
Critical aircraft position data leakes to unauthorised third parties

Confidentiality of ATM information

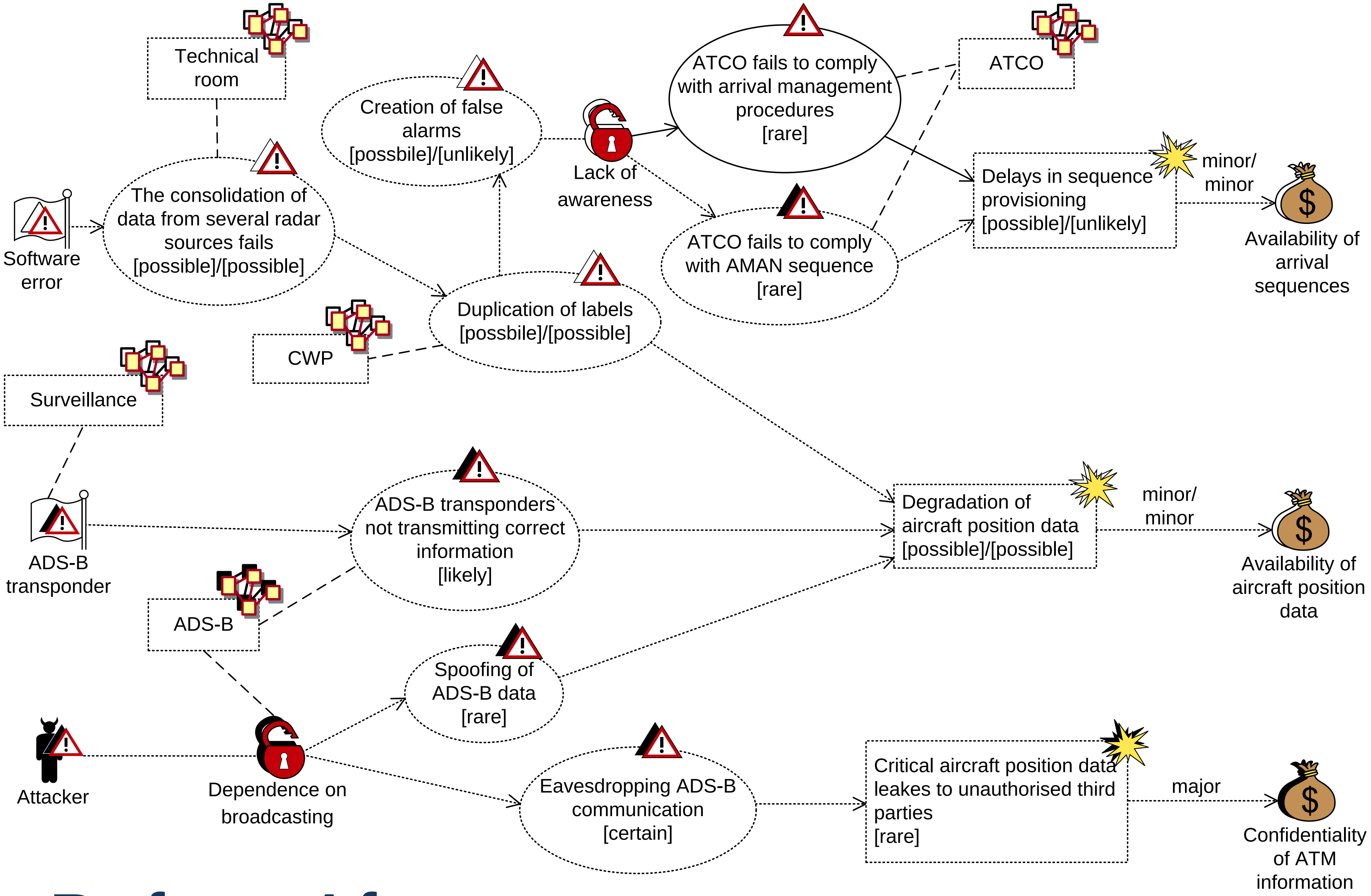
Before-After

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



Technical room

Creation of false alarms [possbile]/[unlikely]

ATCO fails to comply with arrival management procedures [rare]

ATCO

Software error

The consolidation of data from several radar sources fails [possible]/[possible]

Lack of awareness

Delays in sequence provisioning [possible]/[unlikely]

minor/ minor

Availability of arrival sequences

ATCO fails to comply with AMAN sequence [rare]

CWP

Duplication of labels [possbile]/[possible]

Surveillance

ADS-B transponders not transmitting correct information [likely]

Degradation of aircraft position data [possible]/[possible]

minor/ minor

Availability of aircraft position data

ADS-B transponder

ADS-B

Spoofing of ADS-B data [rare]

Attacker

Dependence on broadcasting

Eavesdropping ADS-B communication [certain]

Critical aircraft position data leakes to unauthorised third parties [rare]

major

Confidentiality of ATM information

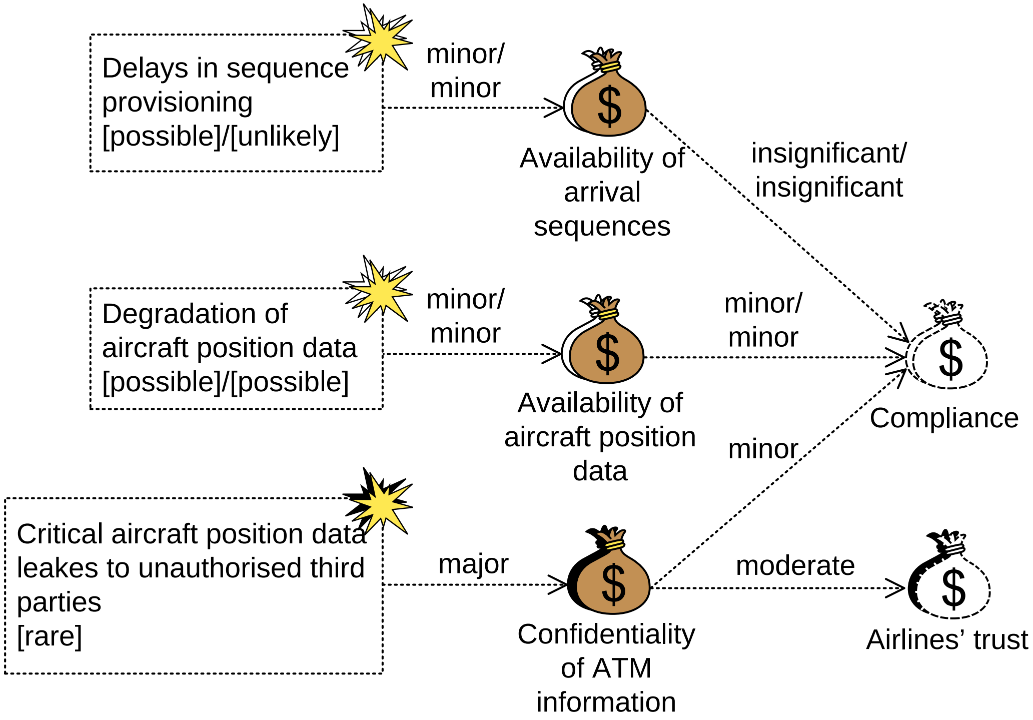
Before-After

Risk Evaluation

CORAS Step 7

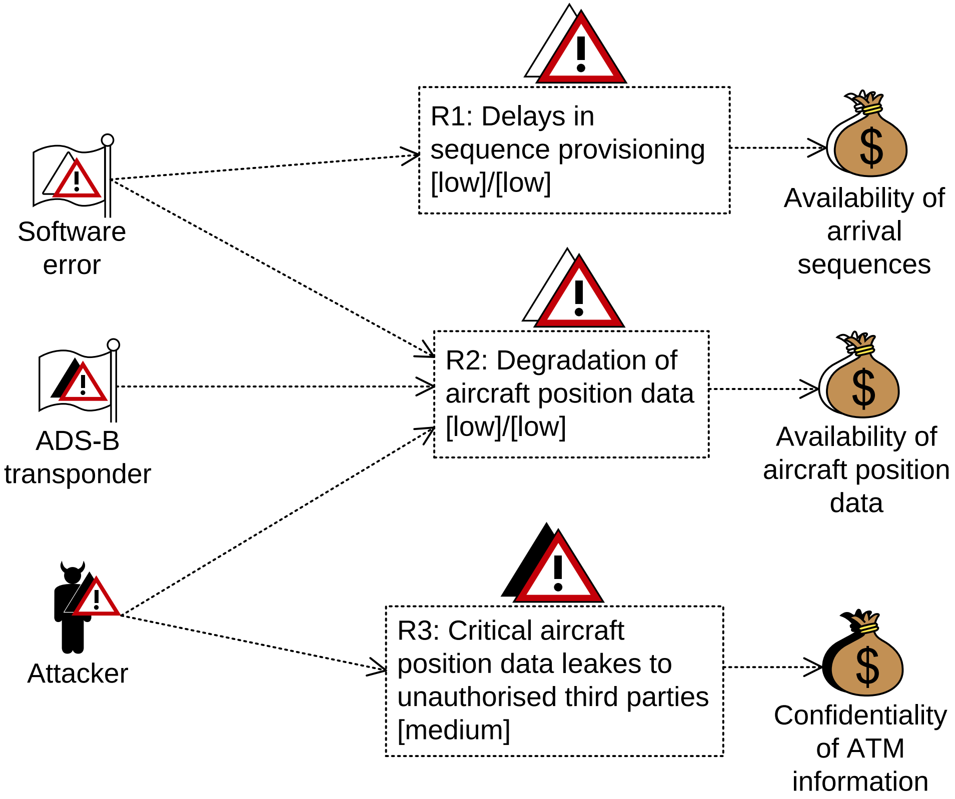
Indirect Assets

- Before-After


Delays in sequence provisioning [possible]/[unlikely]
minor/ minor
Availability of arrival sequences
insignificant/ insignificant
Degradation of aircraft position data [possible]/[possible]
minor/ minor
Availability of aircraft position data
minor/ minor
Compliance
minor
Critical aircraft position data leakes to unauthorised third parties [rare]
major
Confidentiality of ATM information
moderate
Airlines' trust

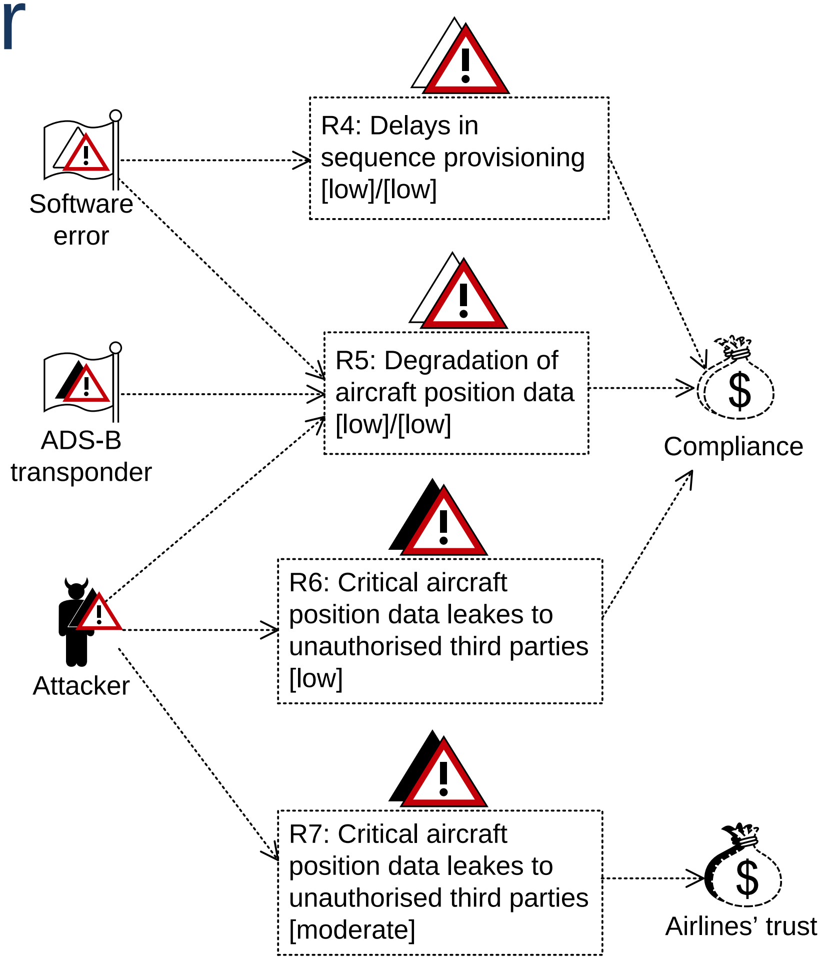
Risk Diagram

- Before-After


Software error
ADS-B transponder
Attacker
R1: Delays in sequence provisioning [low]/[low]
R2: Degradation of aircraft position data [low]/[low]
R3: Critical aircraft position data leakes to unauthorised third parties [medium]
$
Availability of arrival sequences
$
Availability of aircraft position data
$
Confidentiality of ATM information

Risk Diagram

- Before-After


Software error
ADS-B transponder
Attacker
R4: Delays in sequence provisioning [low]/[low]
R5: Degradation of aircraft position data [low]/[low]
R6: Critical aircraft position data leakes to unauthorised third parties [low]
R7: Critical aircraft position data leakes to unauthorised third parties [moderate]
Compliance
Airlines' trust

Risk Evaluation

Consequence

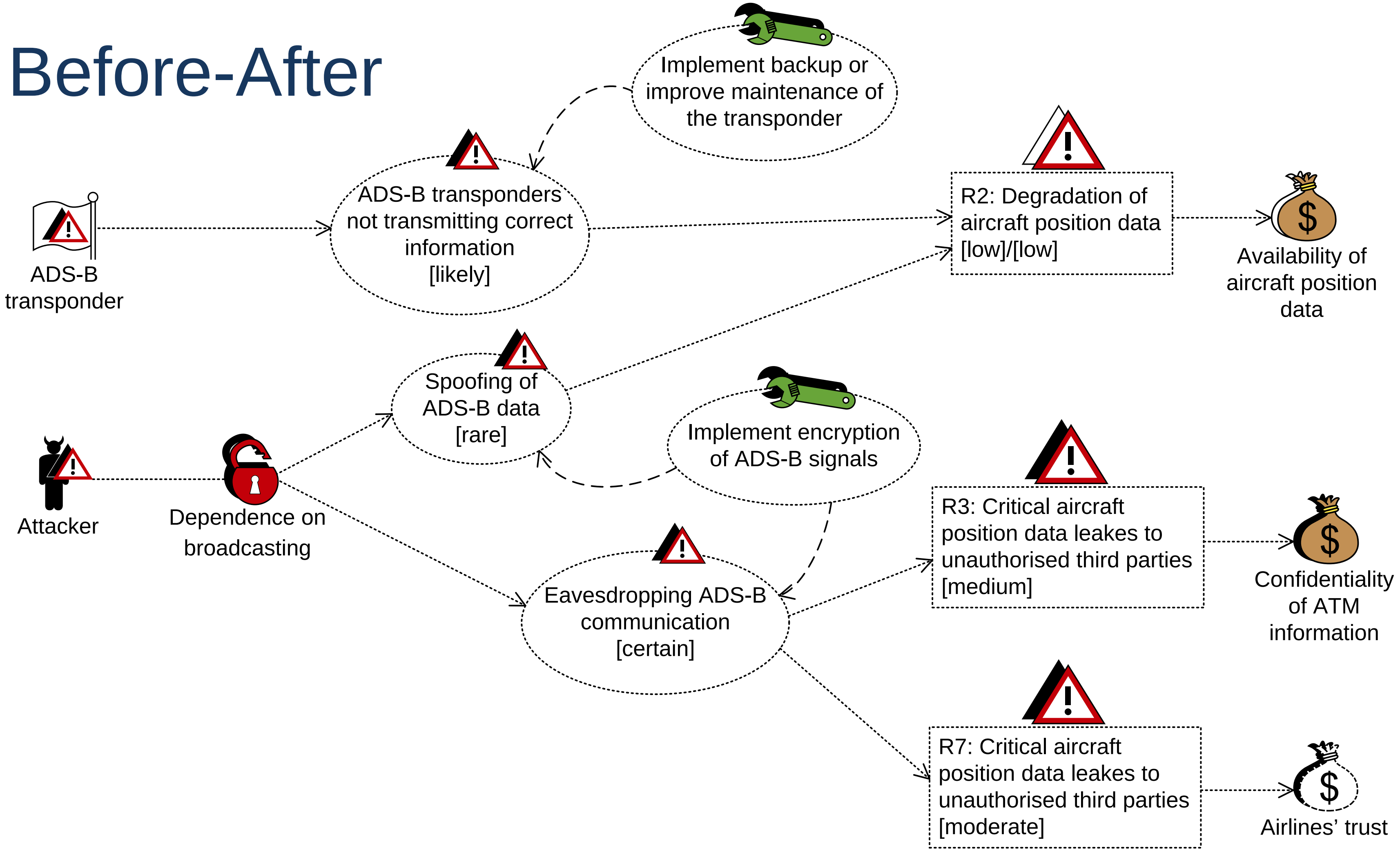
Likelihood

	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


Implement backup or improve maintenance of the transponder
ADS-B transponder
ADS-B transponders not transmitting correct information [likely]
R2: Degradation of aircraft position data [low]/[low]
Availability of aircraft position data
Spoofing of ADS-B data [rare]
Implement encryption of ADS-B signals
Attacker
Dependence on broadcasting
R3: Critical aircraft position data leakes to unauthorised third parties [medium]
Confidentiality of ATM information
Eavesdropping ADS-B communication [certain]
R7: Critical aircraft position data leakes to unauthorised third parties [moderate]
Airlines’ trust