www.thalesgroup.com

Towards automating the construction & maintenance of attack trees: a feasibility study

Stéphane Paul - Thales Research & Technology

Graphical Models for Security (GraMSec) workshop,
ETAPS, Grenoble, April 12, 2014

Agenda

Context

- Why is there industrial interest in automating the construction of attack trees?

Part n 1: High-level principles of the automation approach

- Overview of how it could be done

Part n 2: Example

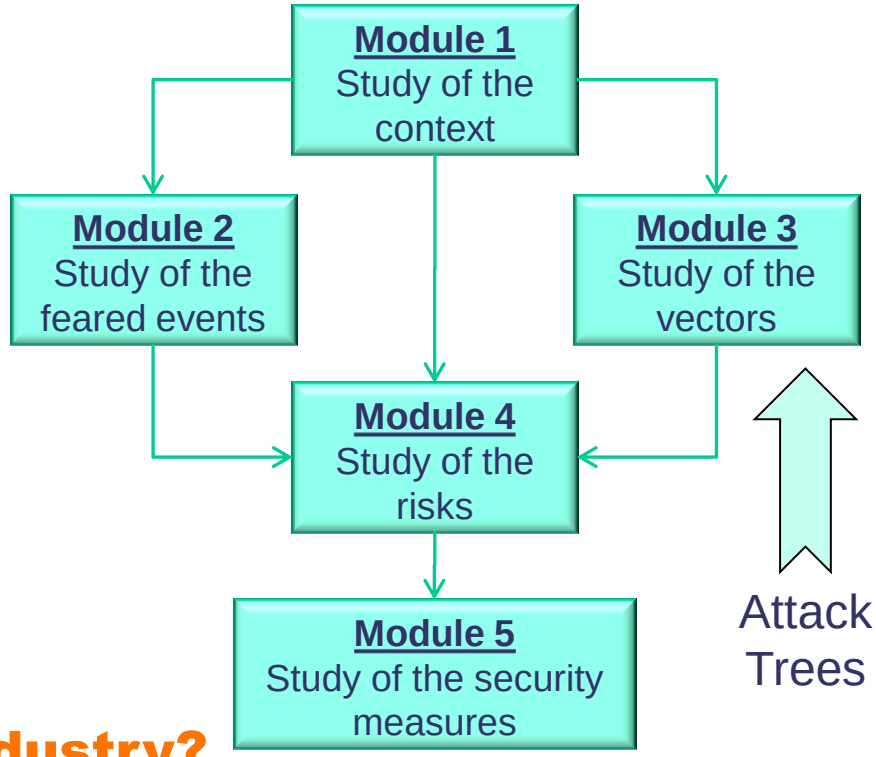
- Automating a simple example (1st two steps only)

Conclusion

Context

Information systems ever more complex… blah-blah

- …in an open interconnected world… blah-blah
- …security concerns are rising… blah-blah
- …risk management… blah-blah
- …attack trees… blah-blah



Industry challenges

- Complexity
- …

But what is complexity for industry?

Example of complexity for industry

System models

Prime-contractor, site n 1
Mainstream system engineering
(multi-billion € project)

Auditor, Pen tester, Ethical hacker
Security IVVQ

Prime-contractor, site n 2
Mainstream system engineering

System models

2: Security objectives

1: Initial model (3000+ security rqs)

3: Model updates (risk treatment = 5000+ security rqs)

Security experts (5+ persons)
Security risk assessment

Subcontractors
Subsystem engineering

Security experts
Sub-system security risk assessments

Consolidation

Typical industrial set-up

…running over many years….

Multi-user development configuration
+
Sub-contractor configuration

OPEN

THALES

Context (cont.)

Complexity reflects on

- Tooling, and…
- Humans

One (partial) solution: introduction of Attack Trees

- Recognised Threat & Vulnerability Assessment Technique
- Extends Classical Risk Assessment Studies*

But…

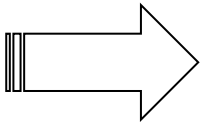
- Attack Trees also grow big (40+ A4 pages)
- Large Attack Trees are difficult to construct…
- …and even harder to maintain

*: See Stéphane Paul, Raphaël Vignon-Davillier, *Unifying traditional risk assessment approaches with attack trees*, In Journal of Information Security and Applications (JISA), Information Security Technical Report (ISTR) – To be published.

Context (cont.)

Challenges with respect to attack trees

- **Consistency Assurance**
  - Across Security Experts* (methodology)
    - In space
    - In time
  - With System Architecture
  - With Risk Management Study
- **Tool support**
  - Software Interfaces (APIs)
  - Traceability / Impact Analysis
  - Formal Semantics / Analyses
- **Scalability**
  - Automatic Tree Layout
  - Multipage and/or directed acyclic graph support



Is is possible to automate the construction of ATs?

*: NIH syndrome.

Empirical background: the Galileo programme

Thales Communications & Security (TCS) is responsible for the overall risk assessment of the European Galileo programme

- **Risk identification & treatment is realised through the use of attacks trees (manual process)**
  - Risk management process approved by 27 Member States in Sept. 2011
- **Feared events are at the root of attack trees**
  - The feared events are defined at strategic (i.e. operational) level
- **The study considers the operations**
  - I.e. people and procedures

Thales Research & Technology reverse-engineered some Galileo attack trees & discussed user-experience*

1. **Identification of tree structuring principles**
2. **Could it have been automated?**

*: Especially, what went wrong, what was corrected, etc.

www.thalesgroup.com

High-level principles of the automation approach

Part n 1

12/04/2014 - TRT-Fr/STI/LSEC/SPA.14/0019

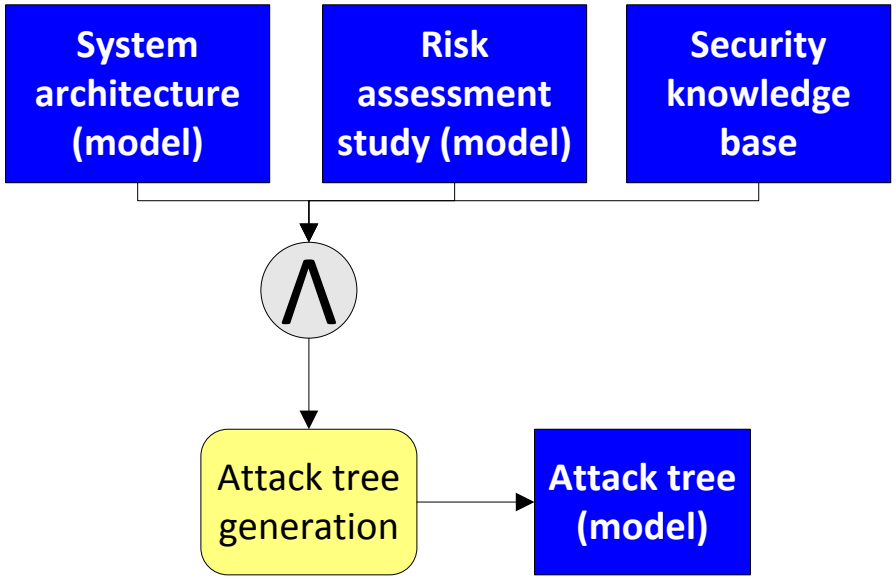
OPEN

THALES

Prerequisites

Inputs are required from

- An architecture framework
  - Operational architecture
  - Logical architecture
- A security risk assessment tool
  - Context information including
    - Primary & supporting assets
    - Existing security solutions
    - Threat sources, etc.
  - Feared events, etc.
- A security knowledge base
  - Supporting Asset Types
  - Threats
  - Vulnerabilities, etc.



Tree structuring principles (1/3)

Structuring principles for constructing attack trees (with feared event at root of tree)

- By system states and modes
- By supporting asset types (e.g. hardware, software, data/control flows…)
- By attack entry points (i.e. supporting asset interface)
- By threats (e.g. using EBIOS-2010 knowledge base)
- By threat sources*
- By the attack itself

The tree structure is driven by exploitation / ergonomic considerations

- Obj: cascade of exploits with essentially OR gates decomposition
- Heuristic: locate AND gates as low as possible in the tree

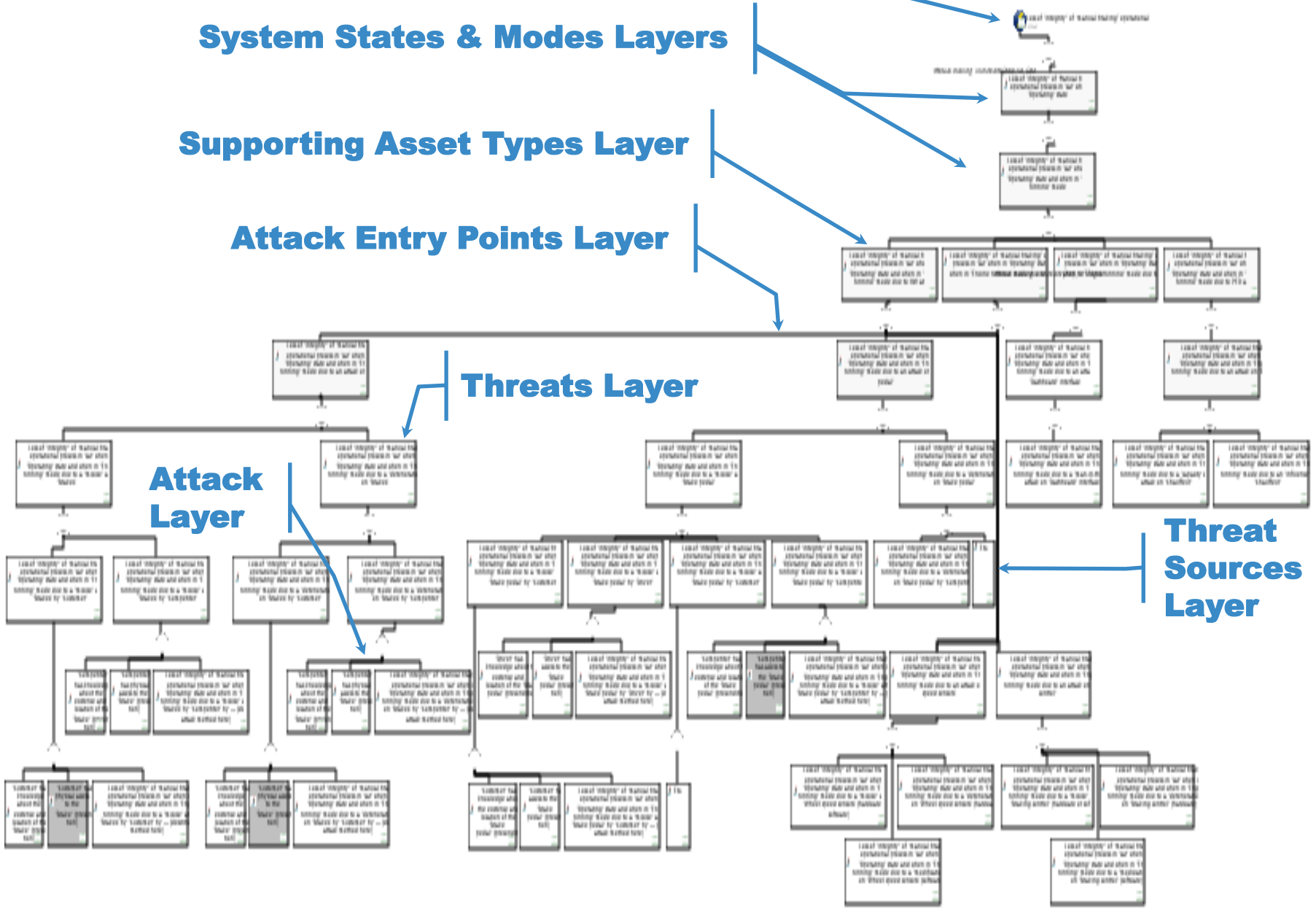
*: In Galileo, the structuring principle is:
- by "teleology" (i.e. intentional, accidental, env.)
- by access types (i.e. insider vs. outsider).

Tree structuring principles (2/3)

Analysis of occurrences of AND gates

- **Capture preconditions to enact the attack**
  - A change in states and modes is required to enact the attack
    - Usually leads to a Directed Acyclic Graph (DAG)
  - Other preconditions
    - E.g. knowledge about existence, location, etc.
- **Capture post-conditions to make succeed the attack (e.g. ensure stealth attack, allow for repudiation of attack)**
  - May lead to a full-blown sub-tree
- **Capture redundancy**
  - In case of attacks with respect to denial of service / integrity
  - In particular for safety-critical systems

Tree structuring principles (3/3)



www.thalesgroup.com

Practical application to assess automation feasibility

Part n 2

12/04/2014 - TRT-Fr/STI/LSEC/SPA.14/0019

THALES

Test case

Loss of integrity of the breaking capacity in a standard modern car used as taxi

Le Parisien

Actualité > **Argenteuil**

Il aurait saboté les freins de la voiture de sa femme

Frédéric Naizot | Publié le 25.03.2013, 07h00

OPEN

THALES

Step n°1: creation of attack tree root

Step n 1: seemingly easy, but need for semantics…

Tree initiation

- **Feared events are defined at strategic level (text!)**
  - I.e. Feared events are related to primary assets of the operational architecture
  - Scope for primary assets: operational processes + data*
- **Feared events are at the root of attack trees**

Structuring principles for constructing attack trees

- **By system states and modes**
- **By supporting asset types**
- **By attack entry points**
- **By threats**
- **By threat sources**

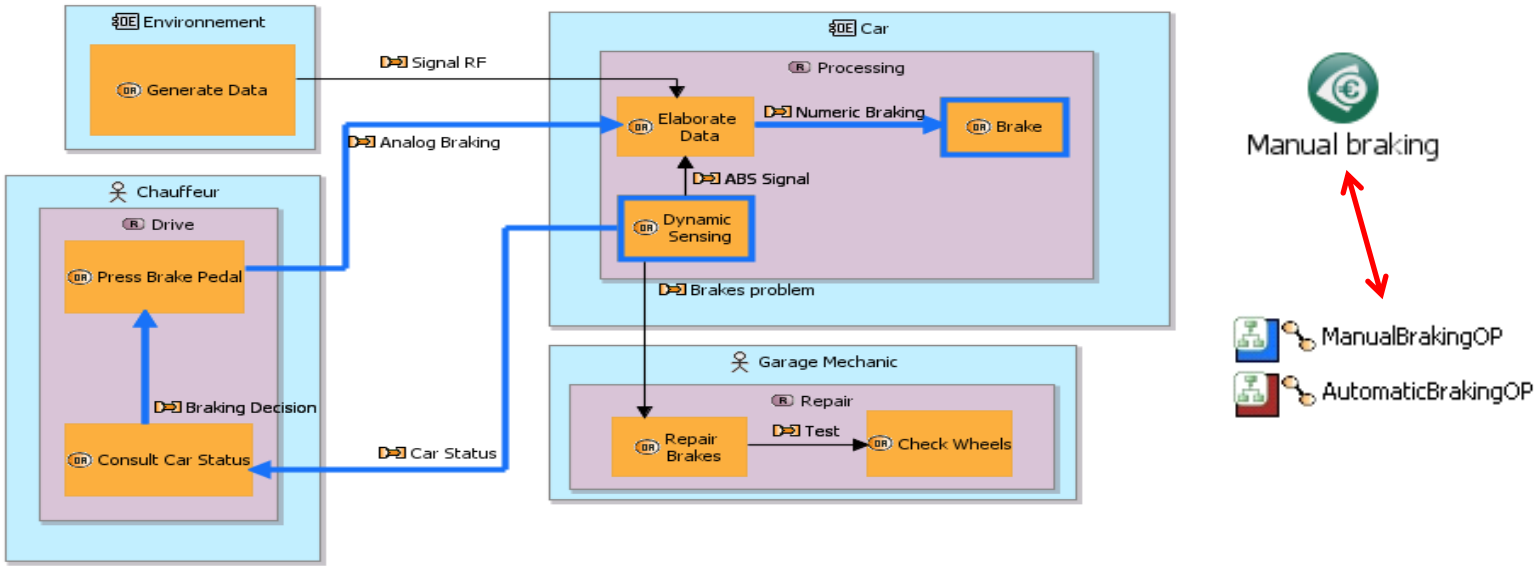
* In the Thales AF, data is part of “Common”, i.e. transverse to all abstraction levels.

THALES

Step n°1: creation of the attack tree root

Feared event: *Loss of 'integrity' of 'manual braking' operational process in 'car'*

- **Artefacts of the operational architecture are mapped**
  - Operational entity: '**car**' → entry point to system architecture
  - Operational process*: '**manual braking**' → primary asset



- **Security-related keywords are recognised**
  - Security criterion: '**integrity**' → entry point to security knowledge base

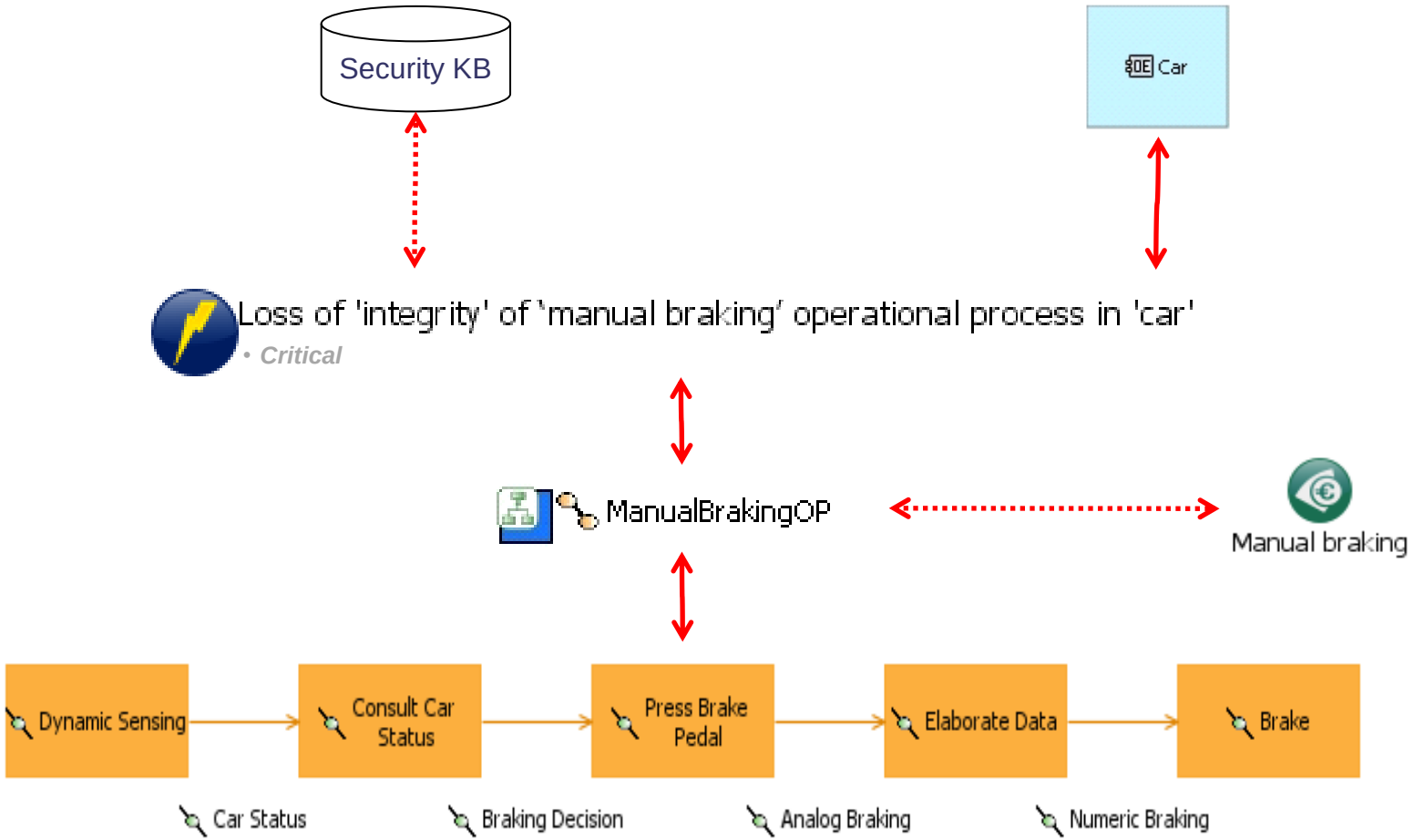
* Logical organisation of interactions and operational activities to fulfil an operational capability

OPEN

THALES

Step n°1: creation of the attack tree root

Consecutive tree (root node only at this stage)

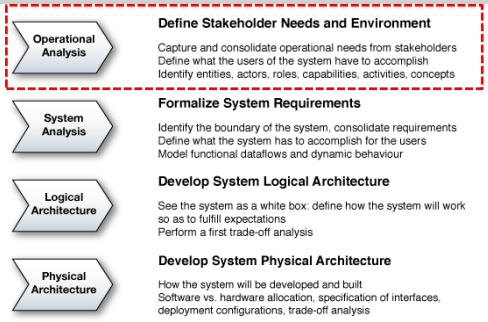


Legend:
Link to architecture artefact: ↔
Link to risk assessment artefact: ⇢

OPEN

THALES

Step n°2: structure tree according to system states and modes



Tree initiation (skipped – see paper)

- Feared events are at the root of attack trees

Structuring principles for constructing attack trees

- By states and modes
  - Need to relate the feared event (i.e. operational process) with the states & modes
- By supporting asset types
- By attack entry points
- By threats
- By threat sources

Step n 2: which state and mode make sense with respect to the feared event ?

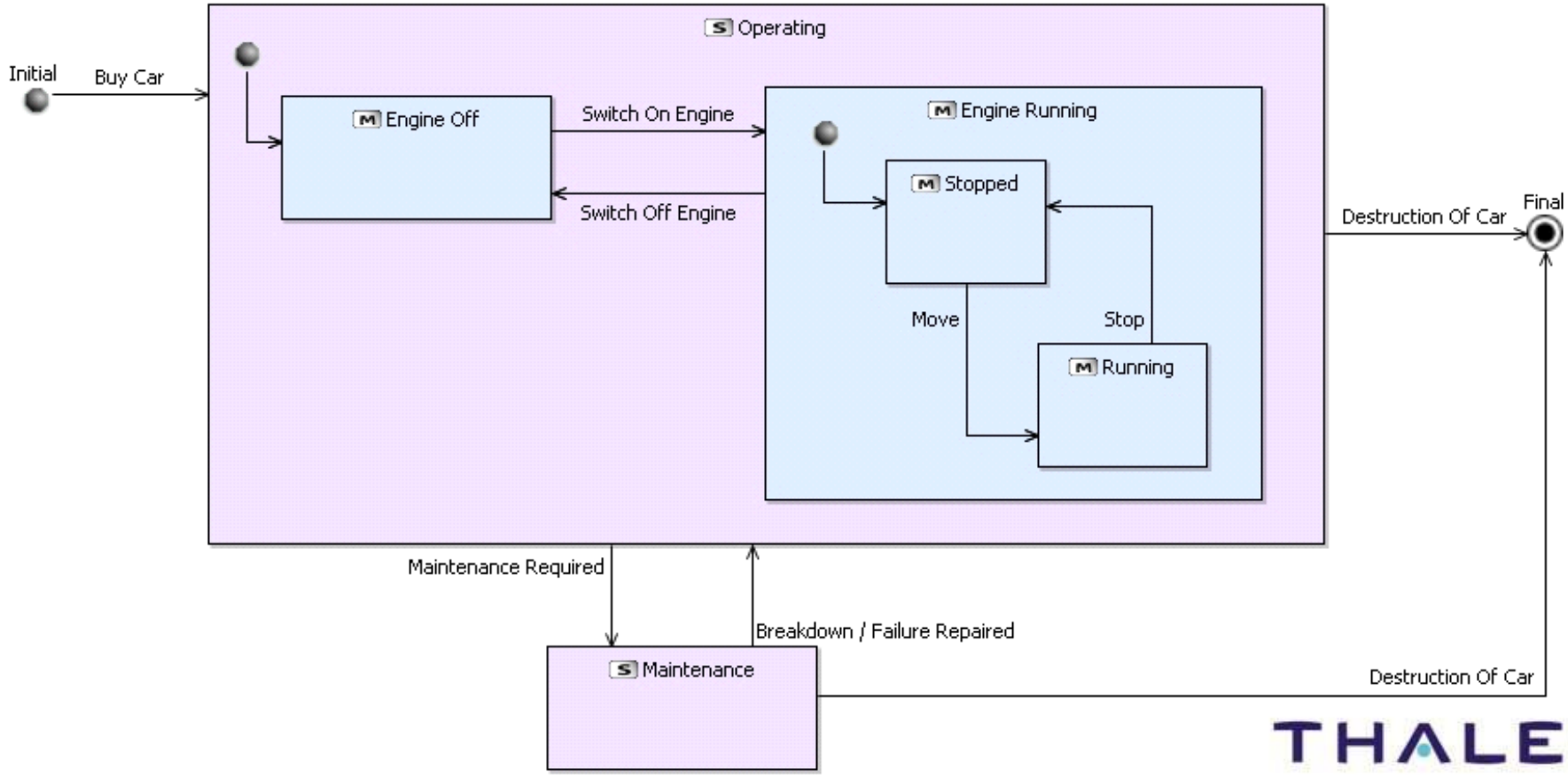
OPEN

THALES

Step n°2: structure tree according to system states and modes

Simplified car states and modes (in system architecture)

- 2 states: ‘operating’ & ‘maintenance’
- 2 top-level modes for ‘operating state’: ‘engine off’ & ‘engine running’

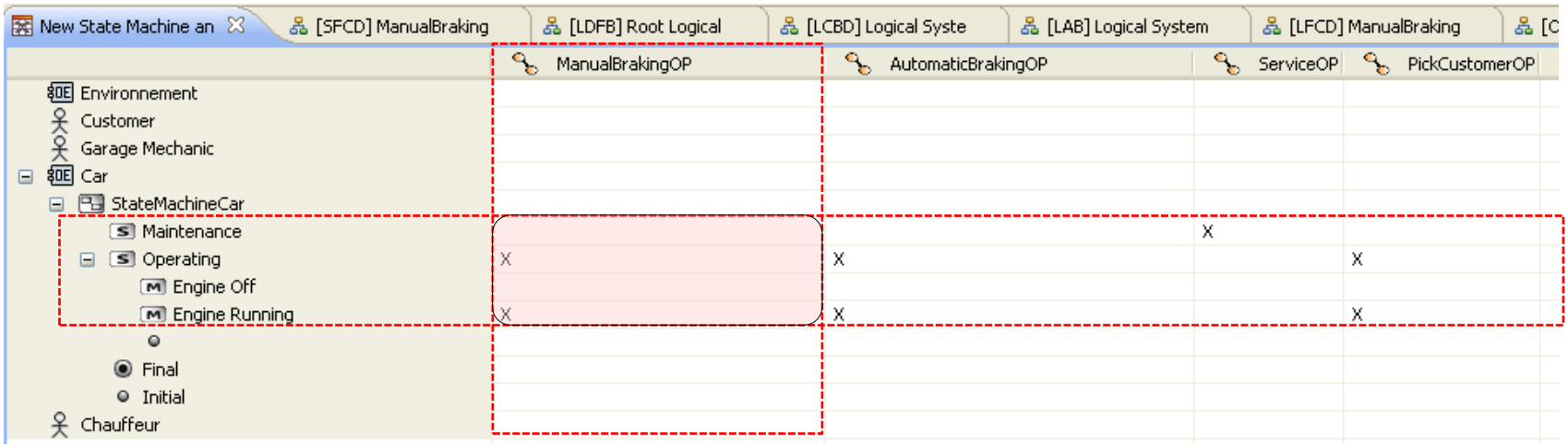


THALES

Step n°2: structure tree according to system states and modes

Running example: *Loss of 'integrity' of 'manual braking' operational process in 'car'*

- State machine and operational activities matrix

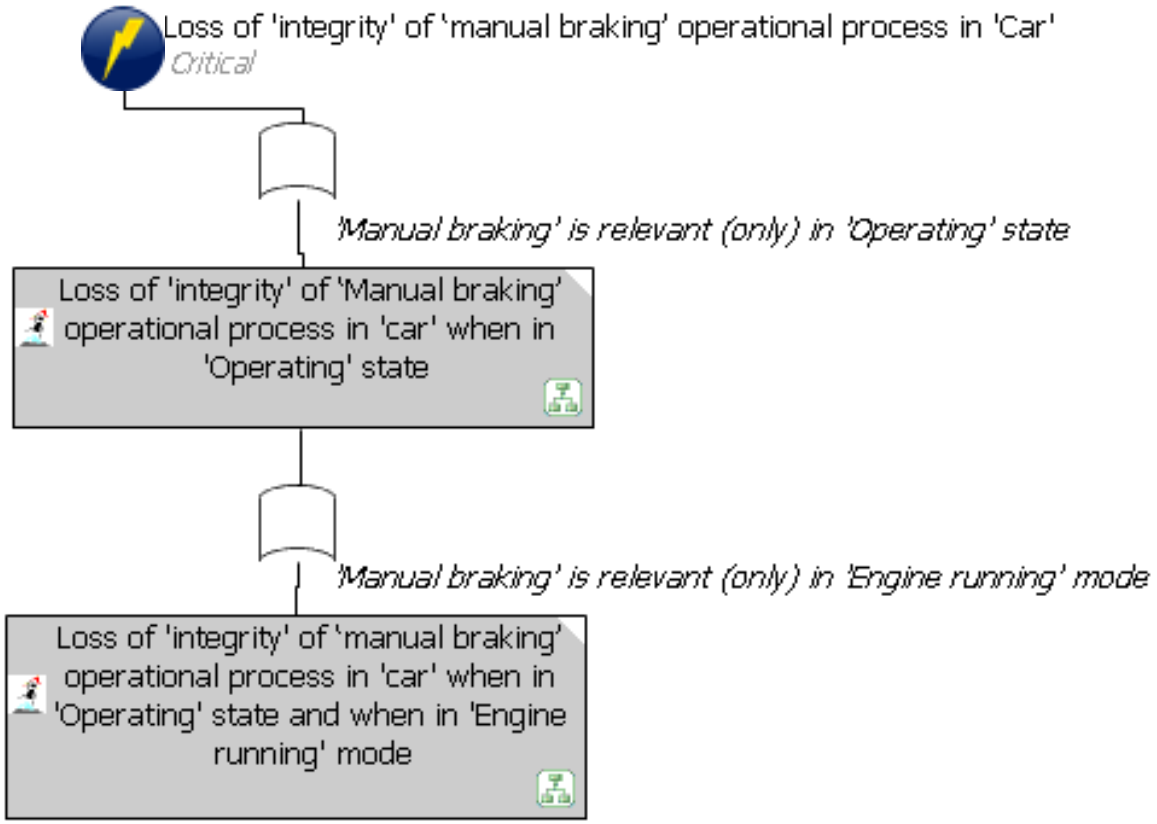


OPEN

THALES

Step n°2: structure tree according to system states and modes

Consecutive tree

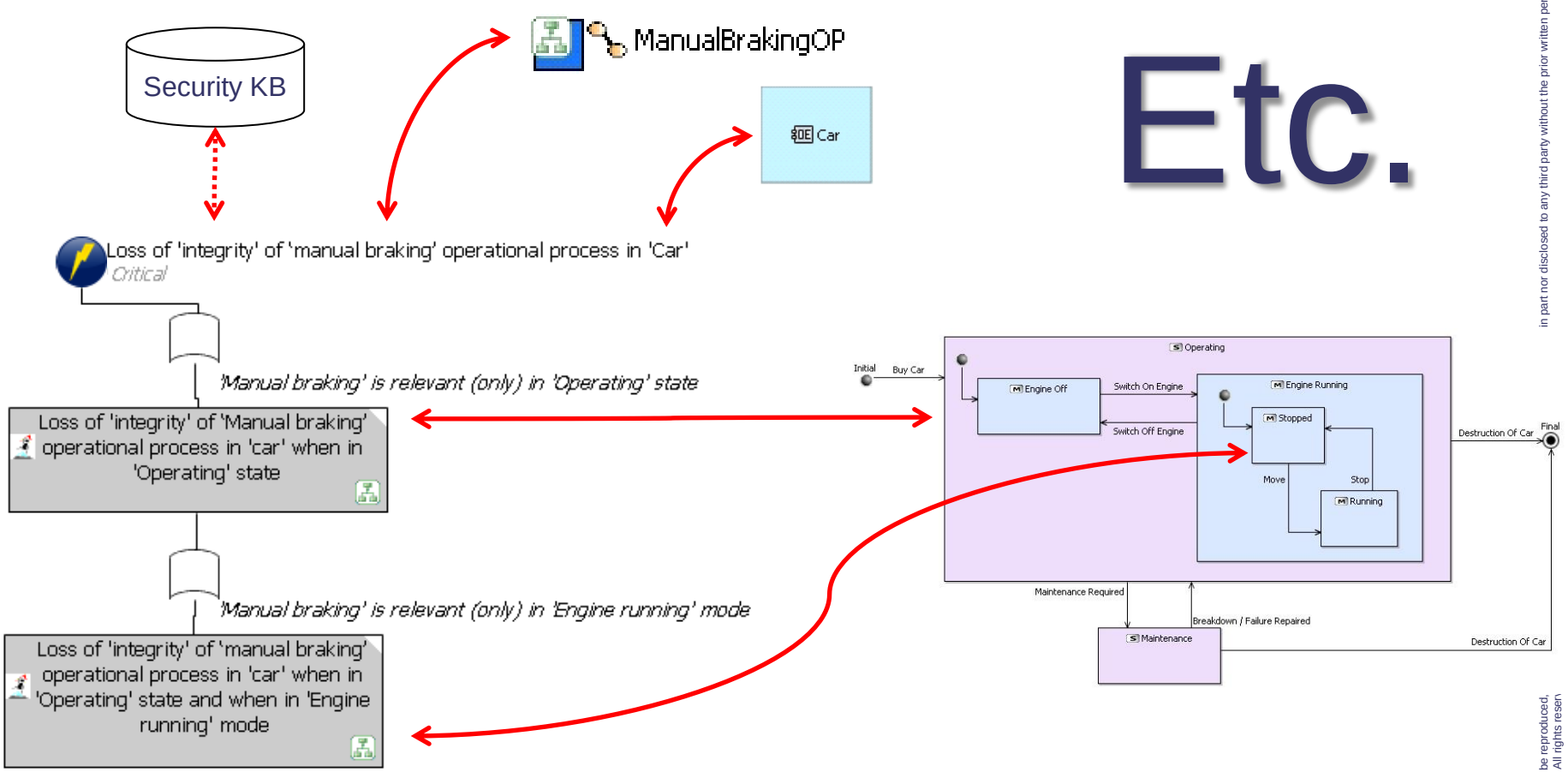


OPEN

THALES

Step n°2: structure tree according to system states and modes

Consecutive tree



Legend:
Link to architecture artefact: ↔
Link to risk assessment artefact: ⇿

OPEN

THALES

www.thalesgroup.com

Conclusions

Conclusions (1/3)

Significant 'draft' trees can be automatically generated

- **A systematic approach is enforced →**
  - Completeness
- **The tree 8 top-level layers are normalised throughout the project →**
  - Consistency amongst end-users
- **Tree node naming is automated →**
  - Productivity
  - Consistency with architecture & knowledge base
- **The lower parts of the tree are left for manual completion* →**
  - Adequacy
- **Traceability to architecture artefacts comes as side-effect →**
  - Impact analysis
  - Consistency assurance…

*: Where generation is doubtful, annotation of tree nodes may be used to explicitly attract security expert attention (e.g. a threat source is not expected to have access, so threat scenario is expected to be removed because it is irrelevant).

Conclusions (2/3)

But… the approach is not yet consolidated

- **Current work was focused on operational processes / logical functional chains →**
  - Need to study attacks on data
- **Some required design information is traditionally missing in the architecture (**e.g. physical vs. logical access specifications**) →**
  - What trade-off between poor tree generation & enriching the architecture?
- **Structuring based on states and modes**
  - What depth makes sense?
- **Etc.**

Conclusions (3/3)

Conclusions with respect to the use of the Thales AF

- No major issues raised due to Melody-Advance specificities
- Need to assess other architecture frameworks

Conclusions with respect to the use of risk assessment tool (i.e. Rinforzando)

- Links between security artefacts and design artefacts are highly valuable
- Need to assess other security knowledge bases

Conclusions with respect to the use of attack tree tools

- Some tools do not scale

QUESTIONS?

Stéphane Paul
Thales Research & Technology

stephane.paul@thalesgroup.com