Fourth All Hands Meeting, 19 - 22nd September 2005 Nottingham
Session R5.3: Requirements, Ontologies and the Semantic Web.

Combining Functional and Security Requirements' Processes.

Martyn Fletcher, Howard Chivers, Jim Austin.
martyn.fletcher@cs.york.ac.uk; hrchivers@iee.org: jim.austin@cs.york.ac.uk

THE UNIVERSITY of York

What the presentation is about.

- Report on the experience of developing security and functionality requirements for the DAME project, including:
  - Problems of developing requirements from a black box view.
  - The interactions between security and functionality requirements.
  - Relationship between business goals and security.
  - Developing other non-functional requirements.

Quick Review of Functional and Security Requirements

- Functional requirements:
  - Behaviour of system
  - Interaction of system with environment
  - A black box view
- Security requirements:
  - Risk to assets – unwanted outcomes
  - Assets:
    - outside the system e.g. data crossing system boundary
    - inside system e.g. algorithms within system
  - Need black box and transparent box view – be able to look inside at the top level design.

Background to the DAME System

- The Distributed Aircraft Maintenance Environment (DAME) project:
  - An e-Science pilot project - a diagnostic system for aero engines.
  - Implemented as a set of collaborating Grid services.
  - Uses sensor data obtained during flight.
  - Provides collaborative environment:
    - Geographically dispersed expert users
    - Different organisations work together.

The DAME Partners

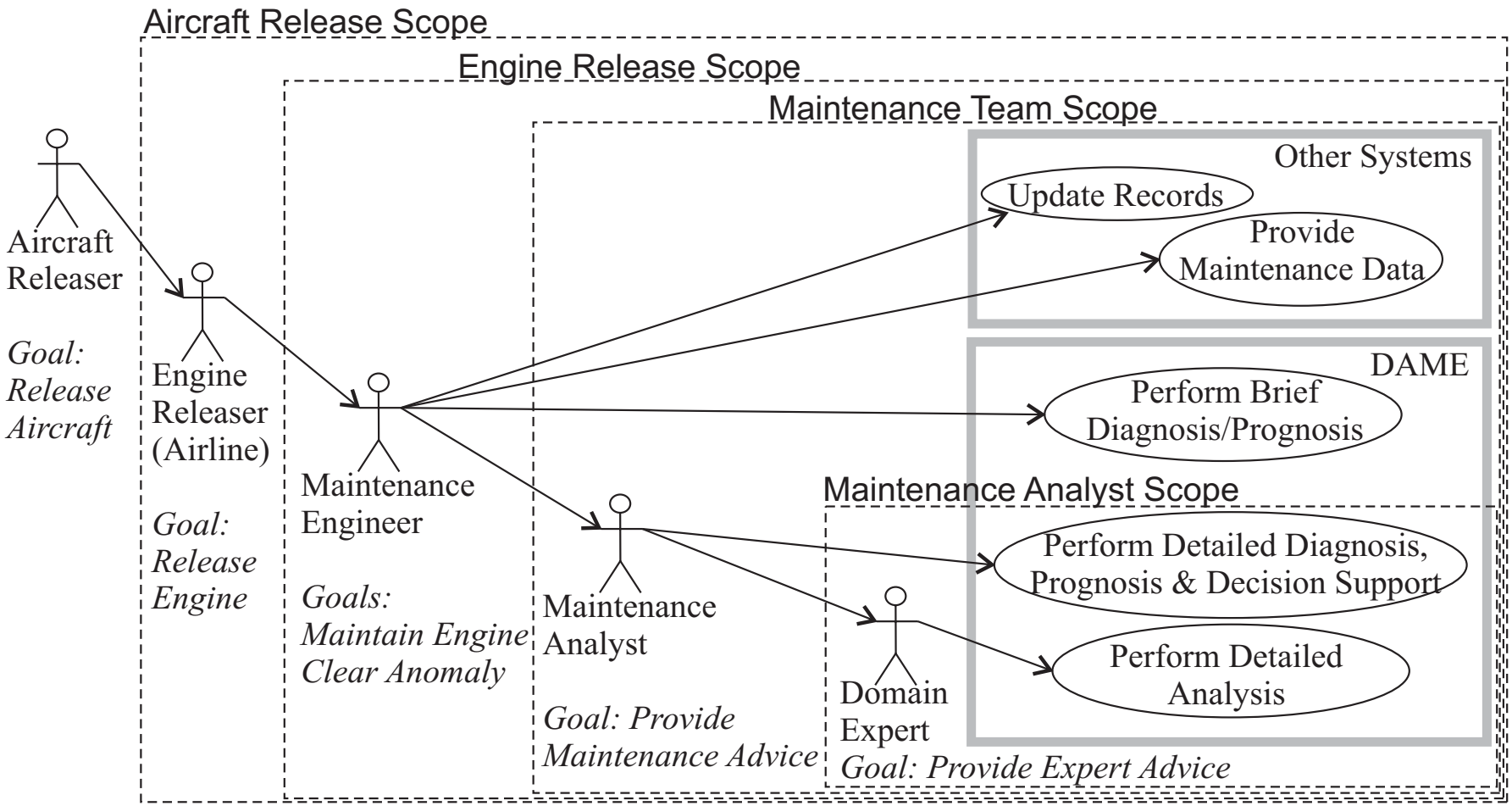
- Industrial customers:
  - Rolls-Royce plc.
  - Data Systems & Solutions, LLC.
- Development teams:
  - University of York.
  - University of Leeds.
  - University of Sheffield.
  - University of Oxford.
  - Cybula Ltd.

Functional Requirements - black box view

- Identify the stakeholders.
- Agree the system context (design scope).
- Identify outermost goals (use cases).
- Refine into relevant sub goals and eventually use cases for other systems and for DAME.
- Observations:
  - Used proxy stakeholders where necessary.
  - Time spent capturing significant behaviours of external actors and systems – very important in understanding the context of the system.

Distributed Aircraft Maintenance Environment
DAME

Breakdown of Use Cases

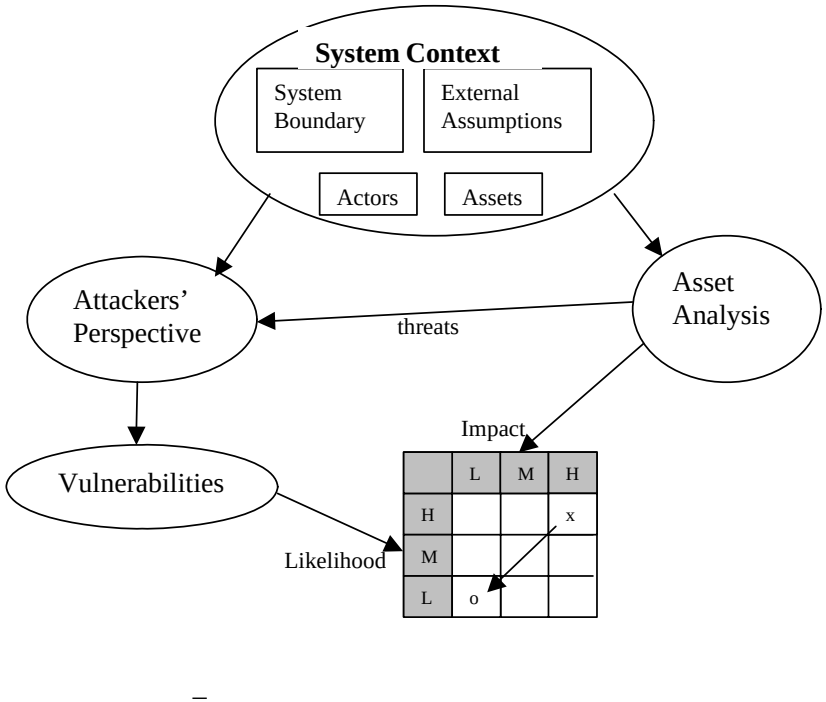


Functional Requirements - summary

- DAME business process is problem identification, escalation and analysis.
- Detected problems or conditions may be escalated through:
  - Maintenance Engineers (airport).
  - Maintenance Analysts (at data centres).
  - Domain Experts (at engine manufacturer).
- Three main DAME use cases were defined.

Distributed Aircraft Maintenance Environment
DAME

Security Process Outline



- Security Requirements are a response to risk …
  - An unwanted outcome
  - On a system asset
  - As a result of an intentioned act
- The initial focus is to determine
  - Unwanted Outcomes (Business Assets, and Stakeholders' Concerns)
  - Possible Sources of Attack
  - Threat Paths

Exposing business assets

- Need to expose *internal* business assets - necessary to establish a ‘transparent-box’ view (top level design) of the system.
- Observations:
  - Criterion of business relevance used to limit level of internal asset exposure.
  - Transparent-box also allows:
    - early assessment of feasibility and technical capability.
    - checking the system boundary.
  - Sequence diagrams are useful tool to explore and analyse how business assets interact to perform scenarios in use cases.

Eliciting business asset concerns

- Assess each asset individually with customer:
  - Concerns (unwanted outcomes)?
  - Usual security keywords used: confidentiality, integrity.
  - Naturally introduced other concerns – availability, reliability and provenance.
  - Define impact:
    - zero (not significant)
    - Low
    - Medium
    - high (prejudicial to the business for a long period).
- Observations:
  - Concerns may not be static.
  - Composite nature of some assets.
  - Avoid confusion of primary and secondary concerns.

Developing business level non-functional goals

- "Cluster" concerns for assets and into high level goals:
  - Revised and agreed by stakeholders.
  - Allowed the completeness and pertinence of the assets and concerns to be established.
  - Allowed traceability between asset-based concerns and goals to be identified.
- Seven top-level goals developed.
- Observation:
  - Example of the use of two complimentary views (asset concerns and goals) - where each can be used to cross check the other.

Distributed Aircraft Maintenance Environment
DAME

Asset Analysis Table

(Extracted from) Asset Table 3 Specific DAME Data Asset threats (concerns)				
Data Assets	**Confidentiality**	**Integrity**	**Provenance**	
3.2 Engine Data Record Performance. (These concerns may change if the data are deployed outside DAME)	RR / DS&S Could divulge proprietary information to 3rd party	RR / DS&S Need to protect accuracy of reference data	RR / DS&S. Protect the reference source of decision data	**Notes**
	I Engine Performance	**III Reliability (L)**	**IV Record decision basis**	**Goal**
	C.A Unauthorised Access	I.A Loss or Corruption	P.B Source of Reference Data	**Concern**
	Medium	Low	Medium	**Impact**

Extract from Asset Analysis Table: Specific Concerns, Impacts and Goals

Distributed Aircraft Maintenance Environment
DAME

Non-functional goals

Title:	IV: To record the provenance of diagnostic decisions and identify individuals' actions in the diagnostic process
Owner:	Rolls-Royce and Data Systems & Solutions
Impact:	Medium
Description:	The process by which diagnostic decisions are made must be recorded with sufficient quality to allow the investigation of problems or marginal decisions after the fact. Individuals that contribute to the diagnostic workflow must be accountable for their contribution to the process.

A Typical DAME Goal

Developing other non-functional goals

- Goals also emerged for other non-functional requirements:
  - Reliability.
  - Availability.
- Stakeholders do not immediately distinguish different requirement types – they just have concerns.
- Observations:
  - It is important to use an open elicitation process that is not constrained by preconceived security checklists.
  - The asset driven approach proves to be as suited to capturing other non-functional requirements as it is to security.

Attackers

- Risk is characterised by two factors:
  - Business assets, concerns and impacts.
  - Likelihood of successful attack:
    - Frequency of attack.
    - Type of attacker.
    - Degree of access.
    - Vulnerabilities - design / implementation issue.
- Frequency of attack, type of attacker, degree of access were considered and documented for each goal.

Attackers (2)

Access Type	Attacker	Goal	Frequency	Notes
Legitimate users	Domain expert Maintenance analyst Maintenance engineer	IV	Low	Users may seek to change or remove records of inappropriate decisions or actions.

A Typical Attacker Record

Conclusions (1)

- Need to invest in understanding business context of the system – especially for grid systems.
- Internal business assets must be exposed to allow elicitation of security concerns.
- Need open asset based concern elicitation – results in elicitation of other non-functional goals.
- Asset based elicitation – complementary viewpoint to functional elicitation - beneficial.
- Non-functional goals – means of testing completeness and pertinence of asset concerns.

Distributed Aircraft Maintenance Environment
DAME

Conclusions (2)

- Practical aspects:
  - Standard approaches for functional and security requirements can be combined to a degree.
  - The processes interact - beneficial.
  - Iteration is vital.

- Next step: conduct further practical work to test feasibility of the process suggested here.

Acknowledgements

This work was undertaken as part of the DAME project, with grateful assistance from Rolls-Royce plc, Data Systems & Solutions, LLC and Cybula Ltd and the teams at the Universities of York, Leeds, Sheffield and Oxford.

This research was supported by the UK Engineering and Physical Sciences Research Council (Grant GR/R67668/01), the Royal Academy of Engineering, and through contributions from Rolls-Royce plc, and Data Systems and Solutions, LLC.