

Security Risk Assessment

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>

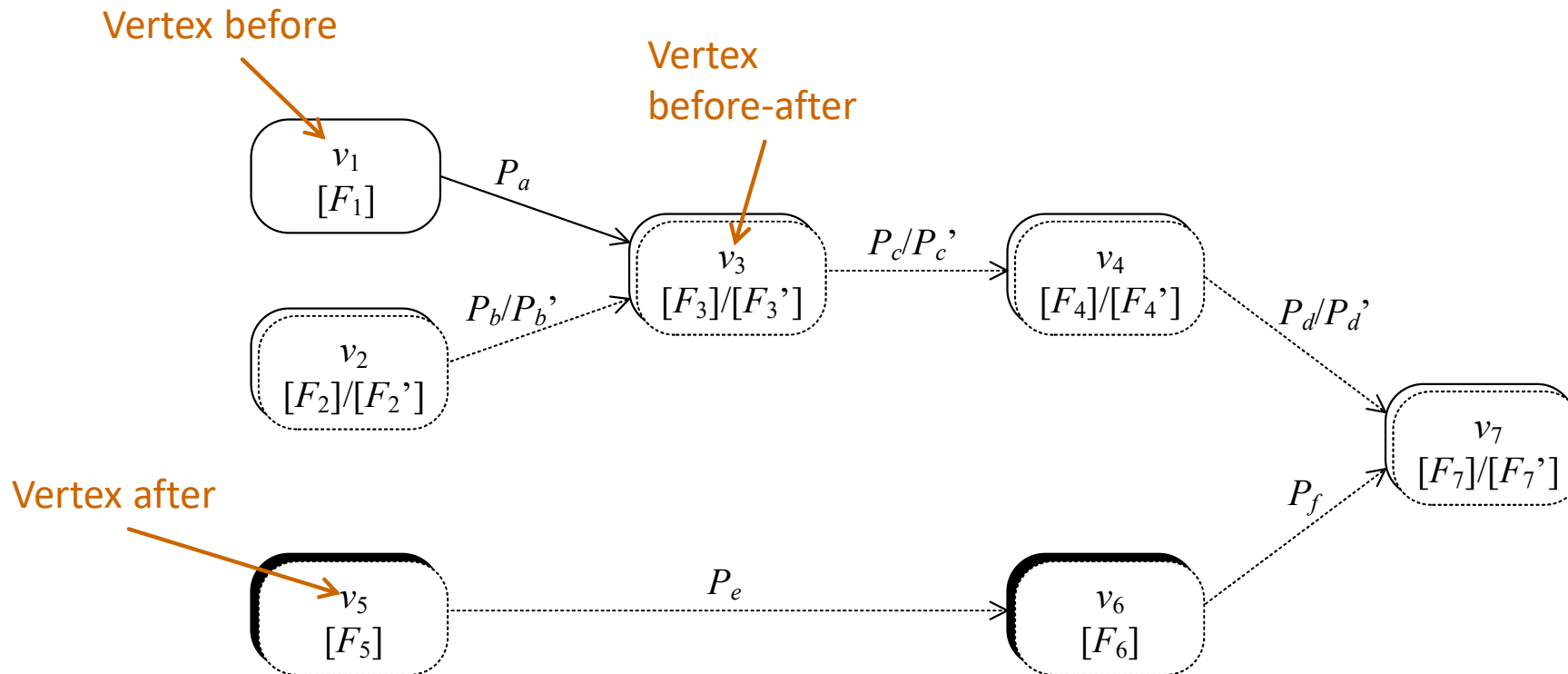
Three Perspectives on Change

- 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

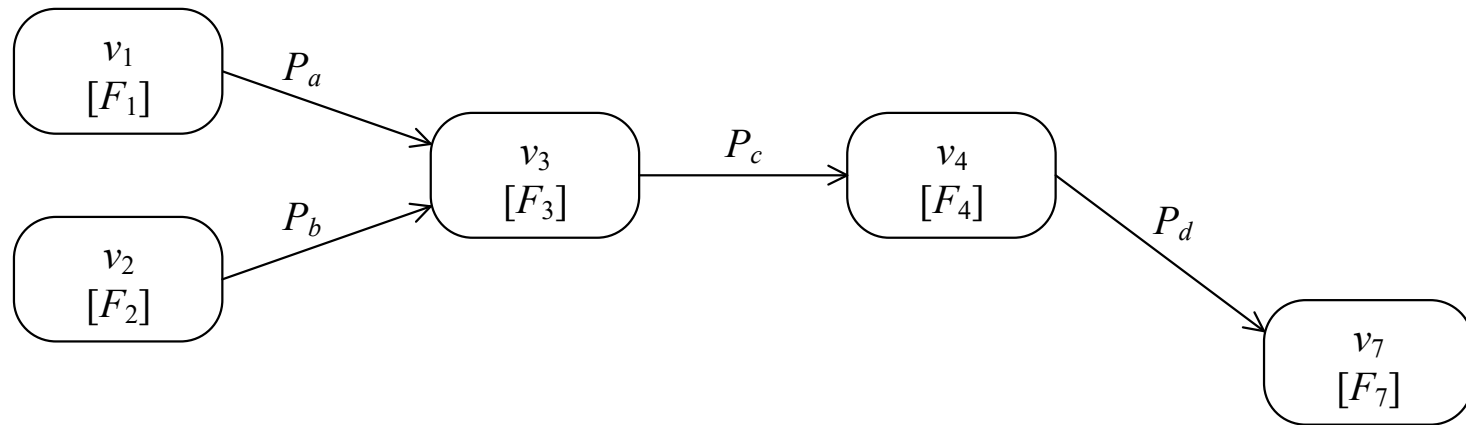
Risk Graphs with Before-After



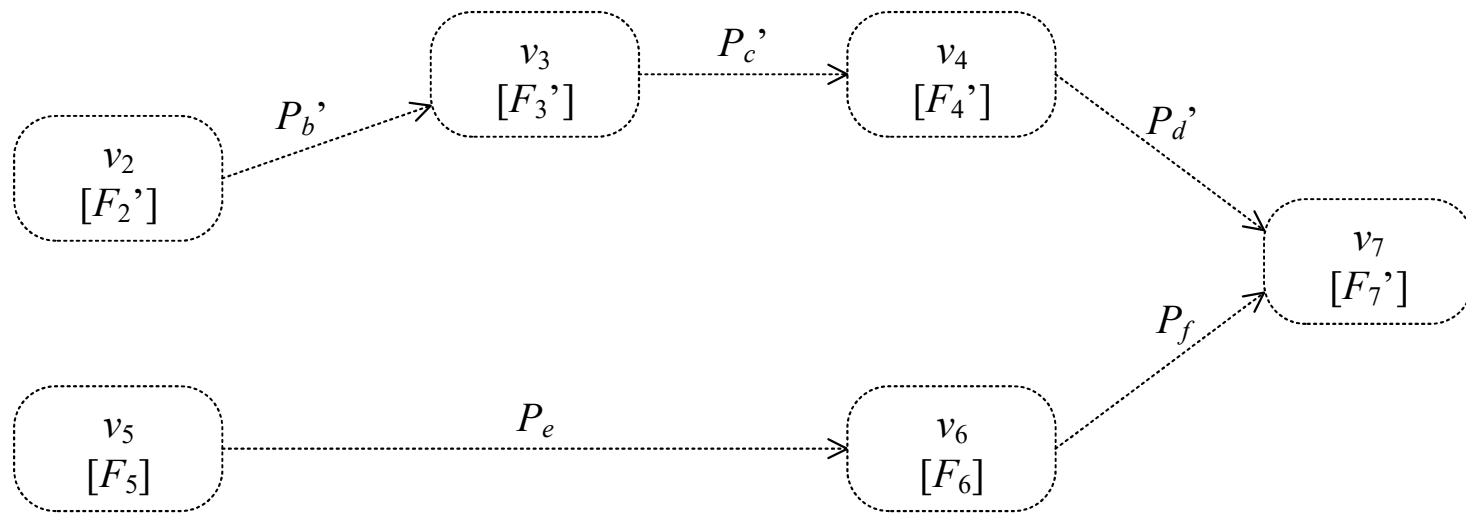
- Explicit modeling of
 - Elements before change
 - Elements after change
 - Changes in likelihood estimates

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

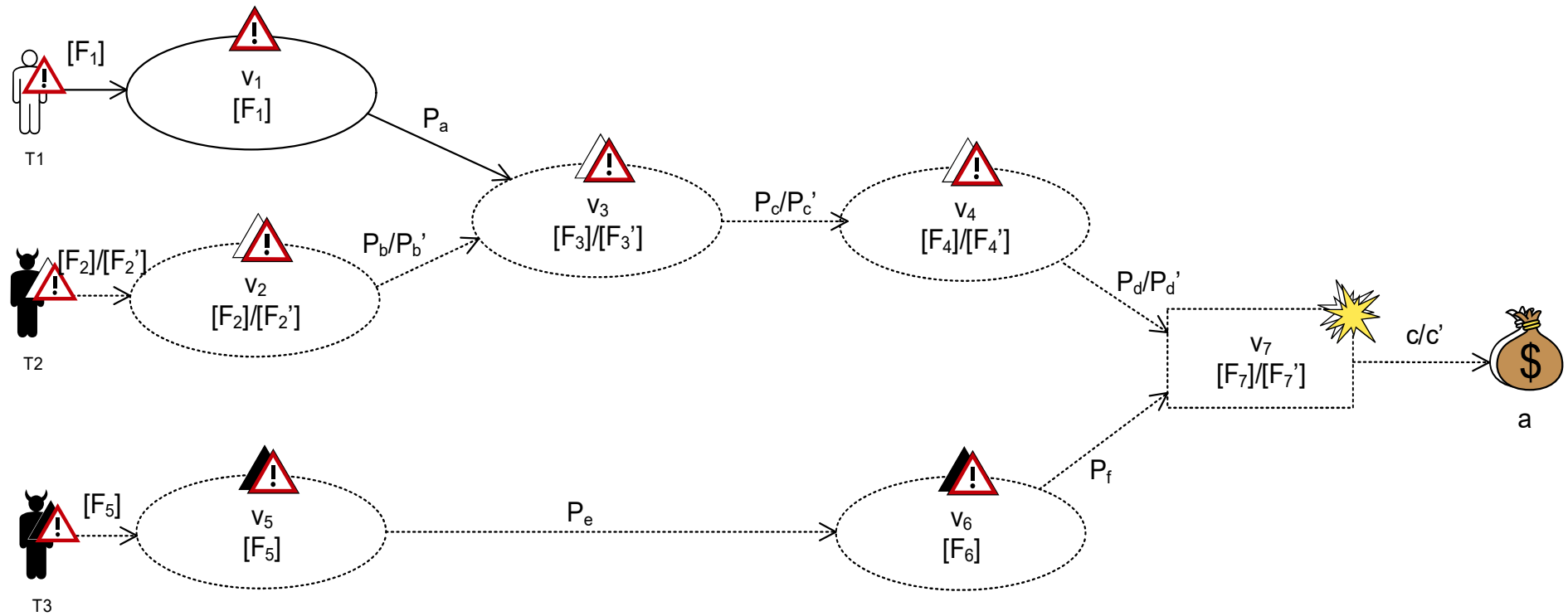
Before



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**

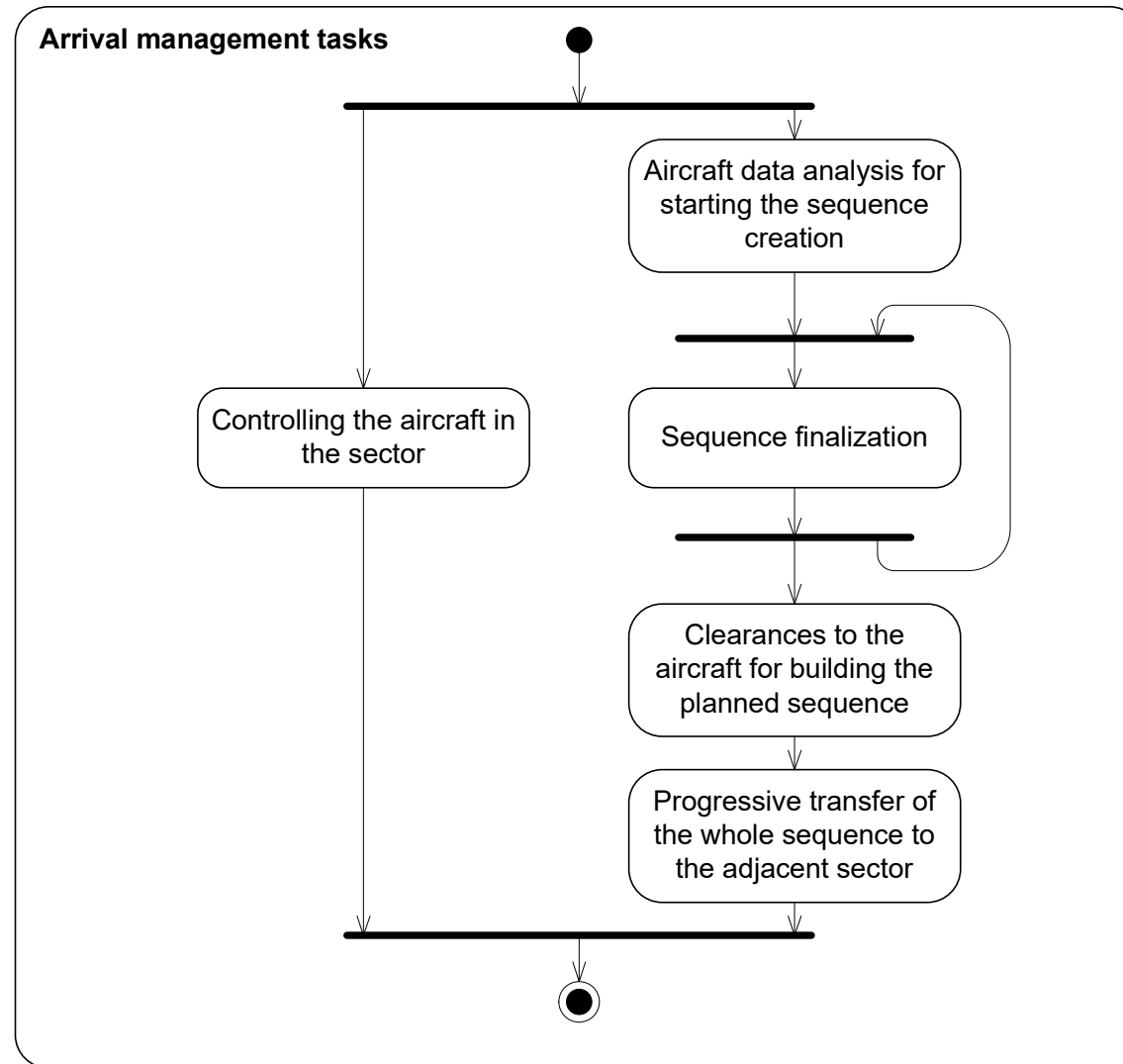
Before:

- Information provision (availability)
- Compliance with regulation

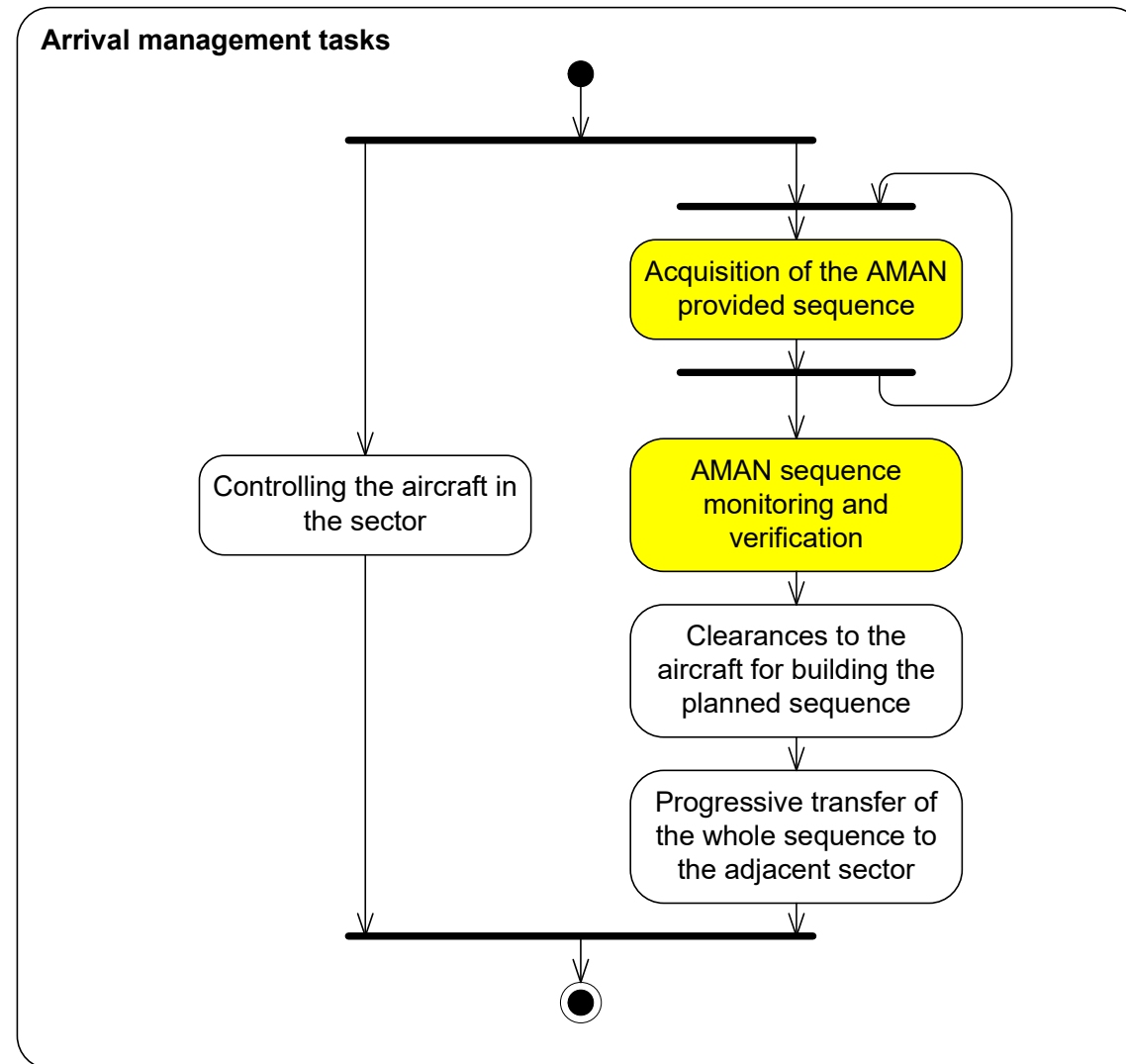
After: Additional concerns

- Information protection (confidentiality)

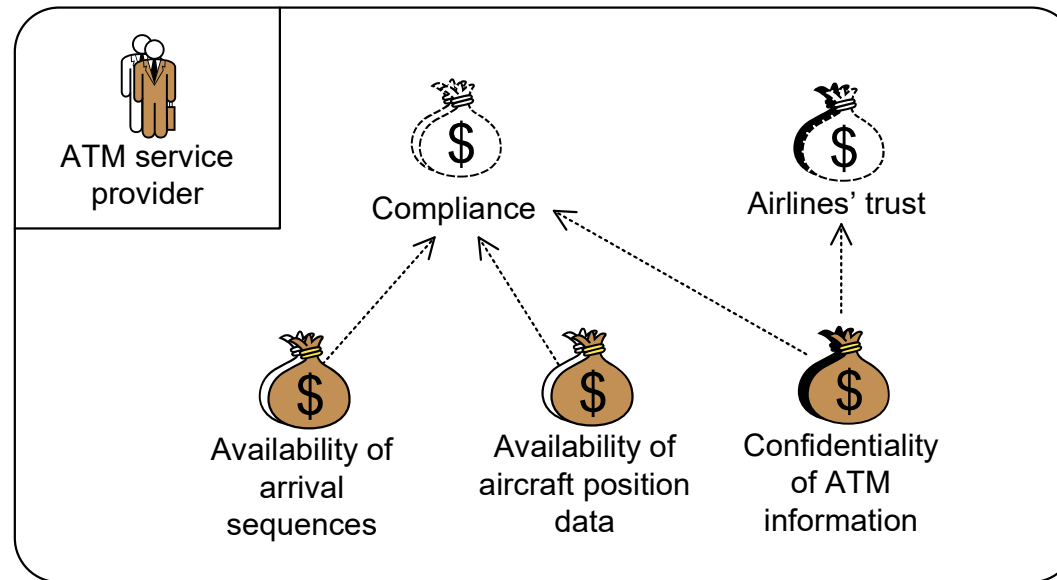
Target **Before** (exemplified by an activity diagram)



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



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



- 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

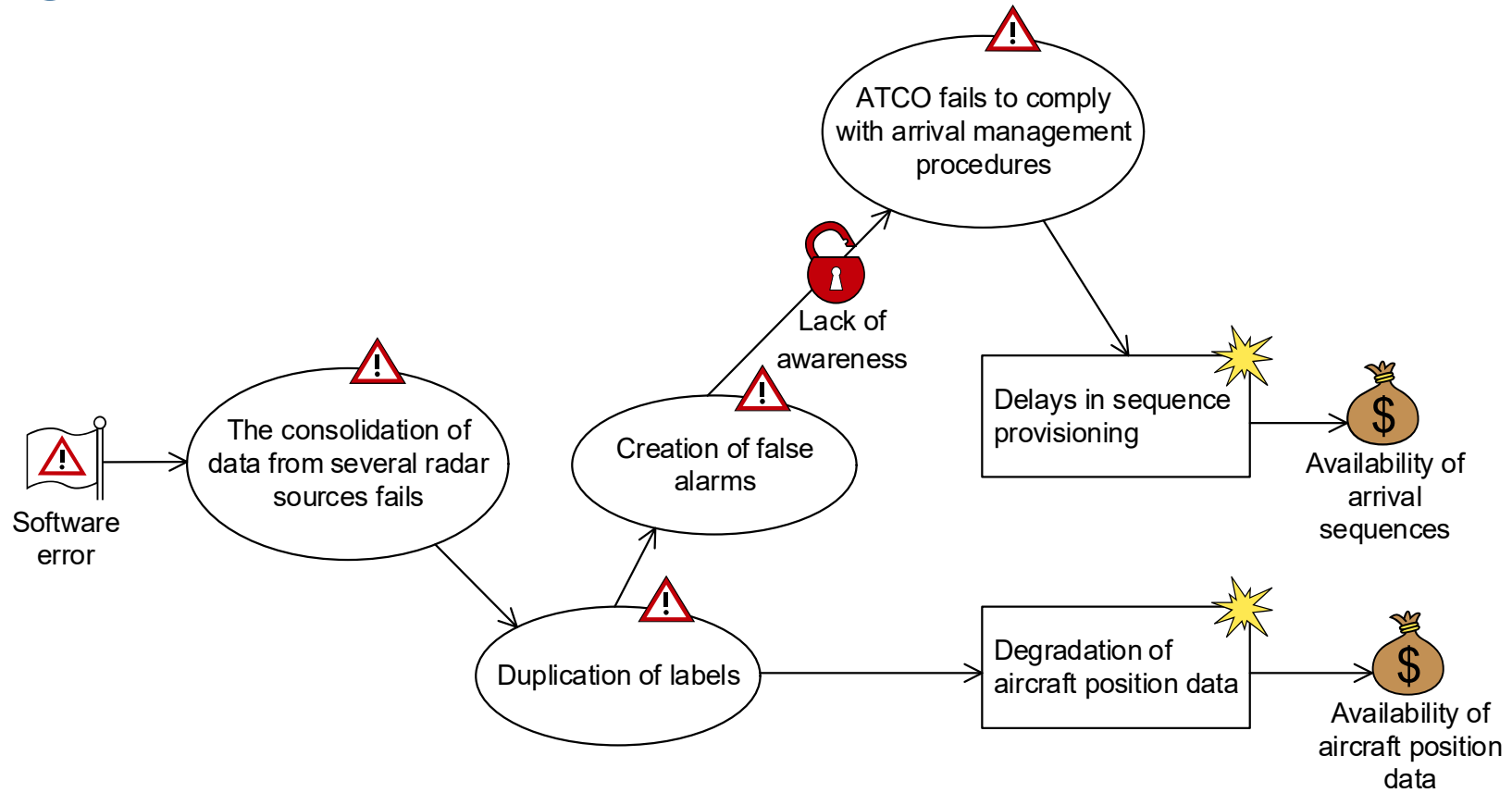
Likelihood	Description
Certain	A very high number of similar occurrences already on record; has occurred a very high number of times at the same location/time
Likely	A significant number of similar occurrences already on record; has occurred a significant number of times at the same location
Possible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

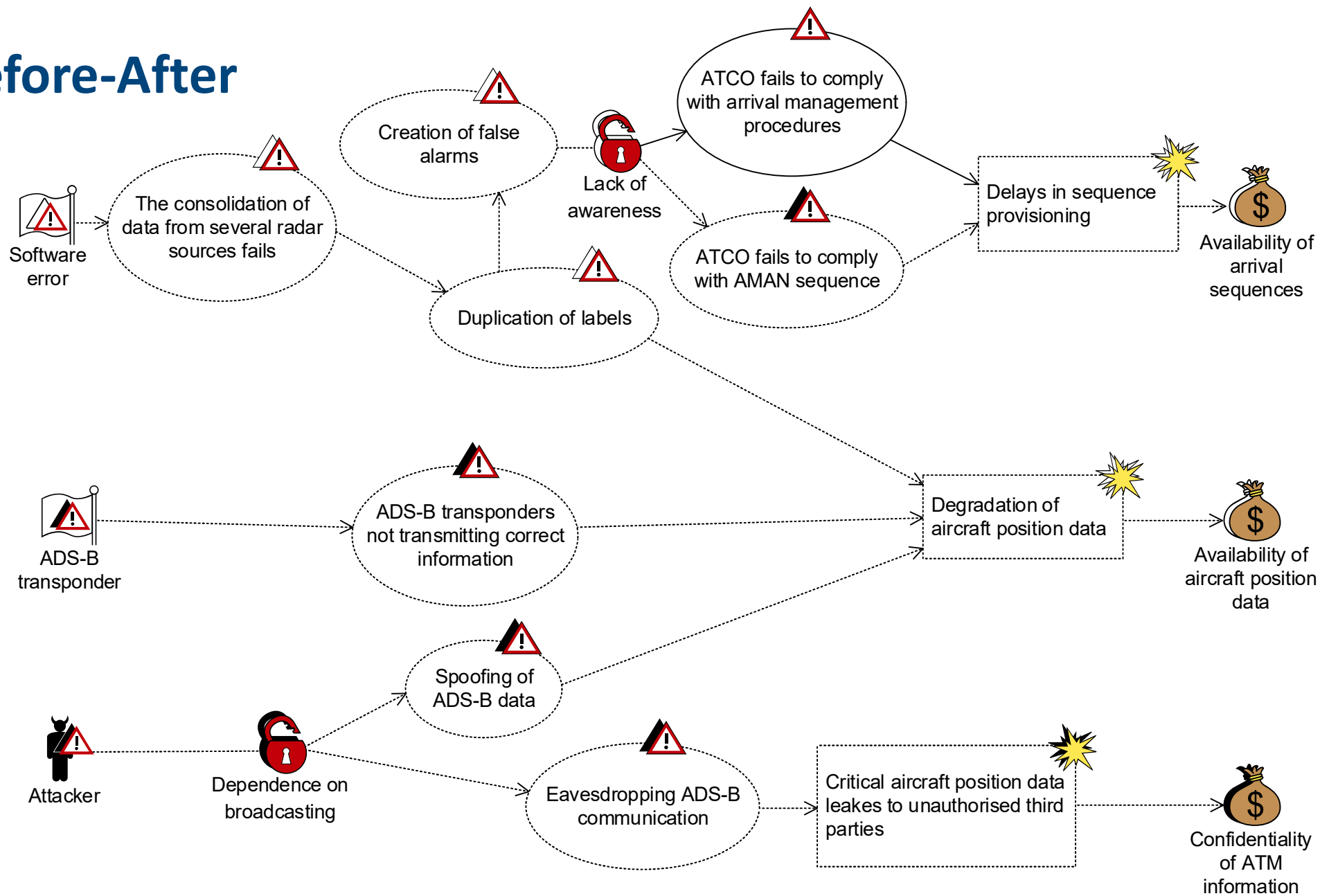
Likelihood	Consequence				
	Insignificant	Minor	Moderate	Major	Catastrophic
	Rare				
	Unlikely				
	Possible				
	Likely				
	Certain				

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

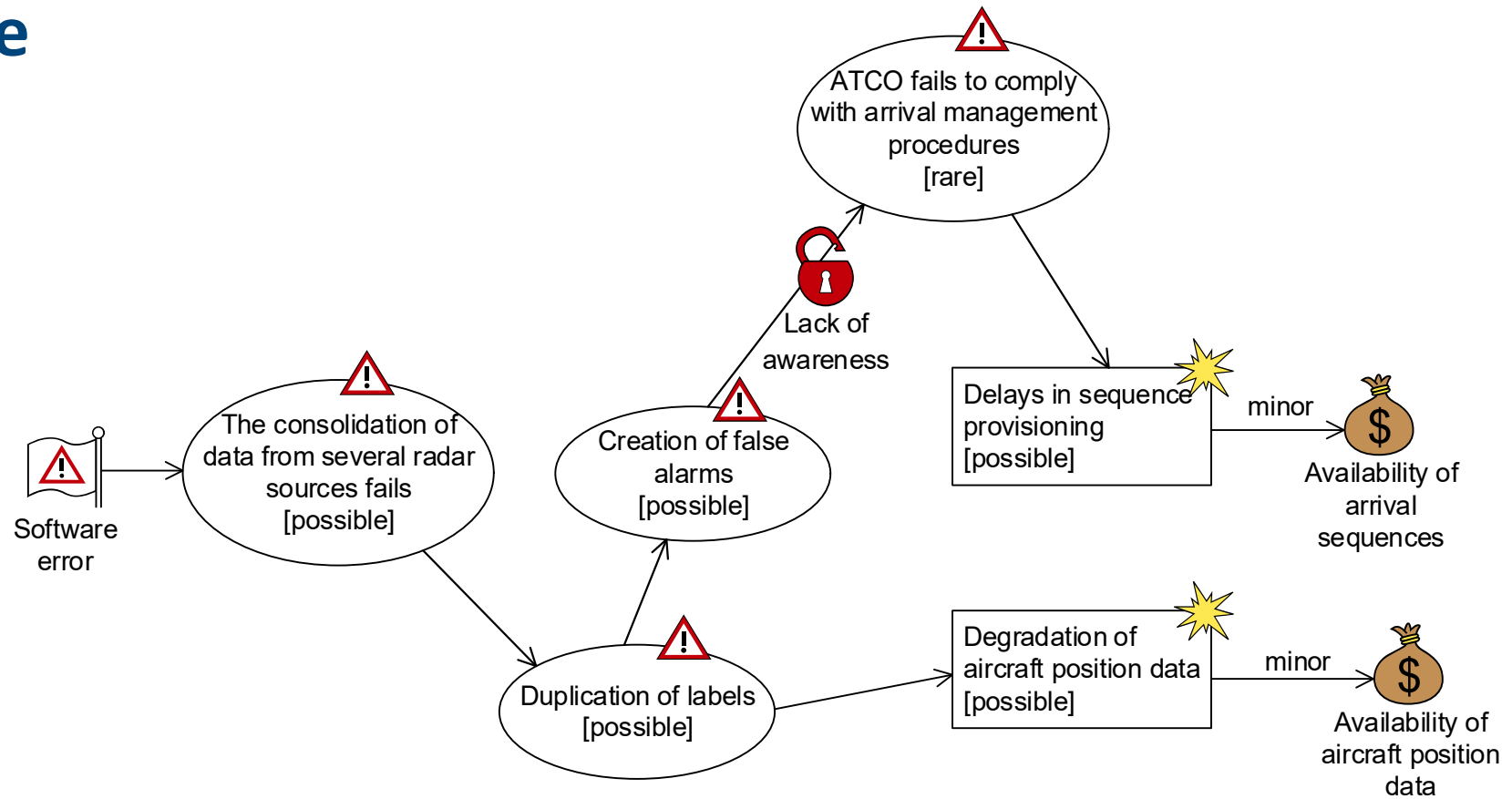
Before



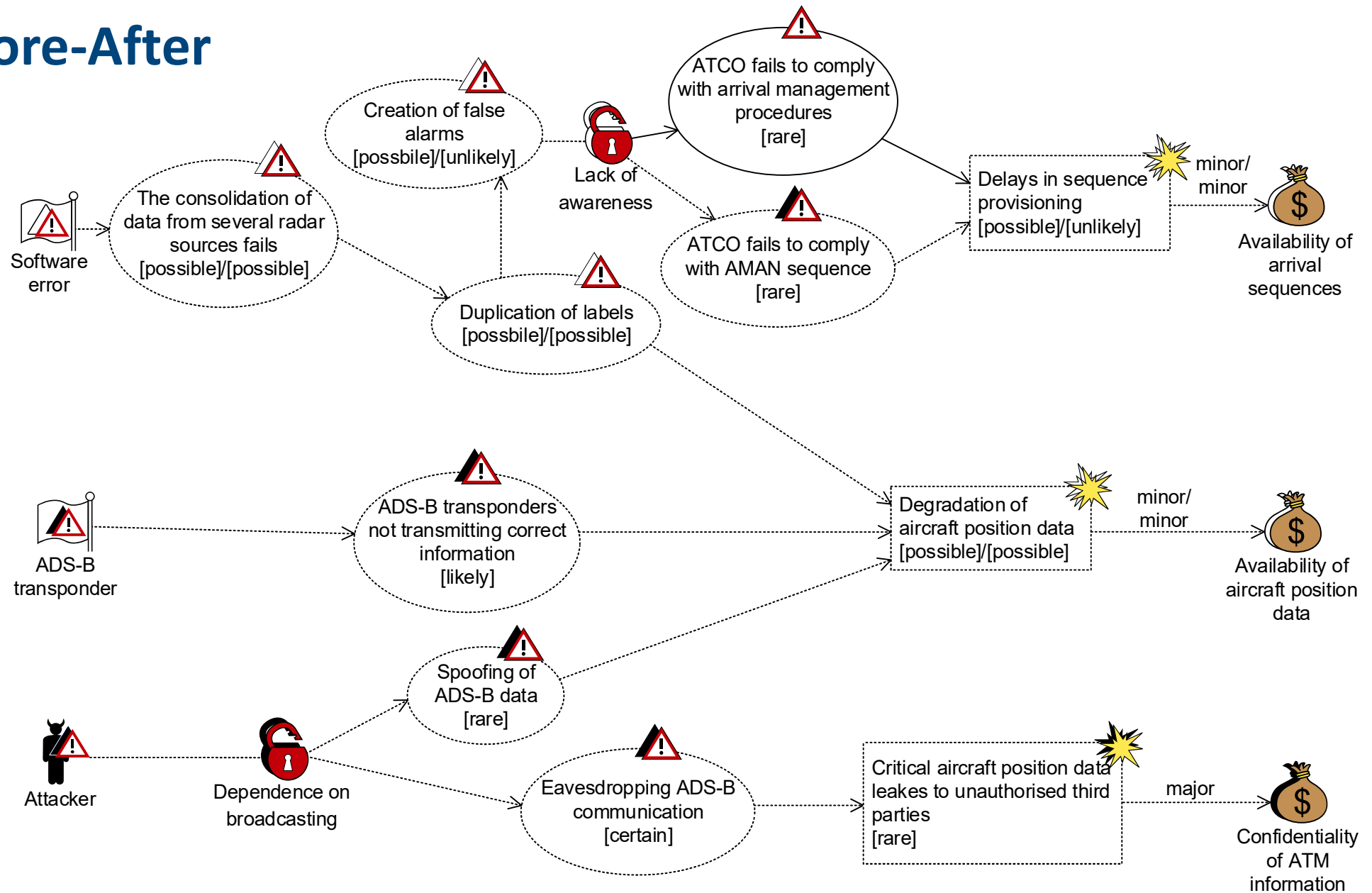
Before-After



Before



Before-After

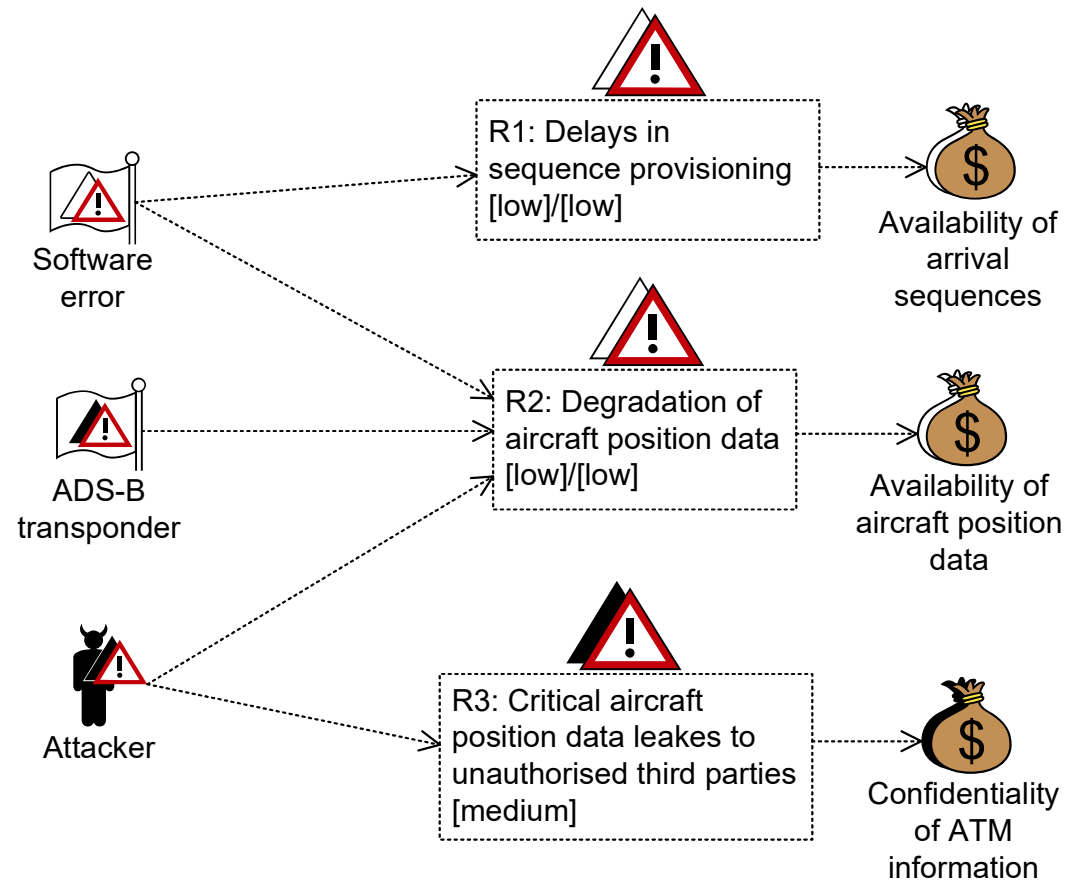


Risk Evaluation: Before-After

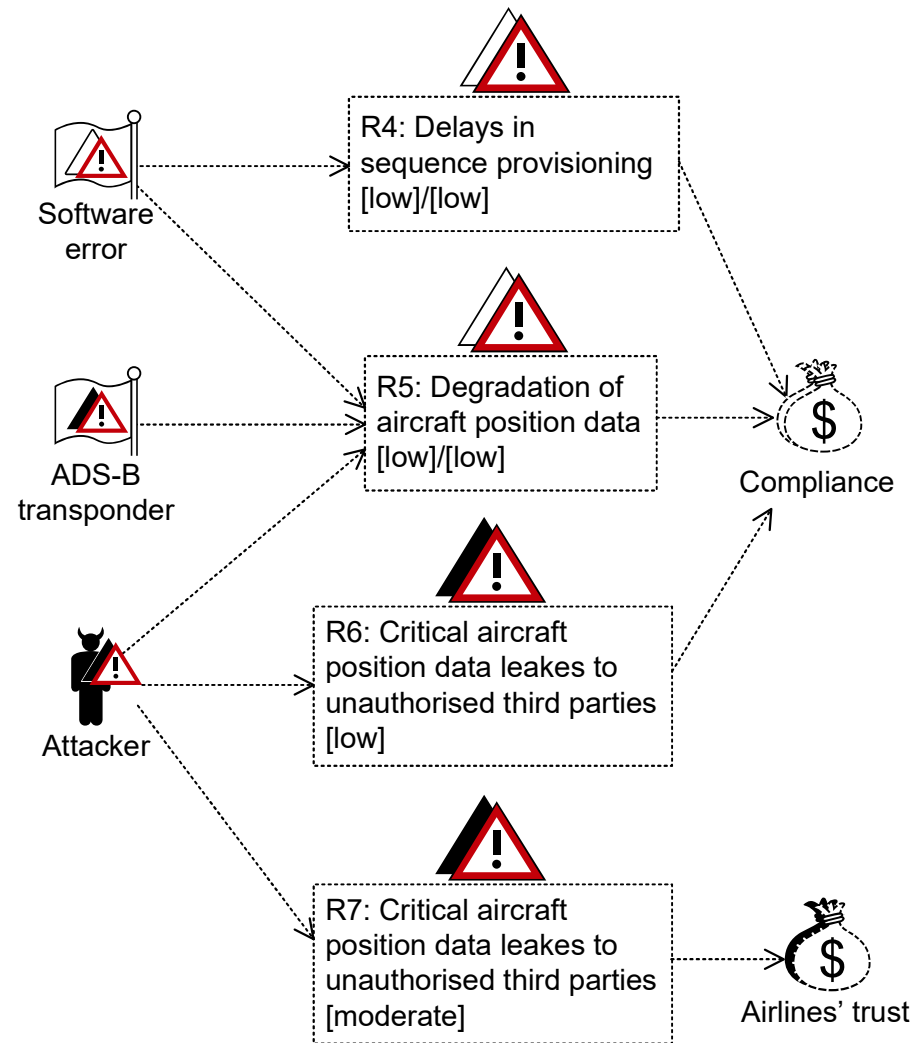
		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Rare		R6	R7	R3	
	Unlikely	R4	R1			
	Possible	R4	R1, R2, R5			
	Likely					
	Certain					

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

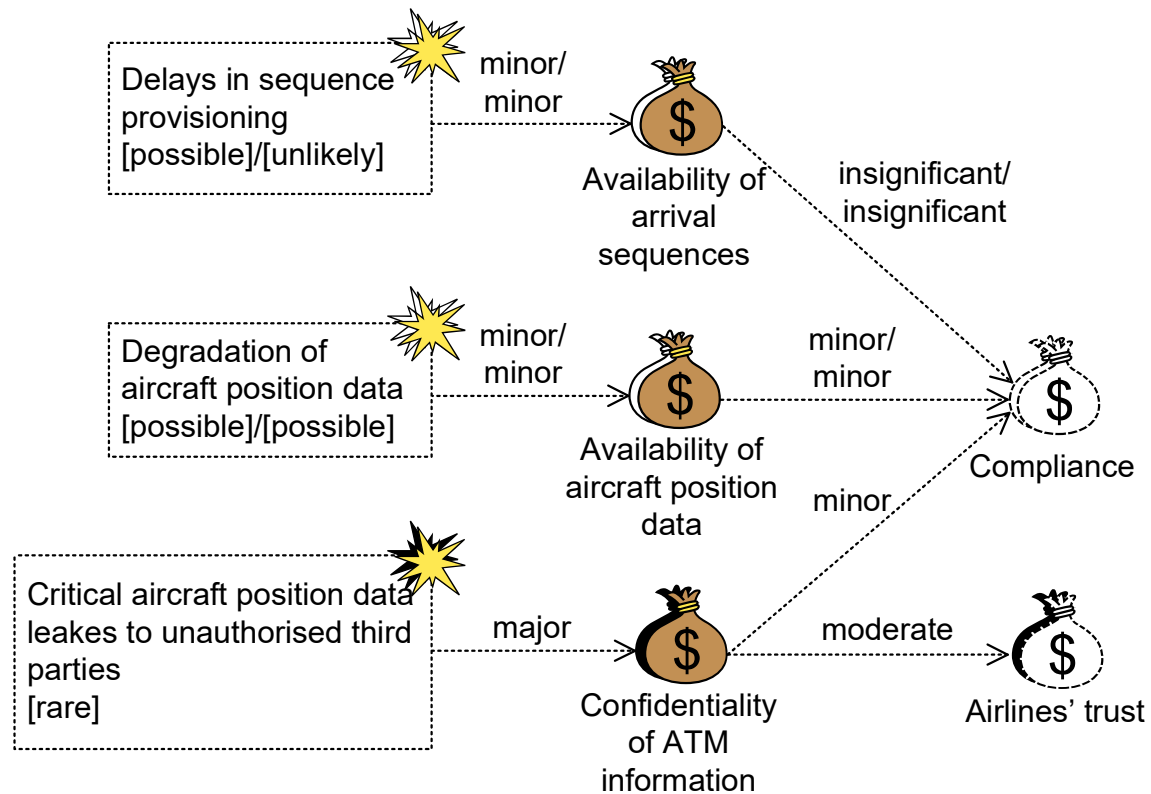
Risk Diagram: Before-After



Risk Diagram: Before-After



Risk wrt Indirect Assets: Before-After



Treatment Diagram: Before-After

