Security Risk Assessment IV

Before-After

Ketil Stølen

Overview

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

Readings:

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

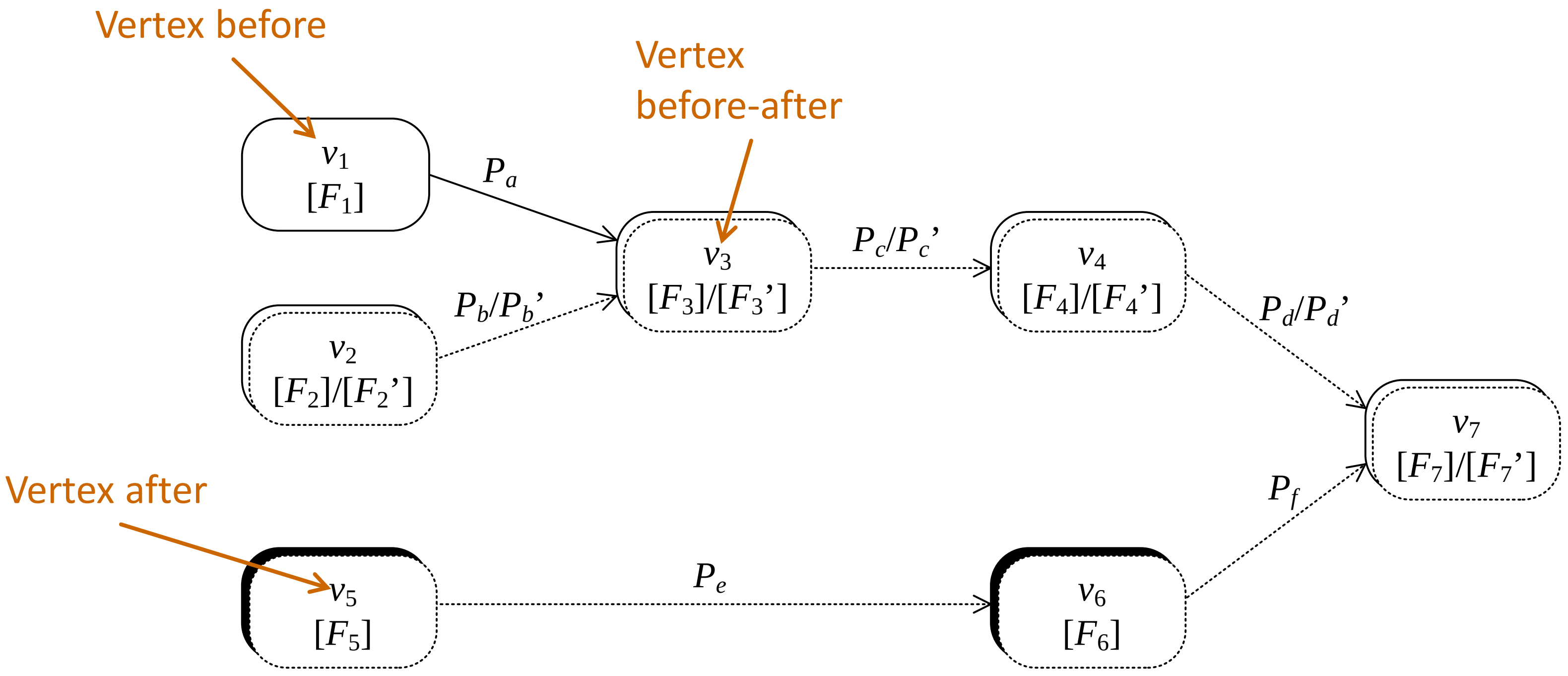
Three Perspectives on Change

- The maintenance perspective
- The before-after perspective
- The continuous evolution perspective

Before-After

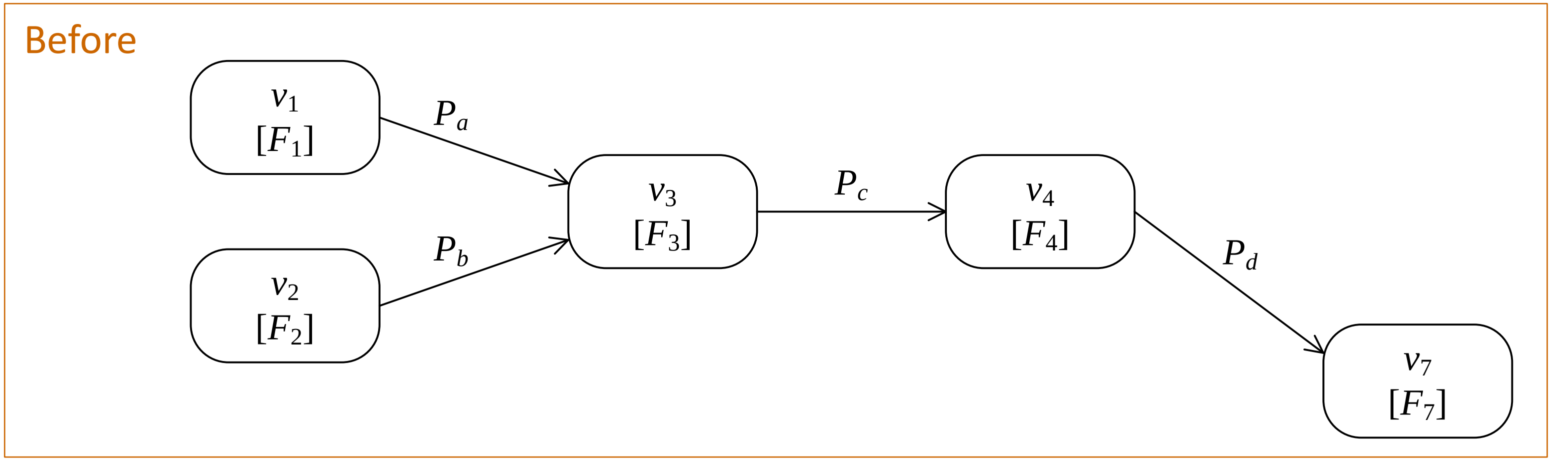
In this lecture and in this course we will cover only the before-after perspective

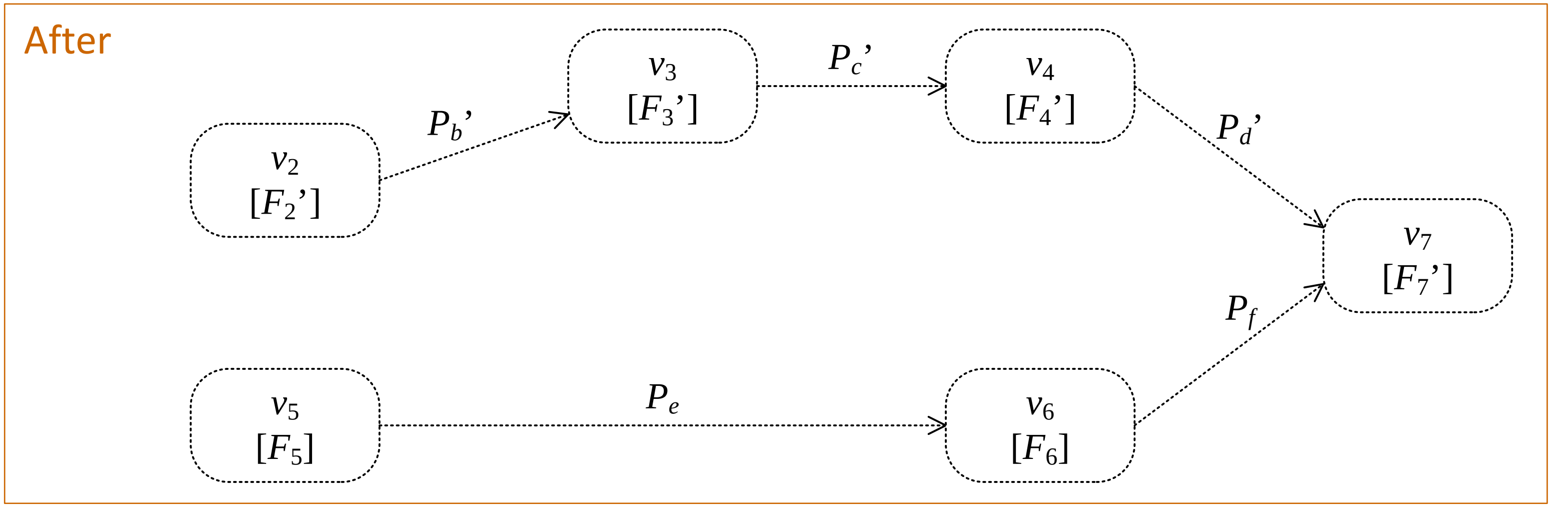
Risk Graphs with **Before-After**



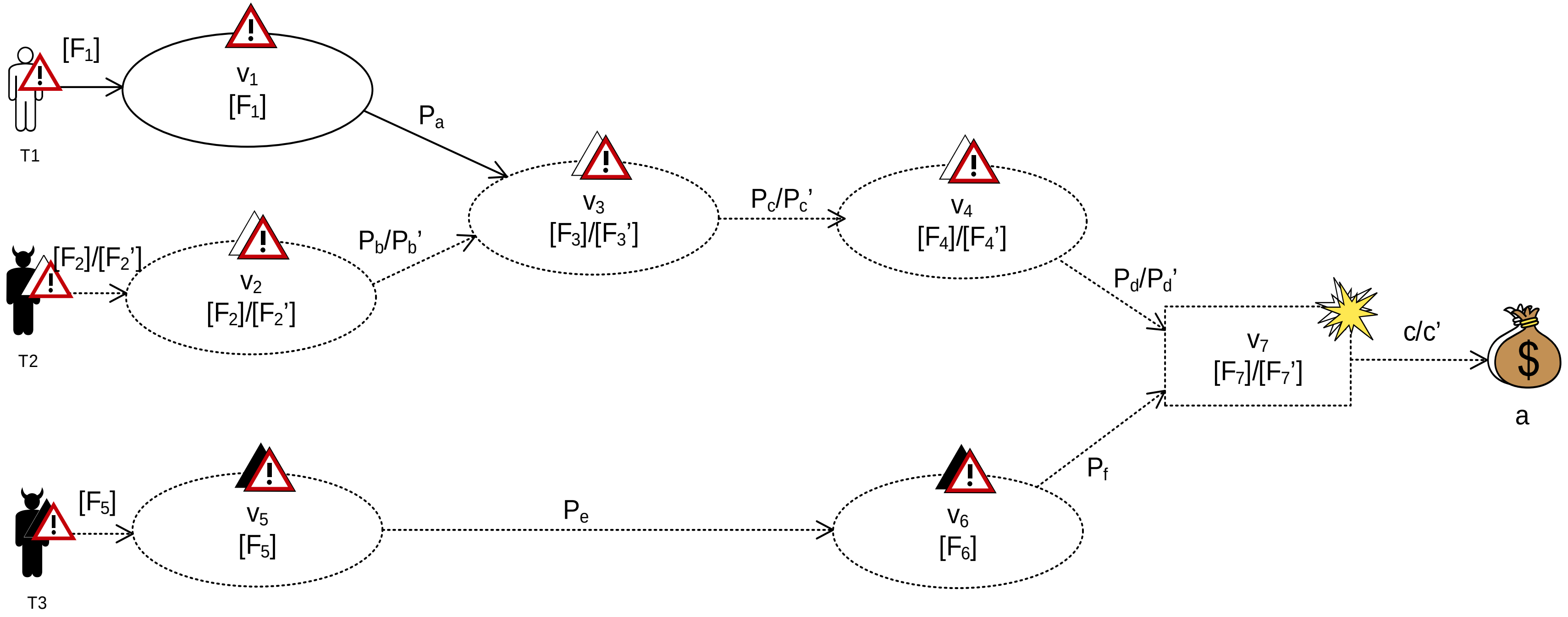
- Explicit modeling of
  - Elements before change
  - Elements after change
  - Changes in likelihood estimates

Two Views on Risk Graphs with **Before-After**





CORAS Instantiation of **Before-After**



We will in the following update the ATM example from the lectures Security Risk Assessment I and II to cover **Before-After**

The ATM models and diagrams in the slides from Security Risk Assessment I and II correspond to the Before View

Before-After view on ATM

Before

- 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

After

- Introduction of new information systems and decision support systems
- Reorganization of services

Target of Analysis: **Before-After**

Before: Arrival management and the role of air traffic controllers (ATCOs) in the area control centre (ACC)

After: 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-After**

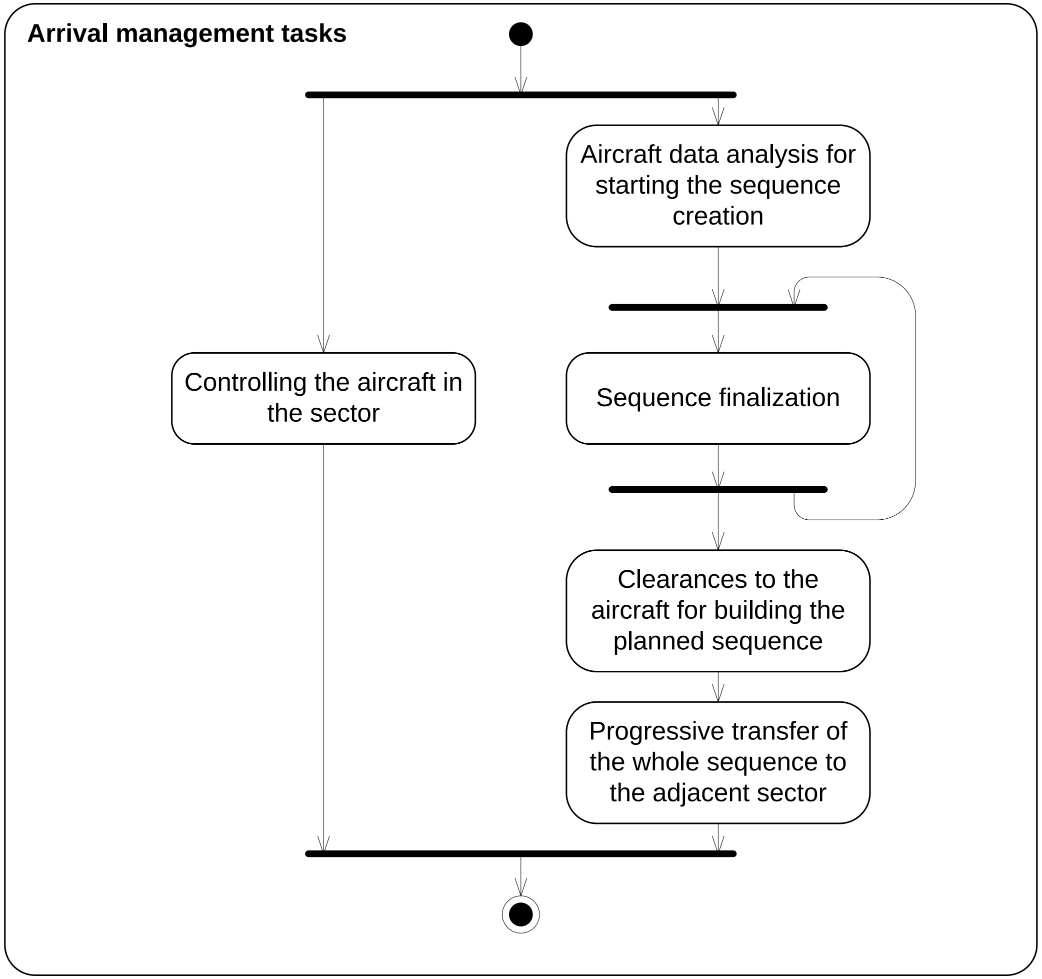
Before:

- Information provision (availability)
- Compliance with regulation

After: Additional concerns

- Information protection (confidentiality)

Target **Before** (exemplified by an activity diagram)



Arrival management tasks

Aircraft data analysis for starting the sequence creation

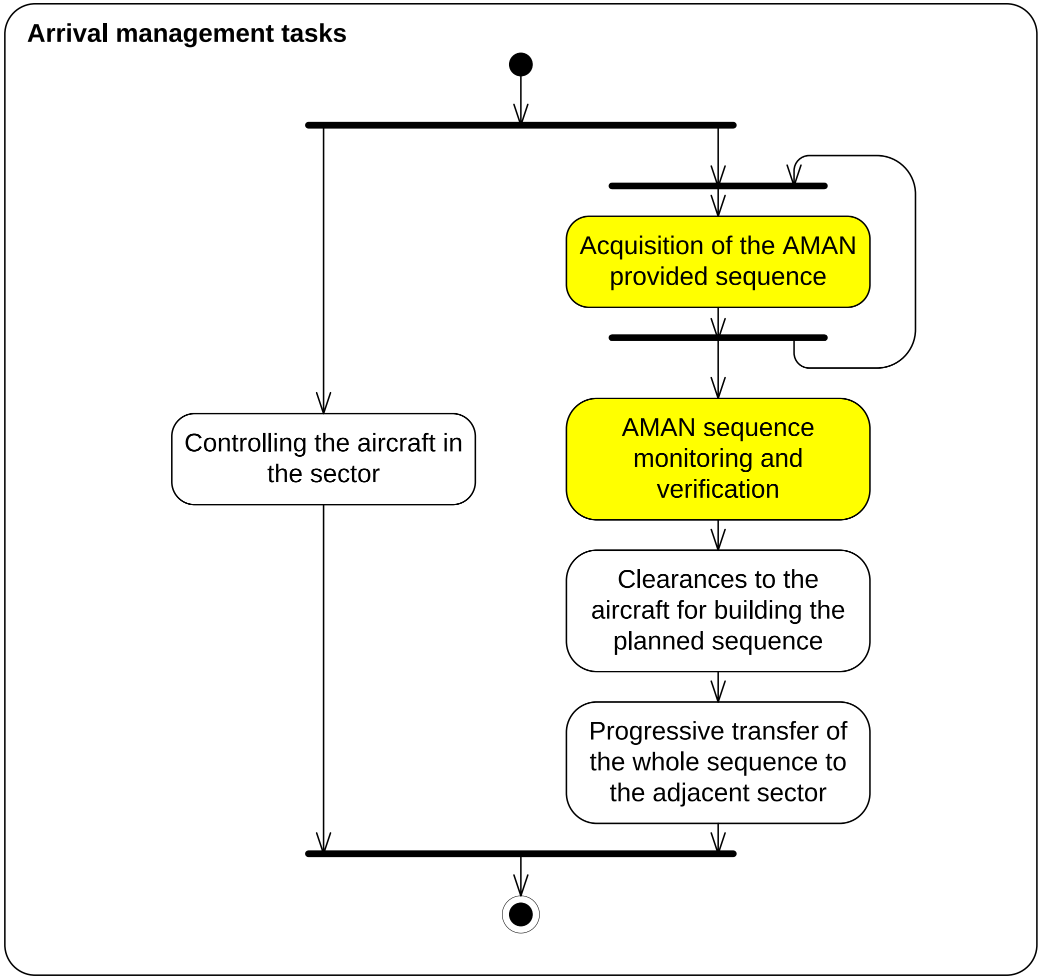
Controlling the aircraft in the sector

Sequence finalization

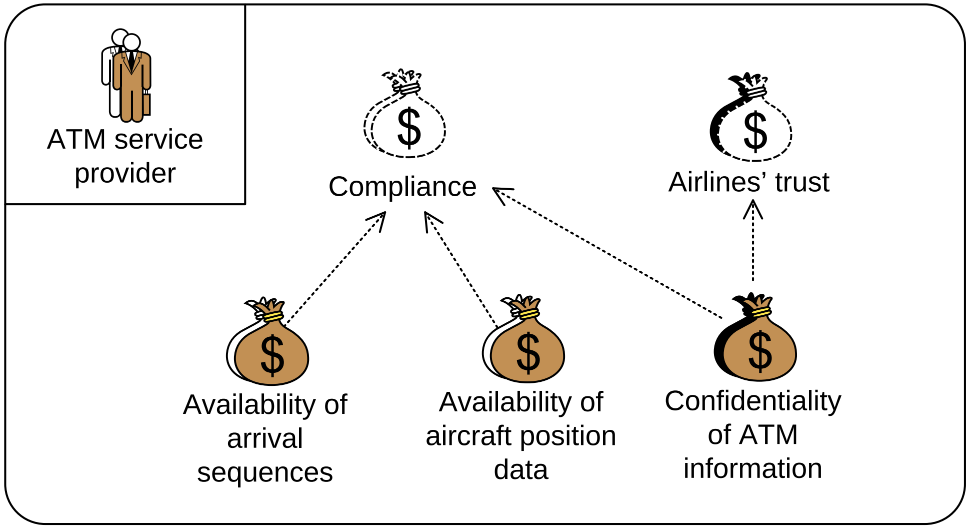
Clearances to the aircraft for building the planned sequence

Progressive transfer of the whole sequence to the adjacent sector

Target **After** (exemplified by updated activity diagram)


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

Update of Asset-diagram to **Before-After**


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

- Direct asset Confidentiality of ATM information is considered only after changes
- Indirect asset Airlines’ trust is considered only after changes
- The rest is unchanged between Before and After

Consequence Scales

Confidentiality (New scale)

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 (Unchanged)

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 - Unchanged

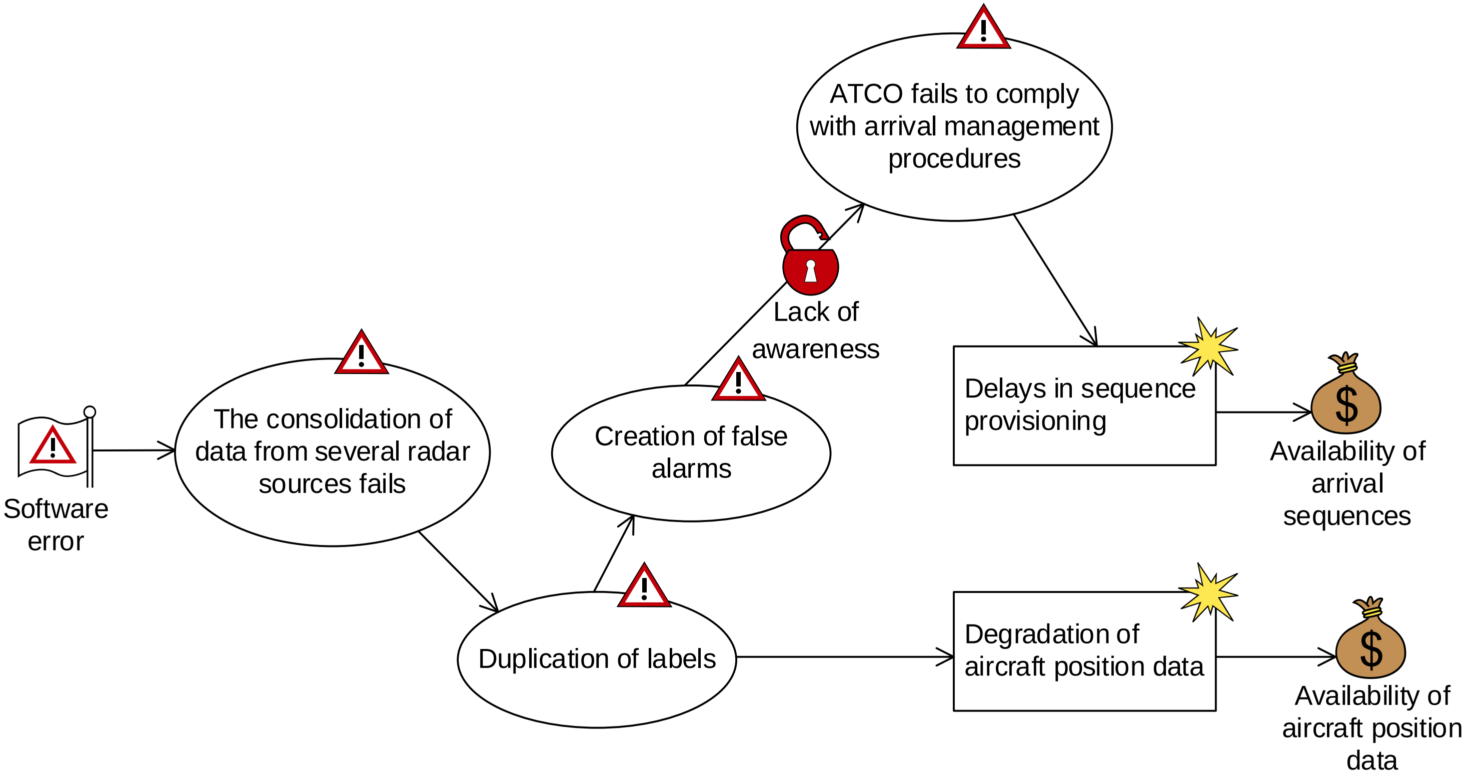
Likelihood	Description
Certain	A very high number of similar occurrences already on record; has occurred a very high number of times at the same location/time
Likely	A significant number of similar occurrences already on record; has occurred a significant number of times at the same location
Possible	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 - Unchanged

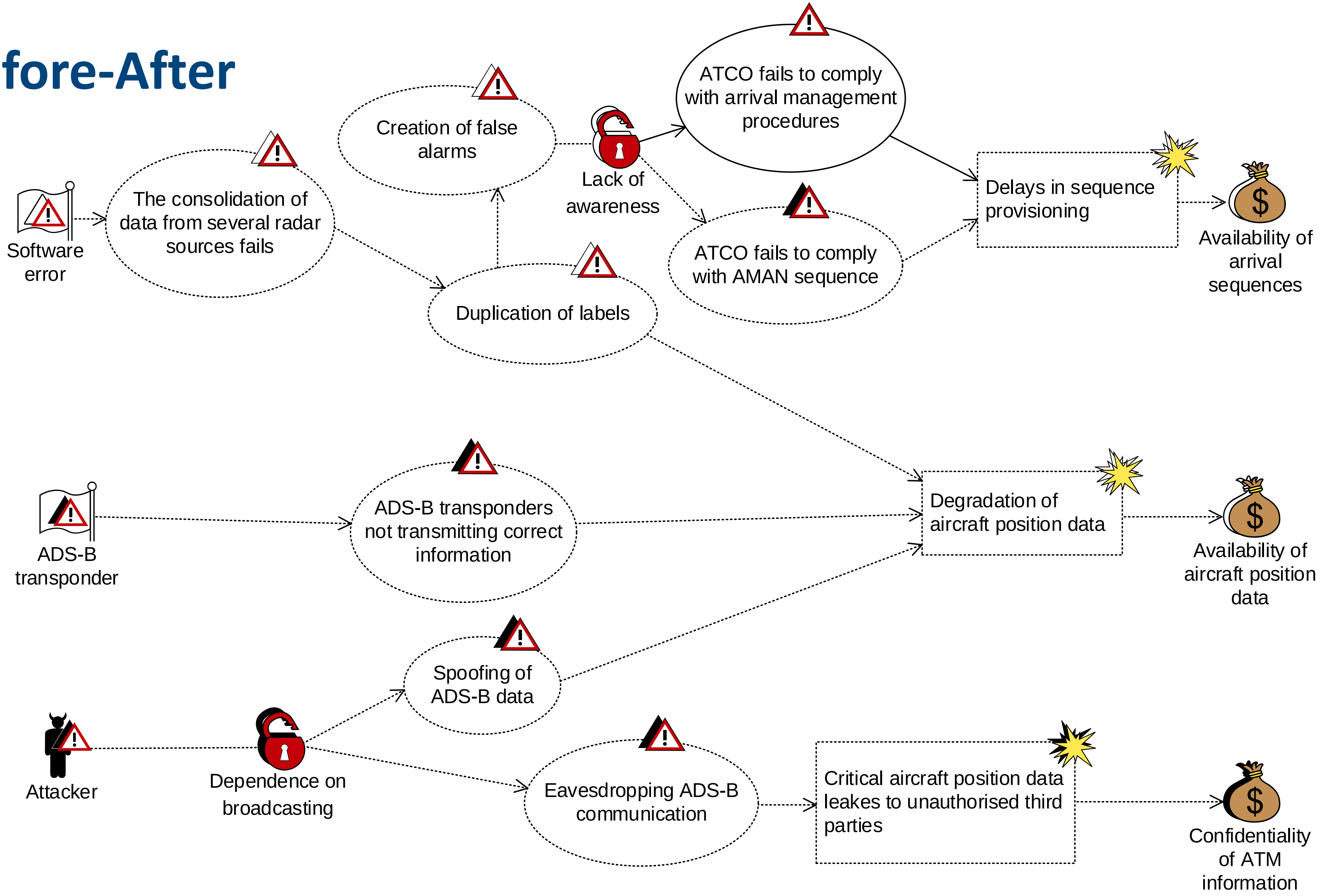
				Consequence		
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Rare	🟩	🟩	🟨	🟨	🟥
	Unlikely	🟩	🟩	🟨	🟨	🟥
	Possible	🟩	🟩	🟨	🟥	🟥
	Likely	🟩	🟨	🟨	🟥	🟥
	Certain	🟩	🟨	🟨	🟥	🟥

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

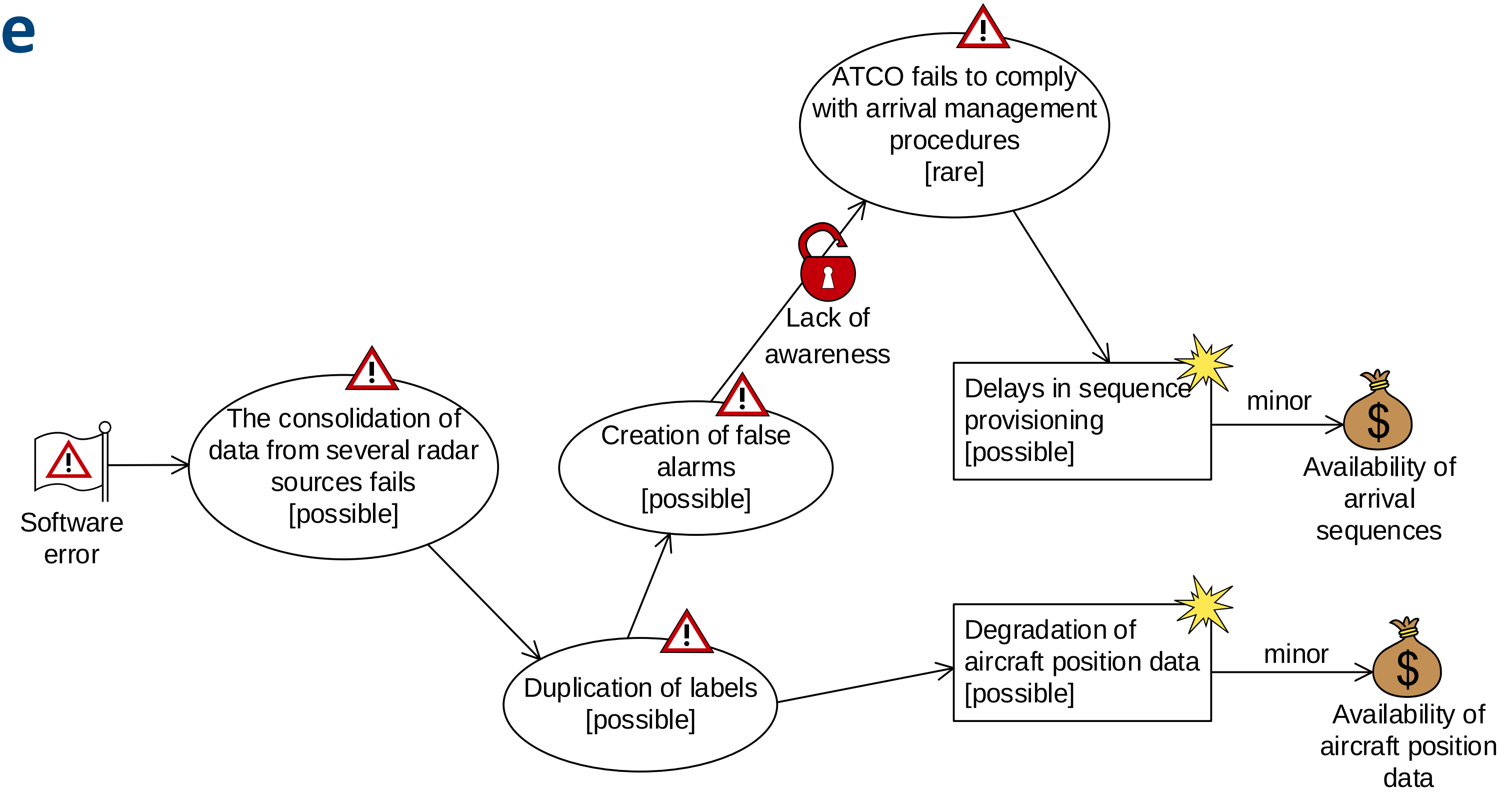
Before


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

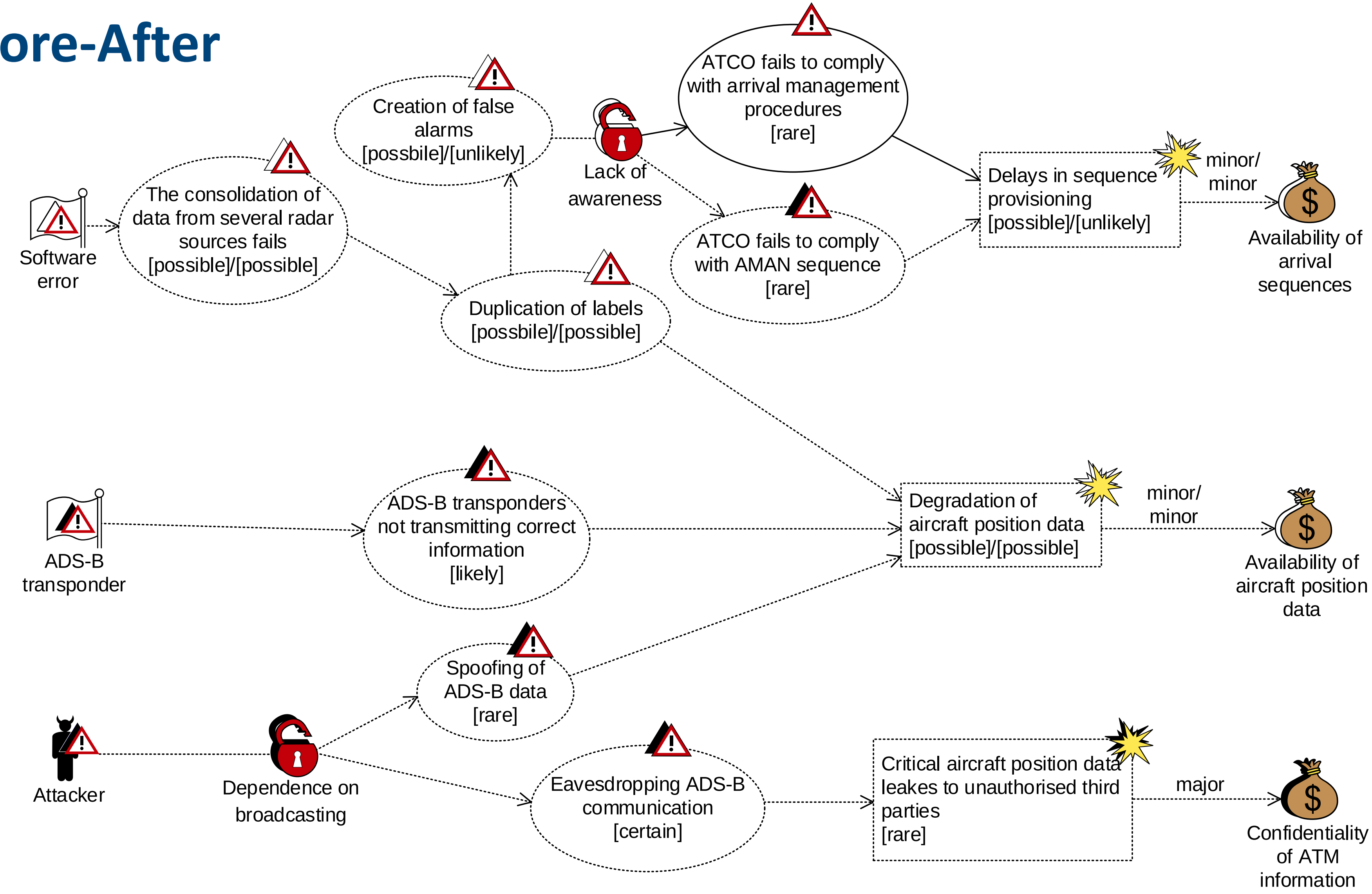
Before-After


Software error
The consolidation of data from several radar sources fails
Creation of false alarms
Duplication of labels
Lack of awareness
ATCO fails to comply with arrival management procedures
ATCO fails to comply with AMAN sequence
Delays in sequence provisioning
Availability of arrival sequences
ADS-B transponder
ADS-B transponders not transmitting correct information
Degradation of aircraft position data
Availability of aircraft position data
Attacker
Dependence on broadcasting
Spoofing of ADS-B data
Eavesdropping ADS-B communication
Critical aircraft position data leakes to unauthorised third parties
Confidentiality of ATM information

Before


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

Before-After


Software error
The consolidation of data from several radar sources fails [possible]/[possible]
Creation of false alarms [possbile]/[unlikely]
Duplication of labels [possbile]/[possible]
Lack of awareness
ATCO fails to comply with arrival management procedures [rare]
ATCO fails to comply with AMAN sequence [rare]
Delays in sequence provisioning [possible]/[unlikely]
minor/ minor
Availability of arrival sequences
ADS-B transponder
ADS-B transponders not transmitting correct information [likely]
Degradation of aircraft position data [possible]/[possible]
minor/ minor
Availability of aircraft position data
Attacker
Dependence on broadcasting
Spoofing of ADS-B data [rare]
Eavesdropping ADS-B communication [certain]
Critical aircraft position data leakes to unauthorised third parties [rare]
major
Confidentiality of ATM information
$
$
$

SINTEF

Technology for a better society

Risk Evaluation: Before-After

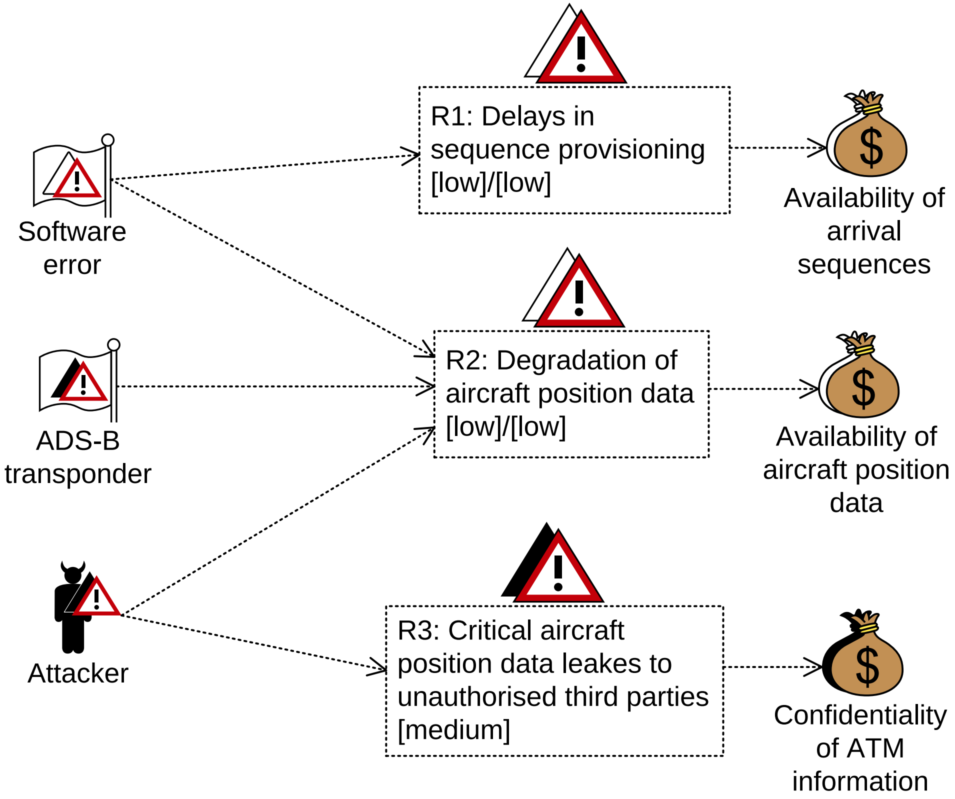
Consequence

Likelihood

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

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

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]

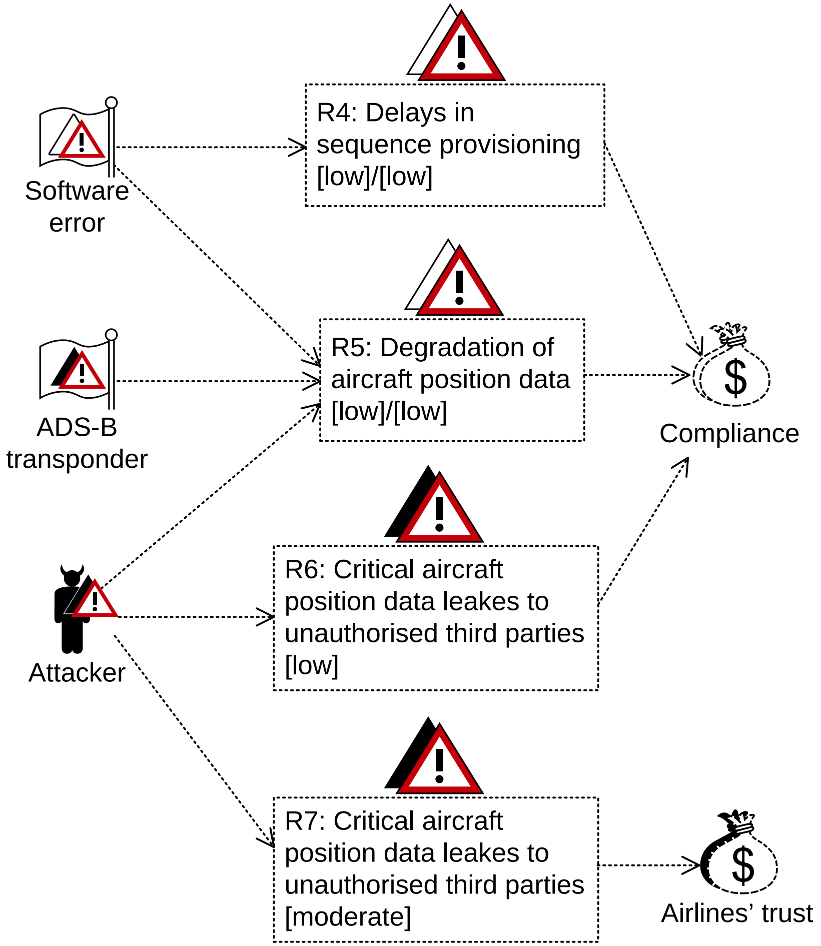
R3: Critical aircraft position data leakes to unauthorised third parties [medium]

Availability of arrival sequences

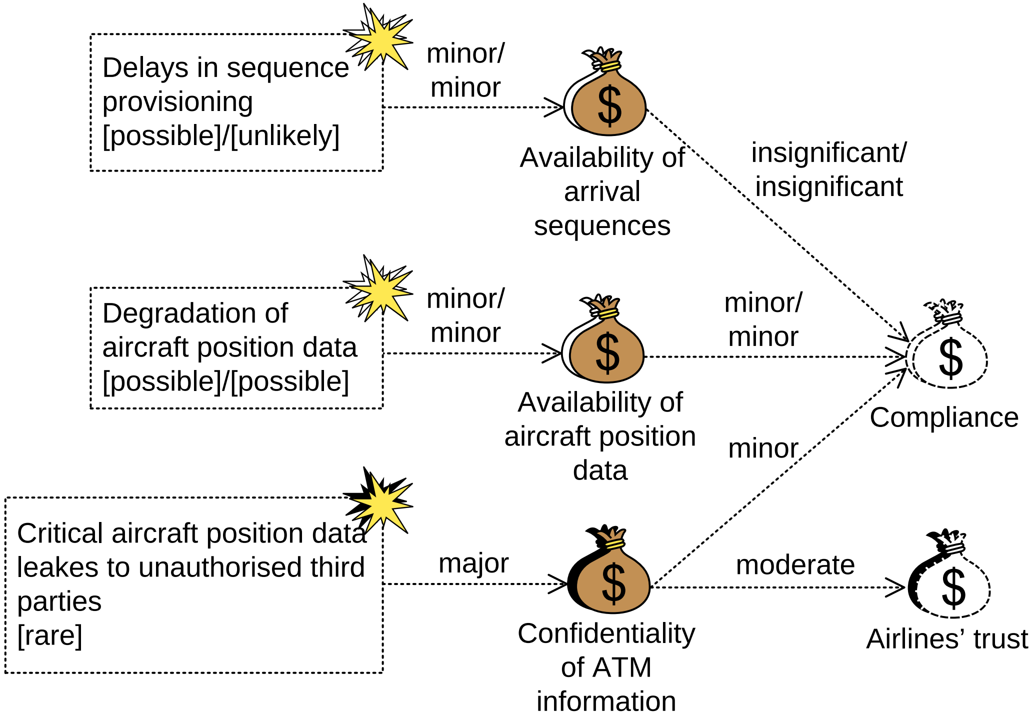
Availability of aircraft position data

Confidentiality of ATM information

Risk Diagram: **Before-After**


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

Risk wrt 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]

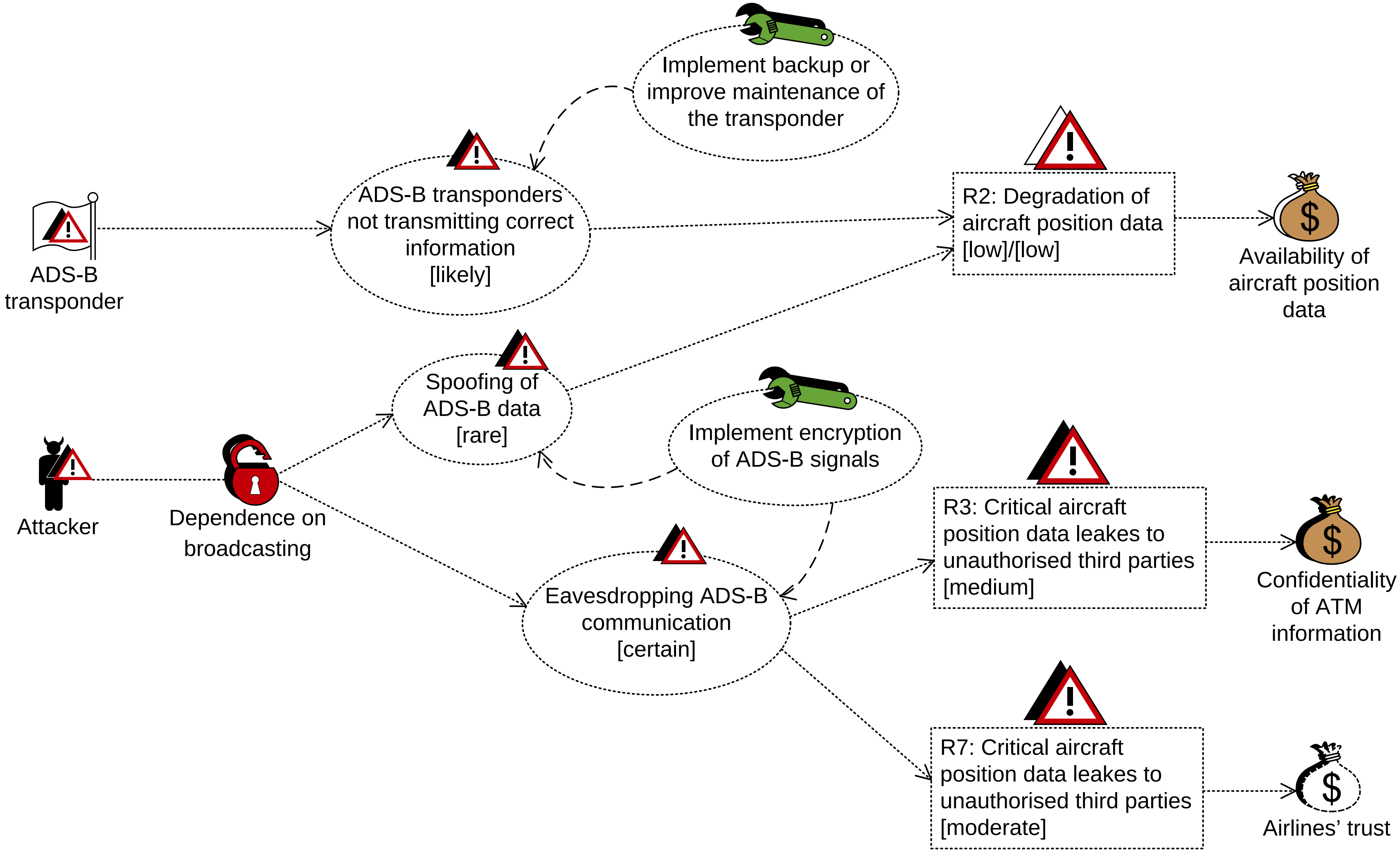
major

Confidentiality of ATM information

moderate

Airlines’ trust

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