SECRET
PROJECT

SECURITY OF RAILWAYS AGAINST
ELECTROMAGNETIC ATTACKS

SEVENTH FRAMEWORK
PROGRAMME

SECRET

SECurity of Railways against Electromagnetic aTtacks

Grant Agreement number: 285136
Funding Scheme: Collaborative project
Start date of the contract: 01/08/2012
Project website address: http://www.secret-project.eu

Deliverable D 5.5

Proposal for TecRec on Redundancy for Resilient Architecture

Submission date: October 2015

Deliverable on Dynamic Protection System
Date: 24/08/2013
Distribution: All partners
Manager: Trialog

Document details:

Title	Proposal for TecRec on Redundancy for Resilient Architecture
Work package	WP5
Date	05/06/2015
Author(s)	P.Lambert (Alstom), S.Mili (Altsom), C.Pinedo (EHU), C.Gransart (IFSTTAR), A Kung (TRIALOG), M Sall (TRIALOG)
Responsible Partner	Trialog
Document Code	SEC-WP5-D55-Proposal for TecRec on redundancy for resilient architecture v1.0 Final.docx
Version	1.0
Status	Final

Dissemination level:

Project co-funded by the European Commission within the Seventh Framework Programme

PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission) Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Document history:

Revision	Date	Authors	Description
0.1	1/09/2015	EHU IFSTTAR TRIALOG	Creation of the document. Contribution from EHU, IFSTTAR and Trialog First contribution to recommendations
1.0	14/10/2015	EHU ALSTOM TRIALOG	Further contribution to recommendations Contribution on architecture instantiation Contribution on guidelines for architecture evaluation

Table of content

1 Executive summary 5

2 Introduction 6

2.1 Purpose of the document 6

2.2 Definitions and acronyms 6

3 Requirements standard references 7

3.1 CEM 7

3.2 Radio 7

4 SECRET recommendation template reminder 8

5 Operational Recommendations 9

5.1 Security Analysis in Confidential Settings (WP4_TecRec_003) 9

5.2 Creating Knowledge Repository based on ISO 27034 (WP4_TecRec_006) 9

6 Engineering Rules Recommendations 11

6.1 Integrating Architecture Features for Communication Resiliency (WP4_TecRec_001) 11

6.2 Ensuring Interoperability of Risk Analysis Methods (WP4_TecRec_002) 11

6.3 Evaluating Architecture Features for Resilience (WP4_TecRec_005) 12

6.4 Transport Technology Independence in ERTMS (WP4_TecRec_007) 12

6.5 Moving to IP in ERTMS (WP4_TecRec_008) 13

6.6 Integrating Multipath Communication in ERTMS (WP4_TecRec_009) 13

7 Guidelines for Architecture Design and Evaluation 14

7.1 Methodology Description 14

7.2 Secret Resilient Architecture Components 14

7.3 Example of Architecture Instantiation 15

7.3.1 Architecture of Radio System – Mobile Part 16

7.3.2 Architecture of Radio System – Network Part 18

7.3.3 Integration of SECRET Resilient Architecture Components 20

7.4 Example of Architecture Evaluation 21

7.4.1 Introduction to Architecture Design 21

7.4.2 Architecture Tradeoff Analysis Method (ATAM) 23

7.4.3 Cost Benefit Analysis Method (CBAM) 25

7.4.4 Applying ATAM to SECRET 30

8 Conclusion 33

1 Executive summary

This deliverable focuses on recommendations for a resilient architecture in railway communication systems. It follows work carried out in WP4 (Dynamic protection: detection system for resilient architecture) and deliverables D4.1, D4.2, D4.3, D4.4, D4.5.

Engineering rule recommendations and operation recommendations are provided.

Guidelines for architecture design and evaluation are provided.

2 Introduction

2.1 Purpose of the document

The purpose of this document is to present recommendations towards a resilient architecture in the railways.

Two types of recommendations are provided:

- Engineering rule recommendations which can be used at design time
- Operation recommendations which focus on solutions/mechanisms that can be used

.The document elaborates on each recommendation as follows:

- The recommendation is described.
- A brief justification is provided.

The document also includes a section on guidelines for architecture design and evaluation, which is structured as follows:

- The methodology is explained
- An architecture example is provided
- An architecture evaluation approach is explained (not that this section is directly taken from an annex of D4.2).

2.2 Definitions and acronyms

	Meaning
BTS	Base Transceiver Station
CENELEC	European Committee for Electrotechnical Standardization
EIRENE	European Integrated Railway Radio Enhanced Network
EM	ElectroMagnetic
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile communications
EVM	Error Vector Magnitude
GSM-R	Global System for Mobile communications - Railways
HSL	High Speed Line
LGV	Ligne à Grande Vitesse (High Speed Line - HSL)
MS	Mobil station
Psd	power spectral density
SJR	signal to jamming ratio
SR	staff responsible
TGV	Train à Grande Vitesse (High Speed Train – HST)
TT	Radius of the IQ constellation
UIC	Union international des chemins fer

3 Requirements standard references

3.1 CEM

- Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements: **ETSI EN 301 489-1**
- Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 23: Specific conditions for IMT-2000 CDMA, Direct Spread (UTRA and E-UTRA) Base Station (BS) radio, repeater and ancillary equipment: **ETSI EN 301 489-23**

3.2 Radio

- Global System for Mobile communications (GSM); Harmonized EN for Base Station Equipment covering the essential requirements of article 3.2 of the R&TTE Directive: **ETSI EN 301 502**.
- Global System for Mobile communications (GSM); Part 4: Harmonized EN for GSM Repeaters covering the essential requirements of article 3.2 of the R&TTE Directive: **ETSI EN 300 609-4**.
- Electromagnetic compatibility and Radio Spectrum Matters (ERM) – Electromagnetic Compatibility (EMC) standard for radio equipment and services – Part 1: Common technical requirements : **ETSI EN 301 489-1**
- Specific conditions for mobile and portable radio and ancillary equipment of digital cellular radio telecommunications systems (GSM and DCS) : **ETSI EN 301 489-7 Part 7**.
- Specific conditions for GSM base stations: **ETSI EN 301 489-8 Part 8**.
- Specific conditions for Terrestrial Trunked Radio (TETRA) equipment : **ETSI EN 301 489-18 Part 18**.

4 SECRET recommendation template reminder

In this document we will use the TecRec standard template defined in D5.1 [1]. From this previous document we present in this section a short reminder of the main topics that defines the template.

The different sections presented below are needed to define every TecRec.

- TOPIC
  - Define what type of issue is addressed by the Technical Recommendation;
- DESCRIPTION
  - Define how the addressed issue is mitigated/solved by the proposed TecRec;
  - A link to an external document can be added if additional details are required";
- WP:
  - The WPs of the SECRET project related to this TecRec;
- TYPE:
  - New standard: the proposed TecRec requires creation of a new standard;
  - Standard update: the proposed TecRec requires an update of an existing standard;
  - Engineering rules: the proposed TecRec indicates engineering rules best practices;
  - Operation: the proposed TecRec indicates operation best practices;
- INVOLVED BODY:
  - The bodies that have to consider the proposed TecRec (CENELEC, ETSI….);
- TECHREC STATUS:
  - New: technical recommendation has been created;
  - Open: technical recommendation has been submitted to SECRET board;
  - Instructed: technical recommendation has been fully processed by SECRET board;
  - Closed: technical recommendation has been processed, i.e. submitted to the involved bodies or cancelled;
- MISCELLANEOUS:
  - Column used for all other topics (identification of standard to be update, TecRec status decision rational, TecRec ID…).

5 Operational Recommendations

5.1 Security Analysis in Confidential Settings (WP4_TecRec_003)

An organization scheme best practice must be set up which allows security analyses and keeps attack use cases confidential.

Topic	Security Analysis in Confidential Settings
Description	Attack use cases in railway critical infrastructures have to be confidential. Information on such attacks must be restricted to a small number of persons only. Consequently engineers building railway communication systems have to specify countermeasures without such information. An organization best practice must be put in place so that such engineers have access to *requirements* information instead of attack information. These requirements information can be illustrated by examples of attacks that are not confidential (e.g. description of a ICT WIFI attack instead).
Type	
Involved bodies	In the SECRET project, the WP1 deliverable on attack scenarios was confidential. It was not disseminated within the consortium.

5.2 Creating Knowledge Repository based on ISO 27034 (WP4_TecRec_006)

A knowledge repository providing updated information on attack, associated measures, and practice must be maintained. It is recommended to follow ISO 27034 (Application security — Organization normative framework).

Topic	Creating Knowledge Repository based on ISO 27034
Description	New attack patterns can be found out in the future. Technology may change (communication, processing architecture). Architecture for resilience may change. Guidelines for architecture resiliency evaluation must be provided This type of concern has been addressed in ISO 27034. It defines the concept of Organization Normative Framework (ONF), a knowledge repository consisting of a suite of application security-related policies, procedures, roles and tools. As stated in ISO 27034, the approach is formal and bureaucratic, e.g. a committee is needed to oversee the ONF. This is most likely to suit organizations which have or want a highly structured way of securing applications they develop.
Type	
Involved bodies	ISO

6 Engineering Rules Recommendations

6.1 Integrating Architecture Features for Communication Resiliency (WP4_TecRec_001)

Security analysis for railways communication resiliency covers architecture decisions. It must include the following features:

- An EM attack detection system
- A local health attack manager (train HAM or trackside HAM)
- A central health attack manager (CHAM)
- Multi-communication capability with dynamic reconfiguration

Topic	Integrating Architecture Features for Communication Resiliency
Description	Railway communication systems are critical assets and therefore they constitute a potential cybersecurity vulnerability. Addressing it has an impact on architecture. Note that while SECRET focused on the resilience of railways communication systems on EM attacks, these features are reusable in the presence of other cybersecurity incidents This recommendation was validated through WP4 work (simulation validation in D4.3, and use case validation in D4.5).
Type	Engineering rules
Involved bodies	Railway industry and operators

6.2 Ensuring Interoperability of Risk Analysis Methods (WP4_TecRec_002)

A common vocabulary on attacks and impact to allow security analysis methodology interoperability must be established

Topic	Ensuring Interoperability of Risk Analysis Methods
Description	Multiple risk analysis methods can be used (e.g. risk analysis for EM incident and risk analysis for ICT incident) in a critical infrastructure. These methods are interdependent and must therefore interoperate. The Bow-tie and TVRA were used in Secret to assess railway incidents and railway communication system incidents. It was realised in discussions with stakeholders familiar with one risk method that they frequently were not aware of the existence of the other method. A study of Bow-tie, TVRA, Cyberprep was then carried out using ontology tools, validating the need for common vocabulary
Type	Engineering rules
Involved bodies	Railway industry and operators

6.3 Evaluating Architecture Features for Resilience (WP4_TecRec_005)

An approach to evaluate a resilient architecture is needed, through evaluation methods or simulation, or implementation of use cases.

Topic	Evaluating Architecture Features for Resilience
Description	Because an architecture decision can have a far reaching impact on the system in terms of cost and cybersecurity preparedness, a wide consensus must be reached, i.e. technical and risk managers should be able to agree. Evaluation methods are processes where such stakeholders are involved. Simulation and use cases implementation are demonstrators which engineers can show to managers In secret, this validation was carried out in • D4.2 Annex A showed how the use of existing architecture evaluation methods (ATAM, CBAM) • D4.3 on simulation • D4.5 on two use cases
Type	Engineering rules
Involved bodies	Railway industry and operators

6.4 Transport Technology Independence in ERTMS (WP4_TecRec_007)

Ensure that the transport technology specified in ERTMS is technology independent.

Topic	Transport Technology Independence in ERTMS
Description	Nowadays, GSM-R is totally linked to the ERTMS specification. Thus, a modification of the wireless technology implies a considerable change in other fields of ERTMS such as the protocol stack for the ETCS message exchange or the definition of new QoS requirements to fulfil. This monolithic design is a handicap to propose changes because any change can have a significant impact on all the ERTMS specification sets. Although, it is important to set one specific transport technology in order to have a realistic and feasible specification, the specification should take into account the future migration towards new wireless technologies and avoid an excessive dependence with the wireless technology.
Type	Engineering rules
Involved bodies	Railway industry and operators

6.5 Moving to IP in ERTMS (WP4_TecRec_008)

It is recommended to switch from OSI-based protocol stack to IP-based protocol stack in the ERTMS specification

Topic	Moving to IP in ERTMS
Description	All the newer wireless technologies since GSM (GPRS, WiMAX, LTE, ...) are based on packet switching technology and IP protocol. Current protocols used for ERTMS are based on OSI protocols which today are hardly used outside the railway domain. Adopting the IP family of protocols, you can use new technologies and protocols in ERTMS more transparently in the future. Furthermore, the custom requirements of the railway industry could be achieved with a detailed parametrization of the protocols.
Type	Standard update
Involved bodies	

6.6 Integrating Multipath Communication in ERTMS (WP4_TecRec_009)

Use of Multipath protocols in the future IP-ERTMS specification

Topic	Integrating Multipath Communication in ERTMS
Description	Multipath protocols can provide flexibility in complex issues such as horizontal and vertical handovers. They can provide even more independency with the wireless technology, easy migrations of technologies, easy use of multiple technologies simultaneously and release applications from managing multiple connections
Type	Standard update
Involved bodies	

7 Guidelines for Architecture Design and Evaluation

This section provides guidelines for architecture design and evaluation. It includes three sections:

- The methodology description
- An example of the resulting architecture instantiation
- An example of evaluation of the resulting architecture

7.1 Methodology Description

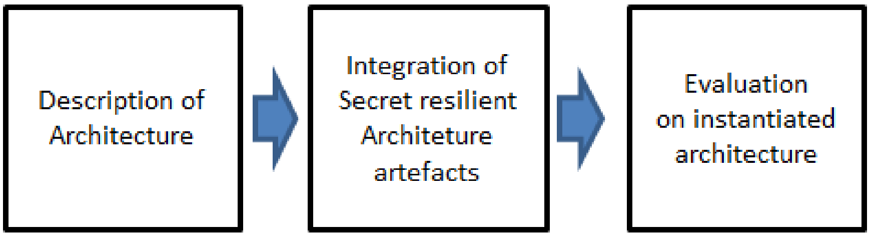

Description of Architecture
Integration of Secret resilient Architeture artefacts
Evaluation on instantiated architecture

Figure 1: Methodology

The methodology is used by stakeholders who are

- designing the architecture of a railway communication system. This case takes place when an entire system is designed from scratch.
- designing the additional architecture features of an existing railway communication system that need to address cybersecurity features. This case takes place when a design and architecture is already available.

The methodology includes the following steps as described by Figure 1:

- Step 1: Description of the architecture components. This can focus on the communication systems but also on the computing elements which are handling such systems (for instance the architecture of a controller system in a train)
- Step 2: Integration of the SECRET resilient architecture components (they are described in the next section).
- Step 3: Evaluation of resulting integration. It is important to assess the cost effectiveness of such integration. We suggest to use the ATAM (Architecture Tradeoff Analysis Method) and CBAM (Cost Benefit Analysis Method) methods[1].

7.2 Secret Resilient Architecture Components

The Resilient Communication Architecture (RCA) in the train is composed of the following main components (see Figure 2):

- Health/Attack Manager (HAM)
- Acquisition System Analyser (ASA)
- Sensors connected to the ASA
- Multipath Communication Manager (MCM)
- Several communication devices behind the MCM

[1] http://www.sei.cmu.edu/reports/03tn038.pdf

The first three components are part of what has been called the protection subsystem (see figure below). The role of this subsystem is to continuously monitor the overall network for detecting EM attacks performed on the network. The two remaining components are part of the MCM. The role of this second subsystem is to provide resilient communications between trains and the command center located at ground.

HAMs are further subdivided in to categories according to their roles:

- Train Health/Attack Management
- Trackside Health/Attack Management
- Central Health/Attack Management

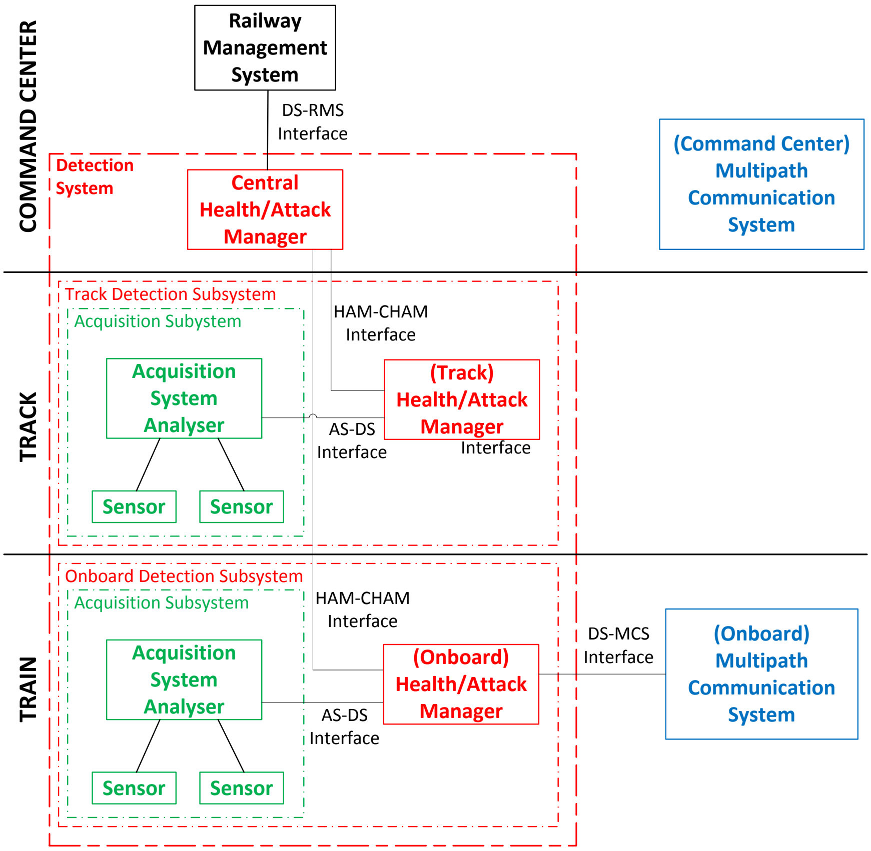

COMMAND CENTER
TRACK
TRAIN
Railway Management System
DS-RMS Interface
Detection System
Central Health/Attack Manager
(Command Center) Multipath Communication System
Track Detection Subsystem
Acquisition Subystem
Acquisition System Analyser
Sensor
Sensor
HAM-CHAM Interface
(Track) Health/Attack Manager
AS-DS Interface
Interface
Onboard Detection Subsystem
Acquisition Subystem
Acquisition System Analyser
Sensor
Sensor
HAM-CHAM Interface
(Onboard) Health/Attack Manager
AS-DS Interface
DS-MCS Interface
(Onboard) Multipath Communication System

Figure 2: Secret resilience components

7.3 Example of Architecture Instantiation

This section is based on work carried out by ALSTOM within WP5 to specify an architecture integrating Secret resilient architecture components.

The objectives was to define a typical architecture that offers qualities like resilience but also traditional qualities like authentication, confidentiality, integrity.

In order to meet such objectives, we had first to define a general system architecture for train control systems or, more generally, railway management systems.

Starting from proprietary solutions historically embedded as part of the application, the radio communication solutions are progressively based on standardized technologies benefiting as such from the leverage and sustainability of the public telecom market.

However, the railway management systems have specific requirements over the radio communications:

- Low cost and long time sustainability
- Easily extendable, scalable

- From very low to high bandwidth, in some case “real-time” capability
- Good immunity to EMC perturbation
- Servicing several applications
- Robust against intentional jammer and cyber attacks
- Highly reliable, available
- Air-gap Interoperability (from physical to application layers)
- Generally designed to allow Operation & Maintenance sub-contracting

Basically the above requirements are applicable over the two parts of the radio system, i.e. the radio mobile (train mounted or portable) and the trackside radio network.

Therefore the system architecture has to support the following concepts :

- Standardized air interface
- Allow coexistence of several radio technologies (“continuous migration”)
- Manage several concurrent communication Quality of Service (QoS)
- Comply to well-established radio frequency regulation
- Supporting standard fixed interfaces for both mobile and network equipment
- Possibly capable of jammer and intrusion detection
- Allow redundancy, ultimately meeting the “no single point of failure” condition
- Conform to railway standardization and certification bodies
- Centrally supervised for both mobile and network equipment

Consequently, the general system architecture shall highlight all physical or logical components that are needed to implement the above concepts.

7.3.1 Architecture of Radio System – Mobile Part

The following figure depicts the general Radio Mobile architecture (mobile)

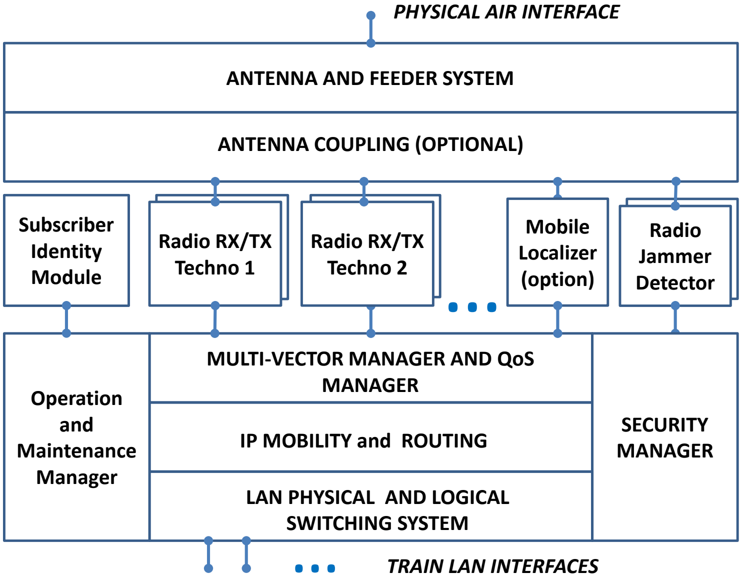

PHYSICAL AIR INTERFACE
ANTENNA AND FEEDER SYSTEM
ANTENNA COUPLING (OPTIONAL)
Subscriber Identity Module
Radio RX/TX Techno 1
Radio RX/TX Techno 2
Mobile Localizer (option)
Radio Jammer Detector
Operation and Maintenance Manager
MULTI-VECTOR MANAGER AND QoS MANAGER
IP MOBILITY and ROUTING
LAN PHYSICAL AND LOGICAL SWITCHING SYSTEM
SECURITY MANAGER
TRAIN LAN INTERFACES

Figure 3: Architecture of the Radio System - mobile part

The external interfaces and building blocks permit a breakdown of the system requirements into specific technical requirements.

- Physical air interface. The physical air interface specification includes requirements for:
    - Frequency allocation
    - Maximum equivalent radiated power and spectral density in band and out of band
- Antenna and Feeder System. The antenna and feeder system includes requirements for:
    - Omnidirectional or directional antenna
    - Single or multi frequency band
    - Antenna Gain
    - MIMO and diversity (depending on technology)
    - Maximum feeder loss
- Antenna Coupling (Optional). The antenna coupling maybe required to limit the number of train antennas.
- Radio Transceiver RX/TX. The radio transceiver RX/TX includes requirements for:
    - Radio Technology (standardized physical and management layers of the air interface)
    - Min signal sensitivity level
    - Medium access control (MAC) protocol layer
    - Radio QoS feature
    - Radio mobility management (cell change)
    - Radio link encryption
    - Redundancy concept
- Subscriber Identity Module. The subscriber identity module is needed to hold the subscriber profile provided by the radio network operator. It can also contain information related to the application performance/QoS and security profile.
- Mobile Localizer (Option). The mobile localizer may be required to perform consistent multi-vector management, and could also be valuable for security and O&M management. The interoperability of train localizer should not be required.
- Radio Jammer Detector. The radio jammer detector becomes more and more relevant to detect denial of service (DoS) attack at the physical air interface. It may be a valuable input for the multi-vector and security managers.
- Multi-vector and QoS Manager. The multi-vector and QoS manager shall include requirements for:
    - Radio transceiver network registration and service attachment
    - Radio transceiver selection criteria and associated management algorithms
    - Radio transceiver lossless switch-over
    - IP protocol context activation
    - Radio resources allocation to IP streams in accordance with QoS profile
    - Optionally, IP load sharing among radio resources
- IP Mobility and Routing. The IP mobility and routing includes requirements for:
    - IP address resolution and IP mobility (IPv4, IPv6)
    - QoS mapping per IP application packet streams
    - IP routing over train LAN interfaces
    - IP security protocols (IPsec, VPN, ...)

- LAN physical and logical switching system. The LAN physical and logical switching system includes requirements for:
  - LAN technology (Standardized physical, MAC layers, …)
  - Physical port configuration
  - Virtual LAN (VLAN) prioritization and QoS mapping
- Security Manager. The security manager includes requirements for:
  - Radio jammer detection monitoring
  - Mobile LAN secured partitioning
  - Perimeter protection : firewall, network intrusion detection, passive access monitoring
  - Web-based access security management (for O&M)
  - IPsec, VPN security management (authentication, key management)
- Operation & maintenance manager. The Operation & Maintenance manager of the Radio Mobile includes requirements for remote :
  - Configuration management
  - Fault Monitoring
  - Performance Monitoring

7.3.2 Architecture of Radio System – Network Part

The following figure depicts the general Radio Mobile architecture (network)

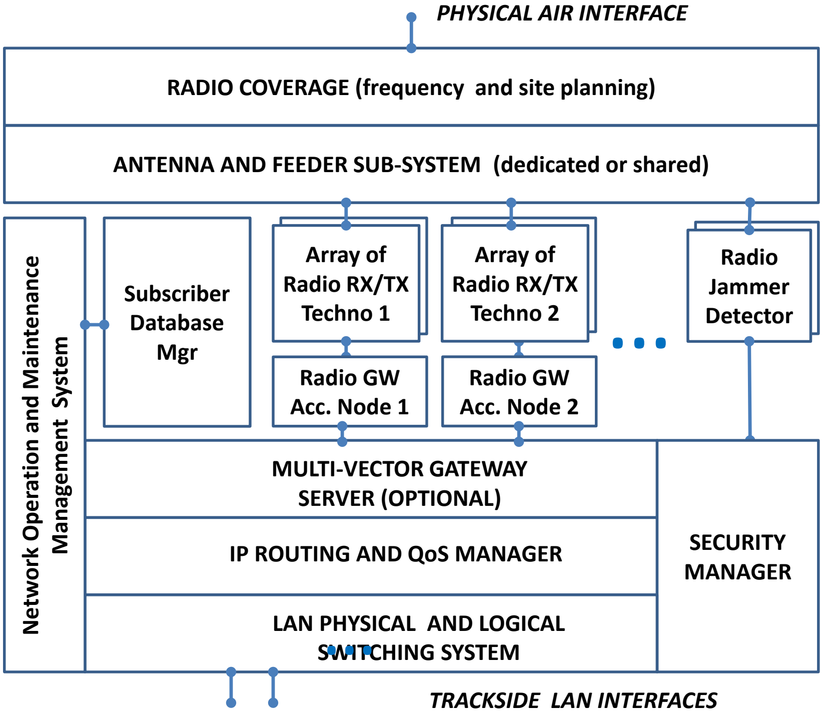

PHYSICAL AIR INTERFACE
RADIO COVERAGE (frequency and site planning)
ANTENNA AND FEEDER SUB-SYSTEM (dedicated or shared)
Network Operation and Maintenance Management System
Subscriber Database Mgr
Array of Radio RX/TX Techno 1
Array of Radio RX/TX Techno 2
Radio Jammer Detector
Radio GW Acc. Node 1
Radio GW Acc. Node 2
MULTI-VECTOR GATEWAY SERVER (OPTIONAL)
IP ROUTING AND QoS MANAGER
LAN PHYSICAL AND LOGICAL SWITCHING SYSTEM
SECURITY MANAGER
TRACKSIDE LAN INTERFACES

Figure 4: Architecture of the Radio System - network part

The external interfaces and building blocks permit a breakdown of the system requirements into specific technical requirements.

- Radio Coverage (frequency and site planning). The Radio Coverage frequency and site planning includes requirements for:
  - Radio spectrum survey and monitoring
  - Frequency allocation and emitted power constraints in line with regulation

  - Min Radio coverage level, possibly according train speed and performance criteria
  - Radio cell planning
  - Concept of redundant coverage (single or dual layer, …)
  - Engineering guidelines for possible site sharing and radio interference management
  - Radio propagation modelling vs radiating components and environmental data
- Antenna and Feeder Sub-System (dedicated or shared). The antenna and feeder sub-system includes requirements for:
  - Selection of radiating component according environmental conditions (antenna type, leaky feeder, ..)
  - Possible sharing of radiating components between Radio Transceivers
  - Single or multi frequency band
  - Antenna type and Gain
  - MIMO and diversity (depending on technology)
  - Maximum feeder loss

- Array of Radio Transceiver RX/TX. The radio transceiver RX/TX includes requirements for:
  - Radio spectrum management
  - Radio Technology (standardized physical and management layers of the air interface)
  - Min signal sensitivity level
  - Medium access control (MAC) protocol layer
  - Radio QoS feature
  - Radio mobility management (cell change)
  - Radio link encryption
  - Redundancy concept
- Radio Jammer Detector. The radio jammer detector becomes more and more relevant to detect denial of service (DoS) attack at the physical air interface. It may be a valuable input for the network operation and maintenance and security managers.
- Subscriber database Manager. The subscriber database manager includes requirements for:
  - Managing the details of each mobile subscriber identity as stored in the subscriber identity module.
  - Managing subscriber access rights in the subscriber home network
  - Managing exchange of subscriber access rights in case of inter-network roaming
  - Managing the application performance/QoS and security subscriber profile
- Radio Gateway Access Node. The Radio Gateway Access Node includes requirements for:
  - Allocating the mobile IP addresses and sub-netting following the mobile IP context activation (access point management)
  - Managing the mobile localization vs radio cells

  - Managing the IP packet flow context (QoS)
  - Inter-networking between radio and IP networks
- Multi-vector Gateway Server. The Multi-vector Gateway server includes requirements for:
  - Radio network selection criteria and associated management algorithms
  - Radio network lossless switch-over
  - Radio network allocation to IP streams in accordance with QoS profile
  - Optionally, IP load sharing among radio networks
- IP Routing and QoS Manager. The IP mobility and routing includes requirements for:
  - IP address resolution and IP mobility (IPv4, IPv6)
  - QoS mapping per IP application packet streams
  - IP routing over fixed LAN interfaces
  - IP security protocols (IPsec, VPN, ...)
- Security Manager. The security manager includes requirements for:
  - Radio network jammer detection monitoring
  - Fixed LAN secured partitioning
  - Perimeter protection : firewall, network intrusion detection, passive access monitoring
  - Web-based access security management (for O&M)
  - IPsec, VPN security management (authentication, key management)
- Network Operation and Maintenance Management System. The Operation & Maintenance manager of the Radio Network includes requirements for remote :
  - Configuration management
  - Fault Monitoring
  - Performance Monitoring
  - Management of Subscriber Service Level Agreement
- LAN physical and logical switching system. The LAN physical and logical switching system shall include requirements for:
  - LAN technology (Standardized physical, MAC layers, …)
  - Physical port configuration
  - Virtual LAN (VLAN) prioritization and QoS mapping

7.3.3 Integration of SECRET Resilient Architecture Components

The table shows the mapping between SECRET resilient architecture components and the instantiated architecture components.

Secret components	Radio system (Train)	Radio system (Track)
Health Attack Manager (HAM)	Security manager	Security manager
Acquisition System Analyser (ASA)	Security manager	Security manager
Sensors connected to the ASA	Radio Jammer Detector	Radio Jammer Detector
Multipath Communication Manager (MCM)	Multi-vector manager and QoS manager, IP mobility and routing	Multi-vector gateway server, IP Routing and QoS manager

Several communication devices behind the MCM	Lan Physical and Logical Switching system	Lan Physical and Logical Switching system

7.4 Example of Architecture Evaluation

This section describes the ATAM and CBAM methods. ATAM and CBAM are to our knowledge the most widely used or known architecture evaluation methods used. This section is based on the following reference:

> [CMU software architecture in practice]: *Software architecture in Practice. 3rd edition. Addison Wesley, 2013. Len Bass, Paul Clements, Rick Kazman.*

This section is structured as follows:

- We first start with an introduction section on architectures and what it entails
- We then explain the ATAM method
- We then explain the CBAM method

7.4.1 Introduction to Architecture Design

There are a number of reasons on why architecture is important:

- Inhibit or enable a system’s quality attribute
- Reason about and manage change
- Prediction of system’s qualities
- Documented architecture for communication among stakeholders
- Allow for the earliest, most fundamental hardest-to-change design decisions
- Defines set of constraints on implementation
- Dictates structure of organisation and vice-versa
- Basis for evolutionary prototyping
- Allows architecture and project manager to reasons about cost and schedule
- Can be created as a transferable reusable model
- Architecture based development focus on assembly of components, not only their creation
- Restrict design alternatives, reduces design and system complexity
- Foundation for training a new team member

Among these reasons, we single out the prediction or system’s quality. This has an impact in the elicitation of the requirements of a system. Several types of requirements are identified:

- ***Functional requirements*** relate to what a system does (e.g. engine control). Another term used in the literature is r*esponsibility*.
- ***Quality attributes requirements*** relate to how well a system does it. Examples of quality attributes could be execution qualities (e.g. security, usability, dependability), evolution qualities (testability, maintainability, scalability), business qualities (time to market, cost. Another term that is close is non-functional requirement[2].
- ***Constraints*** are design decisions that are already taken (e.g. re-use something, use a given operating system, use IP V6)

[2] https://en.wikipedia.org/wiki/Non-functional_requirement.

These requirements lead to architecture decisions: functional requirements are satisfied by defining appropriate set of responsibilities within design. Quality attributes are satisfied by structures and behaviors of the architecture.

Quality Attributes

The approach is to specify scenarios, which are structured means to state attribute requirements. A scenario includes the following elements:

- Source At security level, the source is typically an attacker
- Stimulus. At security level, the stimulus is typically an attack e.g. an EM attack
- The stimulated Artefact. At security level, the stimulated artefact is typically the system being attacked.
- The Environment or the conditions under which a stimulus occurs (e.g. normal train operation)
- The Response to the stimulus. The response is influenced by architecture techniques called Architecture tactics (e.g. switch to manual mode operation)
- The Response Measure. This measure is needed in the design process in order to validate the architecture design (e.g. train still in operation at 200 km/h)

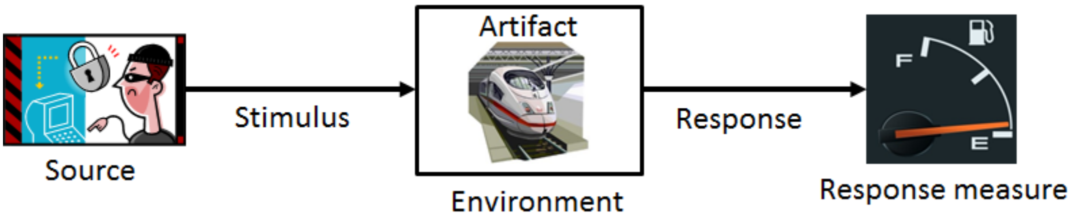


Figure 5: Scenario Model

Figure 5 shows the resulting scenario model. The whole design process can be described as involving three steps:

- Identification of scenarios.
- Influencing the responses by selecting appropriate architecture techniques called in CMU jargon **architecture tactics**.
- Measuring the responses in order to validate the design decisions

An ***architecture tactic*** is a design decision that includes the achievement of a quality attribute response

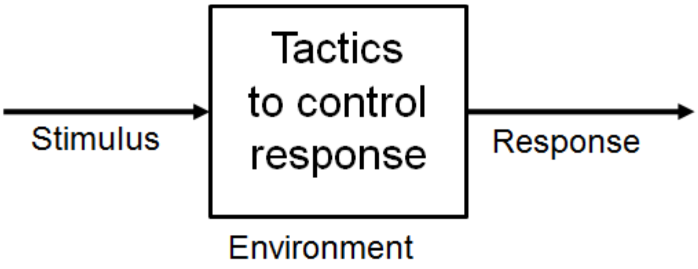


Figure 6: Architecture Tactic

Figure 6 shows where tactics artefacts are displayed in a the scenario model.

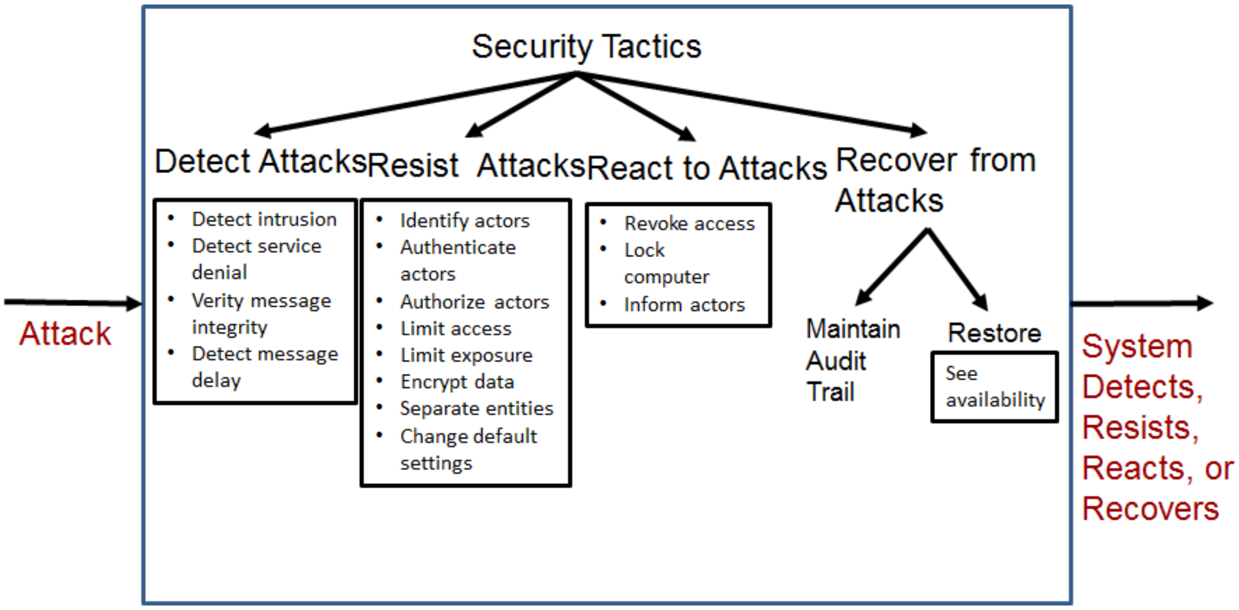


Figure 7: Example of Tactics for Security Attribute

Figure 7 shows the taxonomy of security tactics. Reference 1 provides lists of tactics for a good number of attributes.

Quality attributes are further associated with ***response models***, or functions to predict the response measures given a stimulus for a particular architecture. There are two known approaches for such models:

- analytic models which support quantitative analysis (e.g. Markov models for hardware availability, scheduling theory for predictability),
- check lists/guidelines which support scales (e.g. common criteria level, safety integrity levels).

7.4.2 Architecture Tradeoff Analysis Method (ATAM)

In ATAM, architecture requirements are also known as ***ASR (architecturally significant requirement)***. These requirements are captured in multi-stakeholder workshops (e.g. project managers, members of development team, testers and integrators, maintainers, product line application builders, customers, end users, business managers …). These ASR are specified through ***utility trees***, consisting of 3 levels:

- Level 1 in the tree will describe quality attributes (e.g. performance)
- Level 2 in the tree will describe attribute refinements (e.g. latency)
- Level 3 in the tree will describe the ASR through the following
    - A quality attribute scenario
    - A business value (high, medium, low)
    - An architecture impact value (high, medium, low)

The table below shows 3 examples of utility tree

Level 1	Quality attribute	Performance
Level 2	Attribute refinement	Throughput
Level 3	ASR	At peak load, system is able to complete 150 transations per second
	Business value	Medium
	Impact on	Medium

	architecture	

Level 1	Quality attribute	Security
Level 2	Attribute refinement	Integrity
Level 3	ASR	System resists intrusion and reports intrusion within 90 seconds
	Business value	High
	Impact on architecture	Medium

Level 1	Quality attribute	Configurability
Level 2	Attribute refinement	User-defined changes
Level 3	ASR	A hospital increases the fee for a particular service. Configuration team makes the change in 1 working day
	Business value	High
	Impact on architecture	Medium

The architecture design process ATAM is iteration-based. Each iteration is described with an input, an iteration process and an output. The input is a list of requirements (functional, quality, constraints) and architecture requirements. The output consists of sketches of architectural views. The iteration process includes the following steps:

- The selection of the element of the system to design
- The identification of ASR (architecturally significant requirements) for that part
- The generation of a design solution
- An inventory of remaining requirements and selection of input for the next iterations.

The resulting documentation consists of a number of models. Reference 1 suggests three types of models:

- Modules views which provide a static view or a focus on the decomposition into elements of a system.
- Component and connectors views which provide a dynamic view or a focus on the interactions between elements
- Other views dedicated to the specification of mapping issues to specific environments, i.e. organisation, development, installation. For instance a software architecture consisting of software modules must be mapped on top of a hardware architecture through an allocation view).

When the same design decision is found repeatedly, ***architecture patterns*** are used, i.e. documentation and models can be made readily available for future re-use. Examples of well-known patterns are the following: layers, client-server, publish-subscribe, shared data, isolation.

The application of ATAM involves a well-defined organisation. Participants include

- the evaluation team. It involves specific, important roles:
    - a team leader (in charge of customer relation)
    - an evaluation leader (in charge of the evaluation)

  - a scenario scribe (which lists the proposed scenarios)
  - a proceedings scribe (which lists the adopted scenarios)
  - a questioner (which raises issues of architectural interest in the area where he has expertise)
- the project decision makers
- the architecture stakeholders. These stakeholders could be many in large projects (up to 12 to 15 persons). They do not participate to the entire exercise

The application of ATAM involves a well-defined process with the following phases:

- a preparation phase. It involves the evaluation team and project decision makers. The duration is a few weeks.
- a first evaluation phase. This phase lasts 1-2 days. It involves the evaluation team and the project decision makers. The ATAM process is presented, then business drivers are presented, then the architecture is presented, approaches are identified, and utility trees are identified.
- a evaluation phase which takes place 1 to 3 weeks later. This phase lasts 2 days. It involves architect stakeholders. In this phase, brainstorming and prioritisation of scenarios take place.
- a follow-up phase where the evaluation team provides a final report.

A lightweight version of ATAM is also available (4 to 6 hours).

7.4.3 Cost Benefit Analysis Method (CBAM)

CBAM (Cost Benefit Analysis Method) takes place after ATAM. The objective is to maximise the difference between the benefit derived from system and the cost of implementing the design as showed in Figure 8.

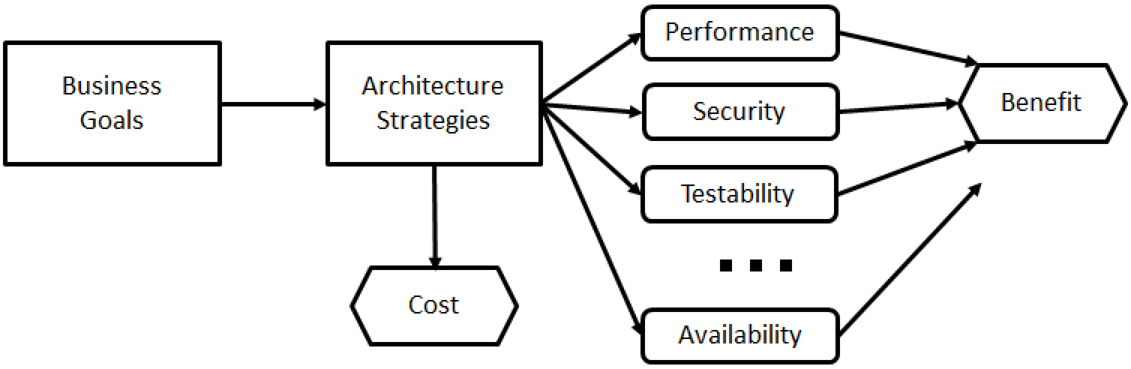


Figure 8: Cost VS Benefit

Basically the objective is to "measure" the utility of a tactic (for performance, security, testability, availability and so forth…). This necessitates the definition of a ***utility-response curve***. Such curves are in general different from one tactic to another. They also depend on the context, i.e. they will change from one company to another. The approach in general is to vary the values of the responses (e.g. a and b in Figure 9) and to "agree" on a utility value (from 0 to 100). For instance a 99.99 percent availability could have an utility of 90/100 while a 90 percent availability could a have a utility of 10.

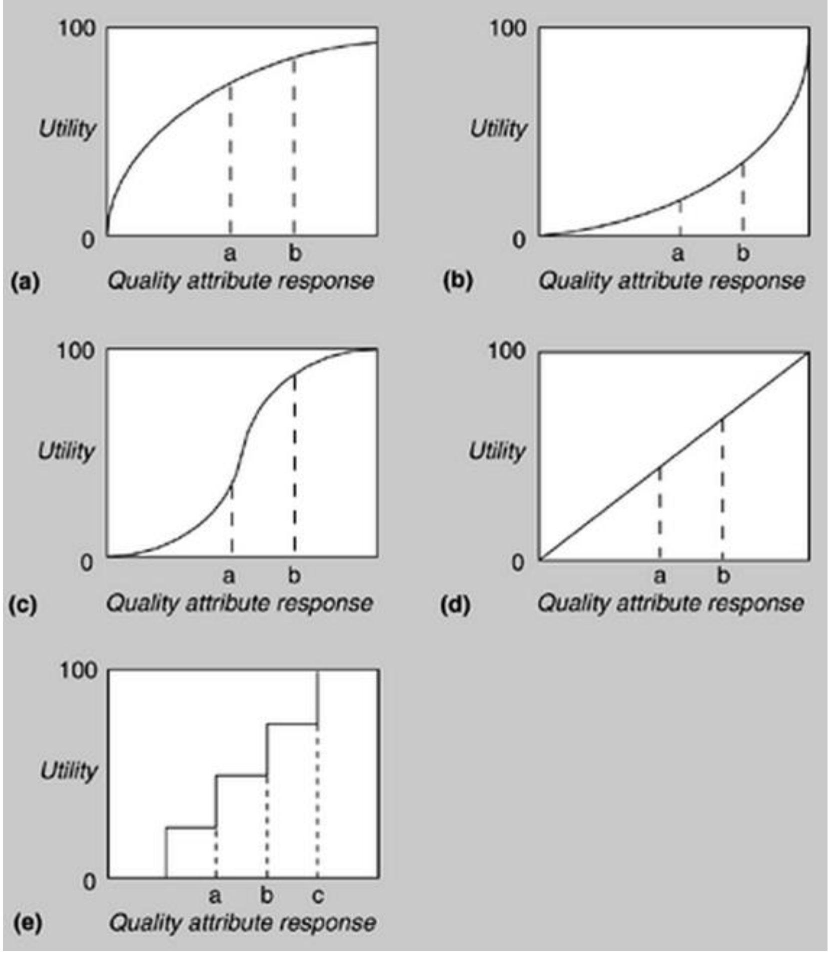


Figure 9: Utility-Response Curves (from Ref 1)

CBAM uses the following metrics:

- Benefit: **B_i**, defined as follows:
  - i denotes a **strategy i**.
  - Strategy I is described through **j scenarios**.
  - Each scenario I receives a **weight W_j**
  - **b_{ij}** is the change in utility caused by scenario j using a utility-response curve (**b_{ij}** $= U_{expected} – U_{current}$)
  - **B_i** is the sum of all changes taking into account the weight : **$B_i = \Sigma_j(b_{ij} \times W_j)$**
- Value for cost, **VFC**, defined as follows:
  - Ci is the cost of implementing architecture Strategy i
  - VFC is the ratio benefit/cost (VFC = Bi / Ci)

Evaluation using CBAM

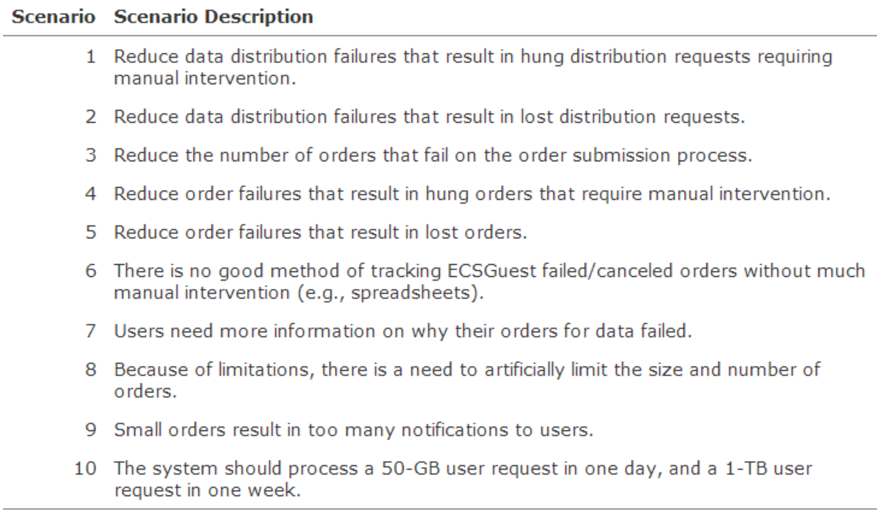
It is important to understand the following points in CBAM: Utility curves and weights are based on **heuristics which depend on corporate decisions and knowledge. The overall quality and accuracy of CBAM the measure therefore depends on a good understanding of how these values are assigned.**

The proposed practice is as follows:

- Utility-response curves are obtained by providing at least the following four values:
  - The best case quality-attribute level which receives value 100. For instance a response time of 0.1 second receives value 100.

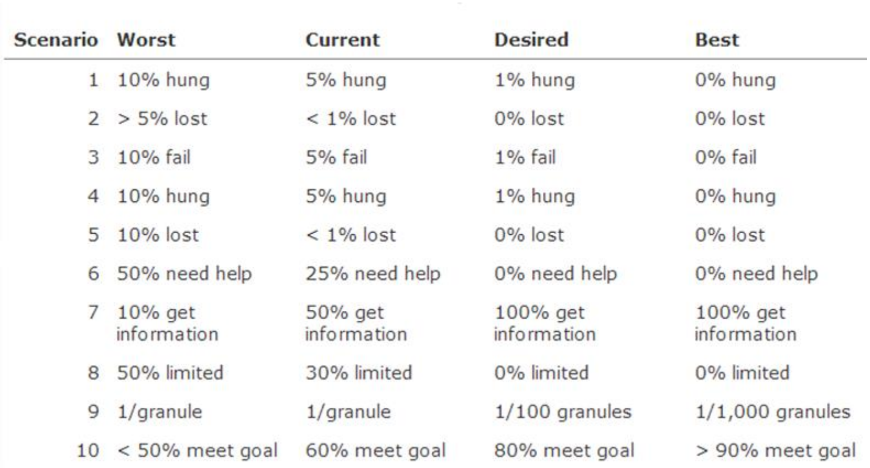
  - The worst case quality-attribute level which receives value 0.
  - The current quality-attribute level
  - The desired quality-attribute level
- Weights of scenarios are determined as follows. The N scenarios are prioritized (from 1 to N). Each stakeholder (e.g. project manager, business manager, developer…) provides a priority list. The weight is the sum.
- Costs values are decided in the organization, e.g. as a scale (e.g. the cost of A is X, while the cost of B is 1.5X)
- The evaluation work includes the following phases:
- Step 1: collate scenarios and prioritise them according to business goals (high, medium, low). Select the top third for further consideration.
- Step 2: refine scenarios. In this step, worst case, current, desired, best case quality attributes level are determined
- Step 3: prioritise scenarios. Each stakeholder receives 100 votes. Choose the top 50 percent. Assign weight of 1.0 to highest rated scenario. Assign related weight to others.
- Step 4: assign utility-response curve for step 3 scenarios
- Step 5: identify architectural strategies and associated scenarios. Determine their expected QA response level
- Step 6: Determine the utility of the expected QA response levels by interpolation
- Step 7: Calculate total benefit obtained from an architectural strategy
- Step 8: Select architectural strategy based on VFC (compatible with cost and schedule constraints)
- Step 9: confirm results with intuition

Here is an example (from [CMU software architecture in practice]), an earth observing system (constellation of NASA satellite):



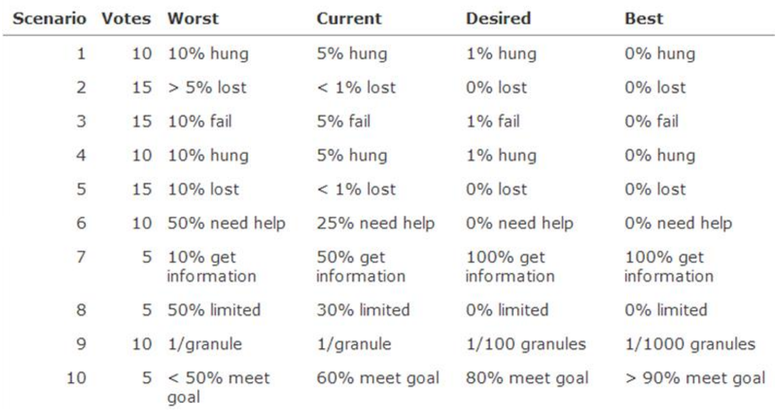
Scenario	Scenario Description
1	Reduce data distribution failures that result in hung distribution requests requiring manual intervention.
2	Reduce data distribution failures that result in lost distribution requests.
3	Reduce the number of orders that fail on the order submission process.
4	Reduce order failures that result in hung orders that require manual intervention.
5	Reduce order failures that result in lost orders.
6	There is no good method of tracking ECSGuest failed/canceled orders without much manual intervention (e.g., spreadsheets).
7	Users need more information on why their orders for data failed.
8	Because of limitations, there is a need to artificially limit the size and number of orders.
9	Small orders result in too many notifications to users.
10	The system should process a 50-GB user request in one day, and a 1-TB user request in one week.

Figure 10: Step 1. Collate scenarios



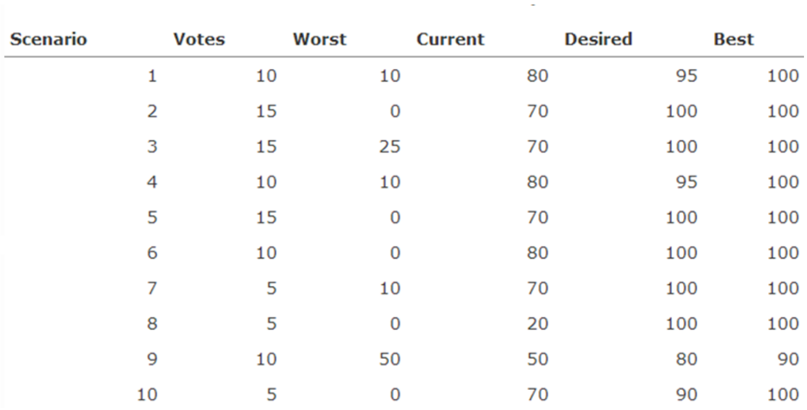
Scenario	Worst	Current	Desired	Best
1	10% hung	5% hung	1% hung	0% hung
2	> 5% lost	< 1% lost	0% lost	0% lost
3	10% fail	5% fail	1% fail	0% fail
4	10% hung	5% hung	1% hung	0% hung
5	10% lost	< 1% lost	0% lost	0% lost
6	50% need help	25% need help	0% need help	0% need help
7	10% get information	50% get information	100% get information	100% get information
8	50% limited	30% limited	0% limited	0% limited
9	1/granule	1/granule	1/100 granules	1/1,000 granules
10	< 50% meet goal	60% meet goal	80% meet goal	> 90% meet goal

Figure 11: Step 2 Refine scenarios



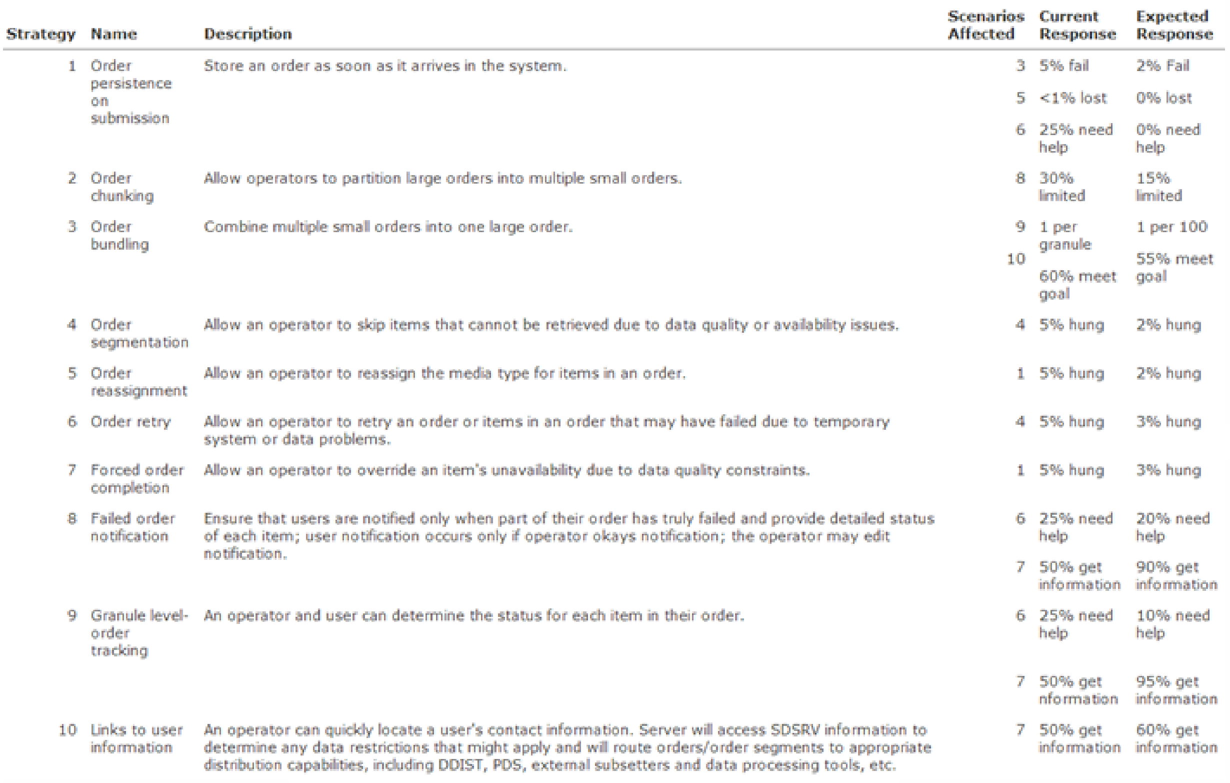
Scenario	Votes	Worst	Current	Desired	Best
1	10	10% hung	5% hung	1% hung	0% hung
2	15	> 5% lost	< 1% lost	0% lost	0% lost
3	15	10% fail	5% fail	1% fail	0% fail
4	10	10% hung	5% hung	1% hung	0% hung
5	15	10% lost	< 1% lost	0% lost	0% lost
6	10	50% need help	25% need help	0% need help	0% need help
7	5	10% get information	50% get information	100% get information	100% get information
8	5	50% limited	30% limited	0% limited	0% limited
9	10	1/granule	1/granule	1/100 granules	1/1000 granules
10	5	< 50% meet goal	60% meet goal	80% meet goal	> 90% meet goal

Figure 12: Step 3 Prioritise scenarios



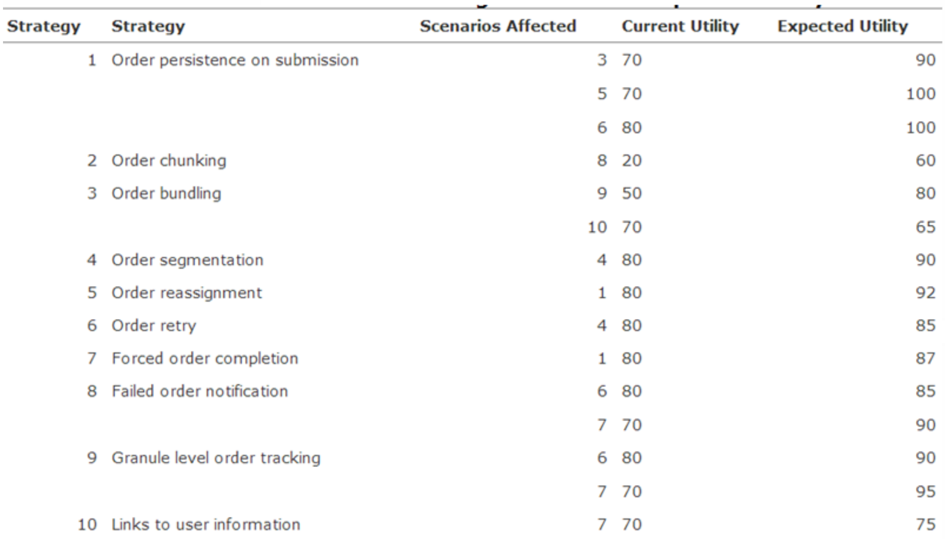
Scenario	Votes	Worst	Current	Desired	Best
1	10	10	80	95	100
2	15	0	70	100	100
3	15	25	70	100	100
4	10	10	80	95	100
5	15	0	70	100	100
6	10	0	80	100	100
7	5	10	70	100	100
8	5	0	20	100	100
9	10	50	50	80	90
10	5	0	70	90	100

Figure 13: Step 4 Assign utility



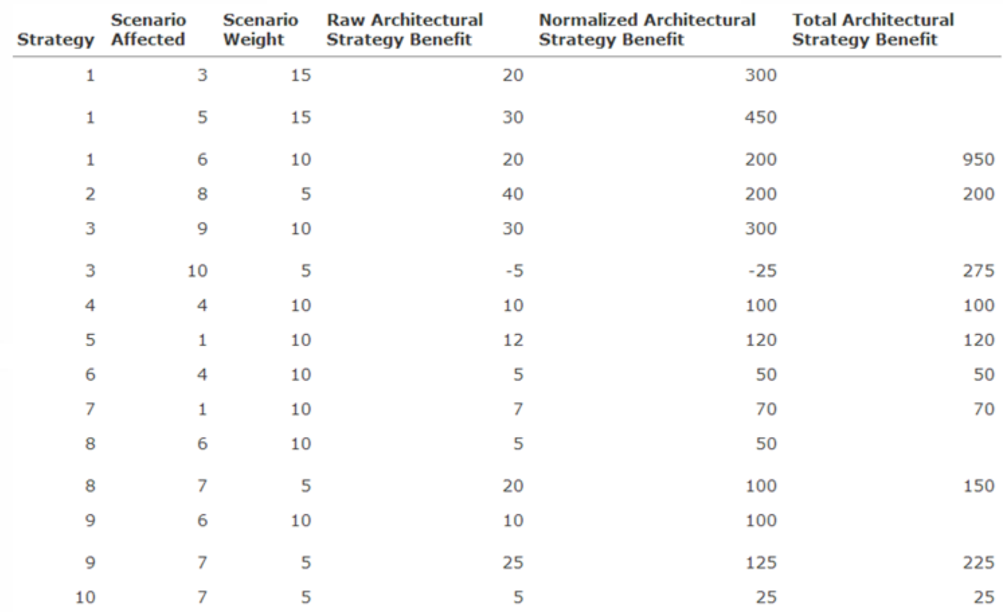
Strategy	Name	Description	Scenarios Affected	Current Response	Expected Response
1	Order persistence on submission	Store an order as soon as it arrives in the system.	3 5 6	5% fail <1% lost 25% need help	2% Fail 0% lost 0% need help
2	Order chunking	Allow operators to partition large orders into multiple small orders.	8	30% limited	15% limited
3	Order bundling	Combine multiple small orders into one large order.	9 10	1 per granule 60% meet goal	1 per 100 55% meet goal
4	Order segmentation	Allow an operator to skip items that cannot be retrieved due to data quality or availability issues.	4	5% hung	2% hung
5	Order reassignment	Allow an operator to reassign the media type for items in an order.	1	5% hung	2% hung
6	Order retry	Allow an operator to retry an order or items in an order that may have failed due to temporary system or data problems.	4	5% hung	3% hung
7	Forced order completion	Allow an operator to override an item's unavailability due to data quality constraints.	1	5% hung	3% hung
8	Failed order notification	Ensure that users are notified only when part of their order has truly failed and provide detailed status of each item; user notification occurs only if operator okays notification; the operator may edit notification.	6 7	25% need help 50% get information	20% need help 90% get information
9	Granule level-order tracking	An operator and user can determine the status for each item in their order.	6 7	25% need help 50% get nformation	10% need help 95% get information
10	Links to user information	An operator can quickly locate a user's contact information. Server will access SDSRV information to determine any data restrictions that might apply and will route orders/order segments to appropriate distribution capabilities, including DDIST, PDS, external subsetters and data processing tools, etc.	7	50% get information	60% get information

Figure 14: Step 5 Architectural Strategies and Determining Expected QA Response Level



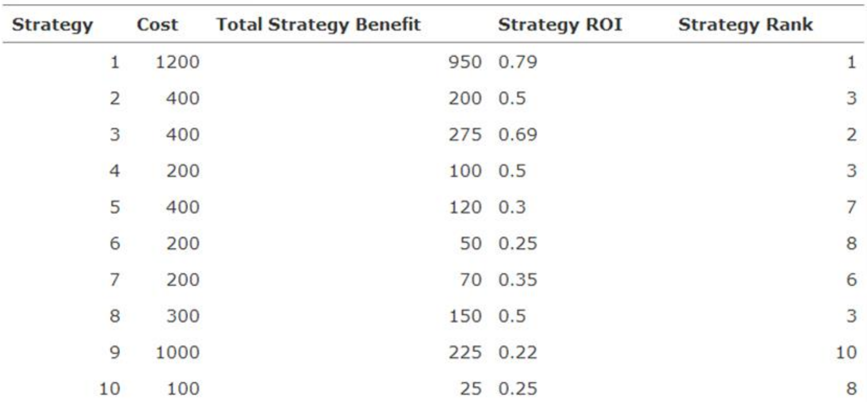
Strategy	Strategy	Scenarios Affected	Current Utility	Expected Utility
1	Order persistence on submission	3	70	90
		5	70	100
		6	80	100
2	Order chunking	8	20	60
3	Order bundling	9	50	80
		10	70	65
4	Order segmentation	4	80	90
5	Order reassignment	1	80	92
6	Order retry	4	80	85
7	Forced order completion	1	80	87
8	Failed order notification	6	80	85
		7	70	90
9	Granule level order tracking	6	80	90
		7	70	95
10	Links to user information	7	70	75

Figure 15: Step 6 Utility of Expected QA Response Levels



Strategy	Scenario Affected	Scenario Weight	Raw Architectural Strategy Benefit	Normalized Architectural Strategy Benefit	Total Architectural Strategy Benefit
1	3	15	20	300	
1	5	15	30	450	
1	6	10	20	200	950
2	8	5	40	200	200
3	9	10	30	300	
3	10	5	-5	-25	275
4	4	10	10	100	100
5	1	10	12	120	120
6	4	10	5	50	50
7	1	10	7	70	70
8	6	10	5	50	
8	7	5	20	100	150
9	6	10	10	100	
9	7	5	25	125	225
10	7	5	5	25	25

Figure 16: Step 7 Benefit Obtained from an Architectural Strategy



Strategy	Cost	Total Strategy Benefit	Strategy ROI	Strategy Rank
1	1200	950	0.79	1
2	400	200	0.5	3
3	400	275	0.69	2
4	200	100	0.5	3
5	400	120	0.3	7
6	200	50	0.25	8
7	200	70	0.35	6
8	300	150	0.5	3
9	1000	225	0.22	10
10	100	25	0.25	8

Figure 17: Step8 Select architectural strategy based on VFC

7.4.4 Applying ATAM to SECRET

Two types of scenarios were identified:

- EMC based scenario attacks using the architecture description in Figure 2.
- Associated scenarios (maintainability, survivability, interoperability…).

The scenarios will include unknown X (in bold italic) whenever appropriate.

List of ASR Train Levels

Level 1	**Quality attribute**	**Security**
Level 2	Attribute refinement	Resilience
Level 3	ASR	**Train level** Sensor detects EMC attack ***pattern X1*** and reports intrusion within 10 seconds to acquisition system which reports to on-board HAM
	Business value	High
	Impact on architecture	Medium

Level 1	**Quality attribute**	**Security**
Level 2	Attribute refinement	Resilience
Level 3	ASR	**Train level** Acquisition system detects sensors error behaviors that might have been caused by multiple EMC attacks (***pattern X2***) which reports to on-board HAM
	Business value	High
	Impact on architecture	Medium

Level 1	**Quality attribute**	**Security**
Level 2	Attribute refinement	Resilience
Level 3	ASR	**Train level** Acquisition system does not behave properly with on-board HAM which detects a possible attack (***pattern X3***) which reports to on-board HAM
	Business value	High
	Impact on architecture	Medium

Level 1	**Quality attribute**	**Security**
Level 2	Attribute refinement	Resilience
Level 3	ASR	**Train level** Train communication system channel no longer operational because of EMC attack (***pattern X4***). MCS selects another communication channel within 1 second
	Business value	High

	Impact on architecture	Medium

List of ASR Track Levels

Level 1	**Quality attribute**	**Security**
Level 2	Attribute refinement	Resilience
Level 3	ASR	**Track level** Sensor detects EMC attack ***pattern X1*** and reports intrusion within 10 seconds to acquisition system which reports to on-board HAM
	Business value	High
	Impact on architecture	Medium

Level 1	**Quality attribute**	**Security**
Level 2	Attribute refinement	Resilience
Level 3	ASR	**Track level** Acquisition system detects sensors error behaviors that might have been caused by multiple EMC attacks (***pattern X2***) which reports to on-board HAM
	Business value	High
	Impact on architecture	Medium

Level 1	**Quality attribute**	**Security**
Level 2	Attribute refinement	Resilience
Level 3	ASR	**Track level** Acquisition system does not behave properly with on-board HAM which detects a possible attack (***pattern X3***) which reports to on-board HAM
	Business value	High
	Impact on architecture	Medium

8 Conclusion

This deliverable describes the recommendations coming from different studies and discussions performed in WP4 “Dynamic protection: detection system for resilient architecture”.

The objective of these recommendations is to minimize the impact of jamming on the communications within the Railways.

Finally a long section of the deliverable is devoted to a certain number of guilines for the design of the Secret Resilient Architecture Components.