Part III: Change Management

Bjørnar Solhaug
SECURWARE 2011-08-21

SINTEF
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

- Target at time $t_0$
- Evolution
- Target at time $t_1$
- Evolution
- Target at time $t_n$
- Risk picture
- Risks at time $t_0$
- Risks at time $t_1$
- Risks at time $t_n$
- Risk assessor

CORAS 7
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

Before

\[ v_1 [P_1] \]
\[ v_2 [P_2] \]
\[ v_3 [P_3] \]
\[ v_4 [P_4] \]
\[ v_7 [P_7] \]

Before

\[ v_1 [P_1] \]
\[ v_2 [P_2] \]
\[ v_3 [P_3'] \]
\[ v_4 [P_4'] \]
\[ v_7 [P_7'] \]

After

\[ v_5 [P_5] \]
\[ v_6 [P_6] \]
CORAS Instantiation

\[\begin{align*}
&v_1 \quad [P_1] \\
&v_2 \quad [P_2]/[P_2'] \\
&v_3 \quad [P_3]/[P_3'] \\
&v_4 \quad [P_4]/[P_4'] \\
&v_5 \quad [P_5] \\
&v_6 \quad [P_6] \\
&v_7 \quad [P_7]/[P_7'] \\
&v_i \quad [P_i]
\end{align*}\]
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
5. Risk identification using threat diagrams
6. Risk estimation using threat diagrams
7. Risk evaluation using risk diagrams
8. Risk treatment using treatment diagrams

**Establish context**

**Assess risk**

**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

Flight Data Processing System
Aeronautical Operational Information System
Area Control Centre network
Operation room

Location of Air Traffic Controllers (ATCOs)

Adjacent Air Traffic System unit
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

Arrival management tasks

- Controlling the aircraft in the sector
- Aircraft data analysis for starting the sequence creation
- Sequence finalization
- Clearances to the aircraft for building the planned sequence
- Progressive transfer of the whole sequence to the adjacent sector
Target After
Target After

class OPS Room

: ACC network

: AMAN

: CWP_SUP

: SUP[1..*]

: ACC island[1..*]
Arrival management tasks

- Controlling the aircraft in the sector
  - Acquisition of the AMAN provided sequence
    - 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

- 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

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Loss of data that can be utilized in terror</td>
</tr>
<tr>
<td>Major</td>
<td>Data loss of legal implications</td>
</tr>
<tr>
<td>Moderate</td>
<td>Distortion of air company competition</td>
</tr>
<tr>
<td>Minor</td>
<td>Loss of aircraft information data</td>
</tr>
<tr>
<td>Insignificant</td>
<td>Loss of publically available data</td>
</tr>
</tbody>
</table>

#### Availability

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Catastrophic accident</td>
</tr>
<tr>
<td>Major</td>
<td>Abrupt maneuver required</td>
</tr>
<tr>
<td>Moderate</td>
<td>Recovery from large reduction in separation</td>
</tr>
<tr>
<td>Minor</td>
<td>Increasing workload of ATCOs or pilots</td>
</tr>
<tr>
<td>Insignificant</td>
<td>No hazardous effect on operations</td>
</tr>
</tbody>
</table>
## Likelihood Scale

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certain</td>
<td>A very high number of similar occurrences already on record; has occurred a very high number of times at the same location/time</td>
</tr>
<tr>
<td>Likely</td>
<td>A significant number of similar occurrences already on record; has occurred a significant number of times at the same location</td>
</tr>
<tr>
<td>Possible</td>
<td>Several similar occurrences on record; has occurred more than once at the same location</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Only very few similar incidents on record when considering a large traffic volume or no records on a small traffic volume</td>
</tr>
<tr>
<td>Rare</td>
<td>Has never occurred yet throughout the total lifetime of the system</td>
</tr>
</tbody>
</table>
Risk Evaluation Criteria

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rare</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possible</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **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
Before
Critical aircraft position data leaks to unauthorised third parties

Degradation of aircraft position data

Spoofing of ADS-B data

ADS-B transponders not transmitting correct information

Duplication of labels

Creation of false alarms

ATCO fails to comply with arrival management procedures

ATCO fails to comply with AMAN sequence

Lack of awareness

Delays in sequence provisioning

Availability of aircraft position data

Confidentiality of ATM information

Lack of awareness

Availability of arrival sequences

Confidentiality of ATM information

Eavesdropping ADS-B communication

Critical aircraft position data leaks to unauthorised third parties

Dependence on broadcasting

Attacker

ADS-B transponder

ADS-B

CWP

Surveillance

Technical room

Software error

The consolidation of data from several radar sources fails

CWP

Before-After
Risk Estimation

CORAS Step 6
Before
Critical aircraft position data leaks to unauthorised third parties

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

Spoofing of ADS-B data [rare]

ADS-B transponders not transmitting correct information [likely]

Eavesdropping ADS-B communication [certain]

ATCO fails to comply with AMAN sequence [rare]

ATCO fails to comply with arrival management procedures [rare]

Delays in sequence provisioning [possible]/[unlikely]

Lack of awareness

ATCO

Available of aircraft position data

Availability of arrival sequences

minor/minor

Confidentiality of ATM information

major

Before-After
Risk Evaluation

CORAS Step 7
Indirect Assets

- Before-After
Risk Diagram

- Before-After

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

- Before-After

- R4: Delays in sequence provisioning [low]/[low]
- R5: Degradation of aircraft position data [low]/[low]
- R6: Critical aircraft position data leaks to unauthorised third parties [low]
- R7: Critical aircraft position data leaks to unauthorised third parties [moderate]

Compliance

Software error

ADS-B transponder

Attacker

Airlines' trust
# Risk Evaluation

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rare</td>
<td>R6</td>
<td>R7</td>
<td>R3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely</td>
<td>R4</td>
<td>R1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possible</td>
<td>R4</td>
<td>R1, R2, R5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely</td>
<td>R1, R2, R5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certain</td>
<td>R1, R2, R5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Legend:**
  - *Italic* denotes risk before
  - **Bold** denotes risk after
Eavesdropping ADS-B communication
Spoofing of ADS-B data [rare]
ADS-B transponders not transmitting correct information [likely]
Implement encryption of ADS-B signals
Implement backup or improve maintenance of the transponder
R2: Degradation of aircraft position data [low]/[low]
R3: Critical aircraft position data leaked to unauthorised third parties [medium]
R7: Critical aircraft position data leaked to unauthorised third parties [moderate]

Before-After
Dependence on broadcasting
Airlines’ trust
Confidentiality of ATM information
Availability of aircraft position data

CORAS 47
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: