DAY 3

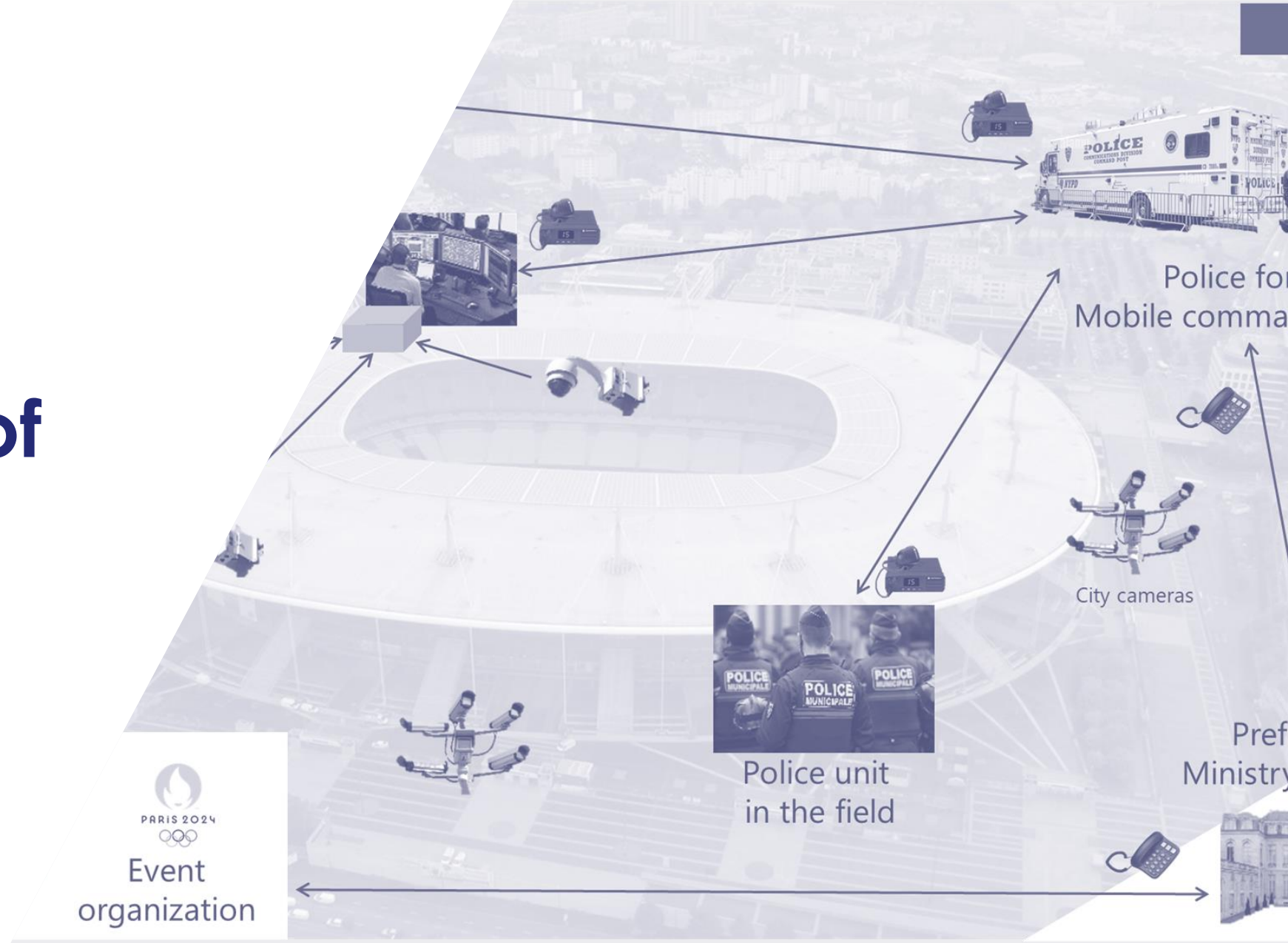
THALES
Building a future we can all trust

# Advanced Model-Based Systems Engineering

## Model-based Architecting to cope with growing complexity

www.thalesgroup.com

# Restitution of Exercise 2



# Case Study: Concept

# Architectural Concept

**A security-centered, digital based surveillance organization for international events. Deployable in mainland France, starting at the Stade de France at Saint-Denis.**

## > Security-centered:

- The security concern is at the heart of the solution
  - Security of participants, of the public and of the infrastructures, against internal and external threats
  - Security of communications between operators

## > Digital based

- invites to take advantage of new technologies to support operations and seamless collaboration between operators
  - Drone swarms would be used to get on-demand visualization and situation assessment
  - Highly-reliable communications between stakeholders
  - All data sources available in the nearby of the stadium will be exploited. If required, new CCTV cameras may be installed

## > Starting at the Stade de France

- Defines a preliminary scope of the solution and hence a set of relevant (and less relevant) stakeholders

"As-is"


Police unit
in the field

Private Security
Station


Police force
Mobile command center

City cameras


Police unit
in the field

Prefecture /
Ministry of Interior

Transportation
authorities

Event
organization

MAIRIE DE PARIS

"To-be"


Police unit
in the field

NEW

NEW
City cameras video

NEW

Situation awareness,
videoconference, ...

Police Mobile Command
and Control Center

NEW
Stadium cameras video

Private
Security
Station

NEW

NEW

M 13

City cameras

RER

NEW

NEW

NEW

Police unit
in the field

Prefecture /
Ministry of Interior

NEW

NEW

RATP
Transportation
authorities

PARIS 2024
Event
organization

# FRESUS : FRench Events' SUrveillance Solution

## SoS Missions, High-level Capabilities and Key Constraints

Crowd management and control

M

Summary

Surveillance systems can be part of managing access to a specific area, ensuring only authorized individuals enter. Also includes monitoring and optimization of access flows.

Disorders and emergency response

M

Summary

Support public safety by aiding in the identification of disorders, accidents, fires, or emergencies in monitored areas, alerting the appropriate response teams and intervening

Law enforcement

M

Summary

Surveillance systems aid law enforcement by monitoring public spaces for illegal activities, suspicious behavior, or wanted individuals.

**Monitoring**

C

Summary

Continuous or scheduled monitoring of a specific location to ensure security and safety. Common sensors include cameras (night, thermal, ...) and audio, but also social networks. Common monitoring devices are screens, including protable ones.

**Detection**

C

Summary

Detect events or occurrences. This includes detecting movement or changes in the monitored area, identifying faces or license plates, recognizing suspicious activities, and more. Also includes detection of attacks against the solution (e.g. cybersecurity attacks)

**Alerting**

C

Summary

Send alerts or notifications (like alarms, text messages, or email alerts) to appropriate parties when there's a specified trigger—for instance, detecting movement in a secured area off-hours.

**Analysis**

C

Summary

Analyze the situation (incl. people's behavior, identifying suspicious or unusual activities for further attention) and provide recommendations of course of actions

**Intervention**

C

Summary

Execute automatic actions, like turning on lights or close a gate

**Recording**

C

Summary

Record images, video and audio data for later review. This recorded material can be stored onsite, offsite, or in the cloud for retrieval if required, such as after a security incident

{C} Integration with other existing systems

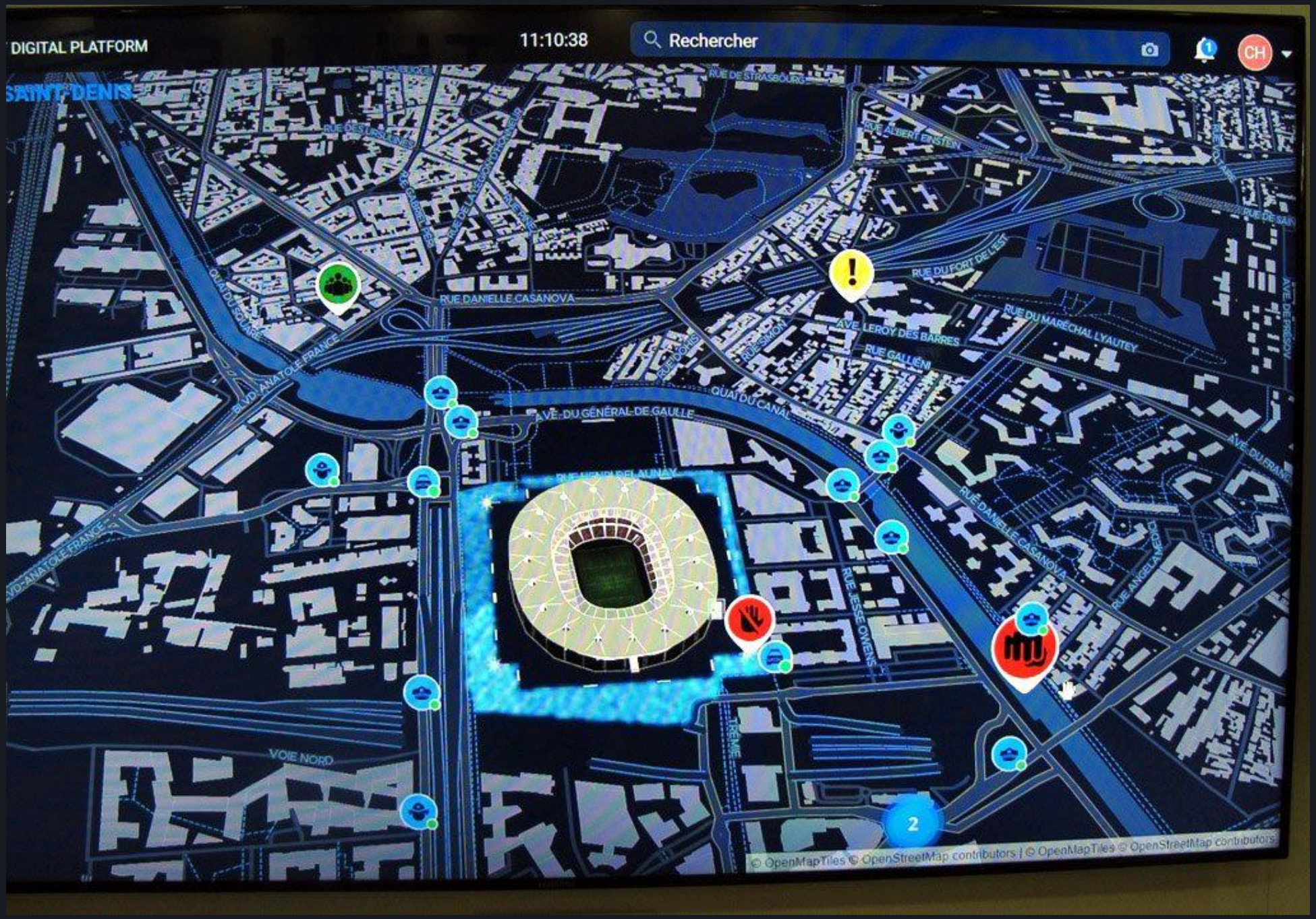
{C} 24/24, 7/7 operations during the event duration

{C} Prevention, Detection, Response and Recovery against cybersecurity threats

{C} Operators optimal User Experience (UX) to be ensured

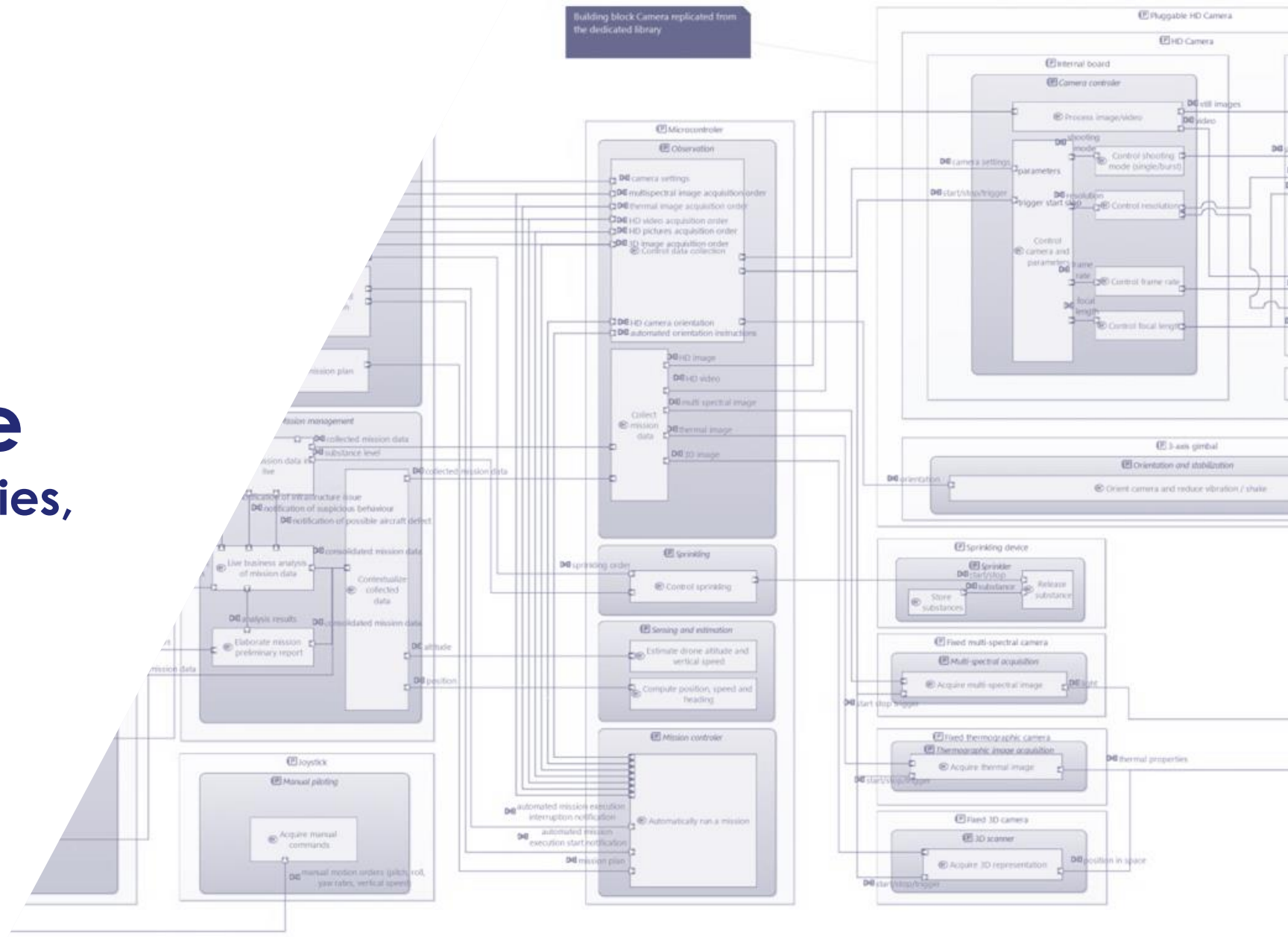

THALES SECURITY DIGITAL PLATFORM
GLOBAL SITUATION
CAM_00001
Stade de France - Gate A
09:12:146
09:20:123
CAM-12345
EMOTIONAL ANALYSIS
Joie
Surprise
Neutre
Triste
Haine
Colère
INTERVENTION TIME
10'58''
INCIDENT PIE
4 NEW
14 CLOSE
6 SOLVED
NUMBER OF INDIVIDUALS
81 000
81 338
max. capacity
BEFORE
17''
8'32''
BLACKLIST
13'15''
VIOLENCE
10'27''
INTRUSION
The suspect is armed and blacklisted, so be careful.
HUMAN RESOURCE
Mission
Profile
CHRONOS 1223
Gate A
01 23 45 67 89
deployed
chr-1223
850
similarit
28/11/19 - 09:10 (1 min ag
Wanted people
Stade de France
- Gate A
Critical
id-12345
09:20:123
TRACKING
18:30
19:30
01
03
10
new
27
solving
08
solved
DENSITY
HOURS
5:00
16:00
17:00
18:00


Gate A
Gate B
Gate C
Gate D
Gate E
Gate F
Gate G
50%
00:01:36
PHONE TIME WAITING
-46%
LAST HOUR
SOCIAL NETWORK
Stade de France
Hooligan
Mbappé
Paris
hoodlum
Abnormal
Monaco
Thug
Behaviour
Target name
09:00:12
00012
96%
Autoroute du Nord
MAP
GATE K cam_0031
LIVE
18/09/21 - 18:35:57
protected
65 264
Stade de France
Paris - Monaco
AFNOR
TARGET NAME #1
TARGET NAME #2
Name
Manuel
Family Name
LUCIANO
ID
125 8920 020
List
Hooligan
Track
Notify me
Description
KEEP A CLOSE WATCH ON THIS PERSON: very dangerous & unpredictable.
Instruction
To arrest if he create a threat for people around
Files
audio-testimony.mp
Title 1
keyword #1
LAST PASSING
ID
Date
Timestamp
Replay
Related partner
POLICE

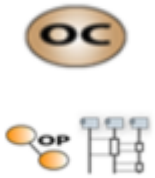
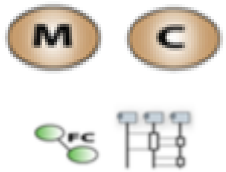
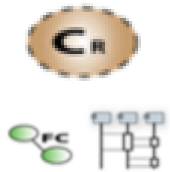
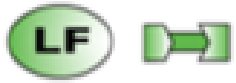
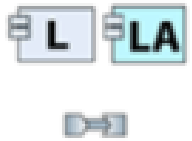
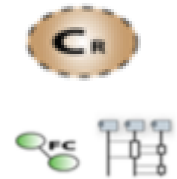
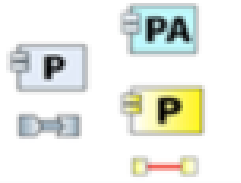

DIGITAL PLATFORM
11:10:38
Rechercher
CH
SAINT-DENIS
RUE DE STRASBOURG
RUE ALBERT EINSTEIN
RUE DANIELLE CASANOVA
RUE DU FORT DE L'EST
AVE. LEROY DES BARRES
RUE DU MARECHAL LYAUTEY
RUE GALLIÉNI
QUAI DU CANAL
AVE. DU GÉNÉRAL DE GAULLE
BLVD. ANATOLE FRANCE
RUE JESSE OWENS
RUE ANGELA DAVIS
VOIE NORD
2
© OpenMapTiles © OpenStreetMap contributors | © OpenMapTiles © OpenStreetMap contributors

# Architecture

## Views, SoS Boundaries, Functional Chains



# ARCADIA Grid – our safety belt when designing complex solutions

| | | ASPECTS | | | | |
|---|---|---|---|---|---|---|
| | | **Purpose** | **Behavior: Function** | **Behavior: Modes & States** | **Structure** | **Interfaces** |
| NEED PERSPECTIVES | **Operational Analysis**<br>What the stakeholders need to accomplish |  |  |  |  |  |
| | **System Needs Analysis**<br>What the system has to accomplish for the stakeholders |  |  |  |  |  |
| SOLUTION PERSPECTIVES | **Conceptual Architecture**<br>How the system will work to fulfill expectations |  |  |  |  |  |
| | **Finalized Architecture**<br>How the system will be developed and built |  |  |  |  |  |

# NAFv4 Grid

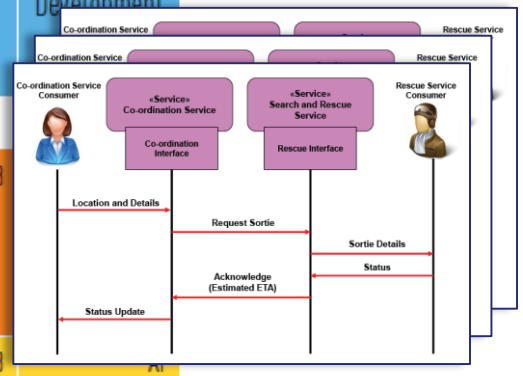
Aspect

Perspective

Viewpoint

View(s)

| | Taxonomy | Structure | | Behaviour: Connectivity | Behaviour: Processes | Behaviour: States | Behaviour: Sequences | Information | Constraints | Roadmap |
|---|---|---|---|---|---|---|---|---|---|---|
| Concepts | C1 Capability Taxonomy NAV-2, NCV-2 | C2 Enterprise Vision NCV-1 | | C3 Capability Dependencies NCV-4 | C4 Standard Processes NCV-6 | C5 Effects | | C7 Performance Parameters NCV-1 | C8 Planning Assumptions | Cr Capability Roadmap NCV-3 |
| | C1-S1 (NSOV-3) | | | | | | | | | |
| Service Specifications | S1 Service Taxonomy NAV-2, NSOV-1 | S2 Service Structure NSOV-2, 6, NSV-12 | | S3 Service Interfaces NSOV-2 | S4 Service Functions NSOV-3 | S5 Service States NSOV-4b | S6 Service Interactions NSOV-4c | S7 Service I/F Parameters NSOV-2 | S8 Service Policy NSOV-4a | Sr Service Roadmap |
| Logical Specifications | L1 Node Types NOV-2 | L2 Logical Scenario NOV-2 | L2-L3 (NOV-1) | L3 Node Interactions NOV-2, NOV-3 | L4 Logical Activities NOV-5 | L5 Logical States NOV-6b | L6 Logical Sequence NOV-6c | L7 Information Model NOV-7 | L8 Logical Constraints NOV-6a | Lr Lines of Development |
| | | | | | L4-P4 (NSV-5) | | | | | |
| Physical Resource Specifications | P1 Resource Types NAV-2, NCV-3, NSV-2a,7,9,12 | P2 Resource Structure NOV-4,NSV-1 | | P3 Resource Connectivity NSV-2, NSV-6 | P4 Resource Functions NSV-4 | P5 Resource States NSV-10b | P6 Resource Sequence NSV-10c | P7 Data Model NSV-11a,b | P8 Resource Constraints NSV-10a | |
| Architecture Foundation | A1 Meta-Data Definitions NAV-2 | A2 Architecture Products NAV-1 | | A3 Architecture Correspondence ISO42010 | A4 Methodology Used NAF Ch2 | A5 Architecture Status NAV-1 | A6 Architecture Versions NAV-1 | A7 Architecture Compliance NAV-3a | A8 Standards NTV-1/2 | Ar Architecture Roadmap |



# [PAB] Focus on mission execution

## PAB: Architecture view (in Physical Architecture perspective)

Structure

Behaviour

**NEED** PERSPECTIVES

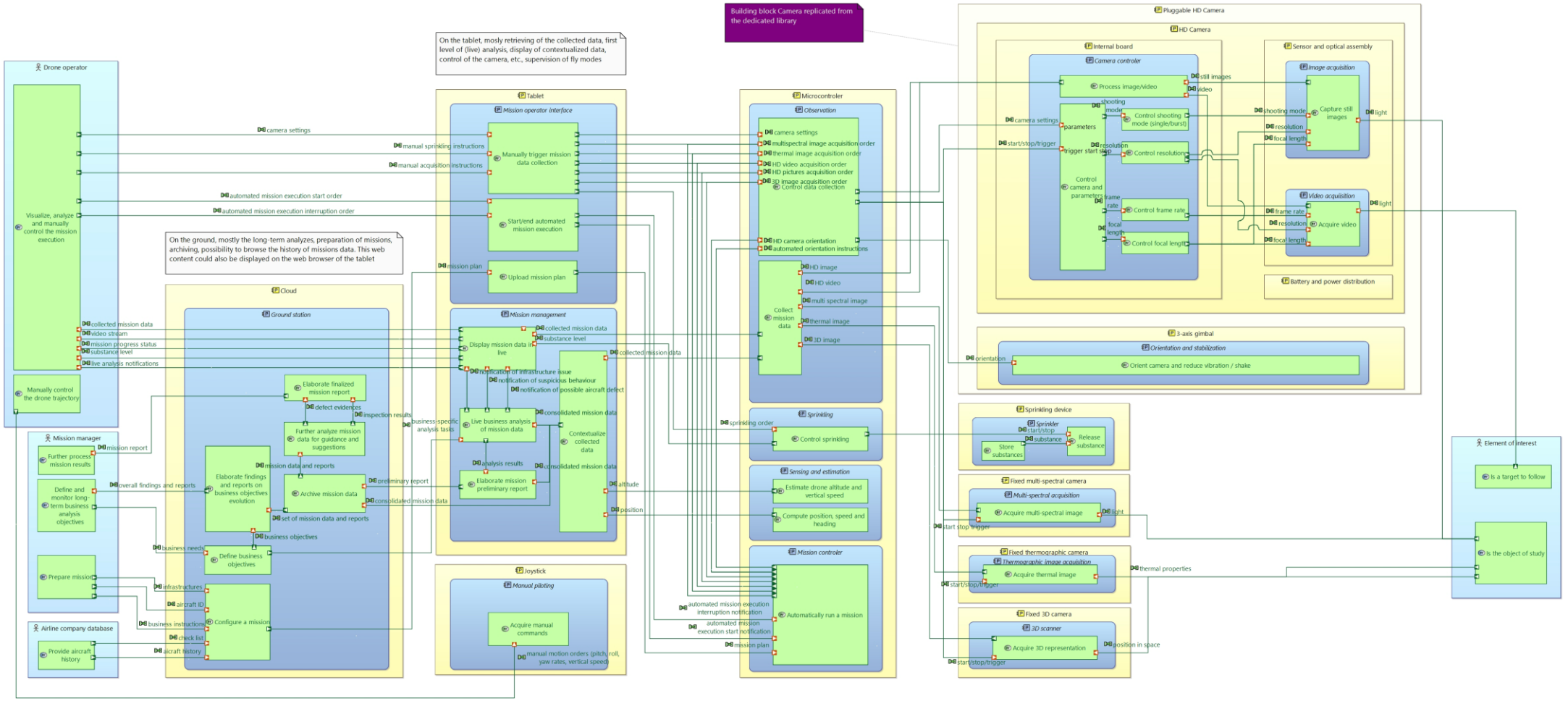
OA

SA

**SOLUTION** PERSPECTIVES

LA

**PA**

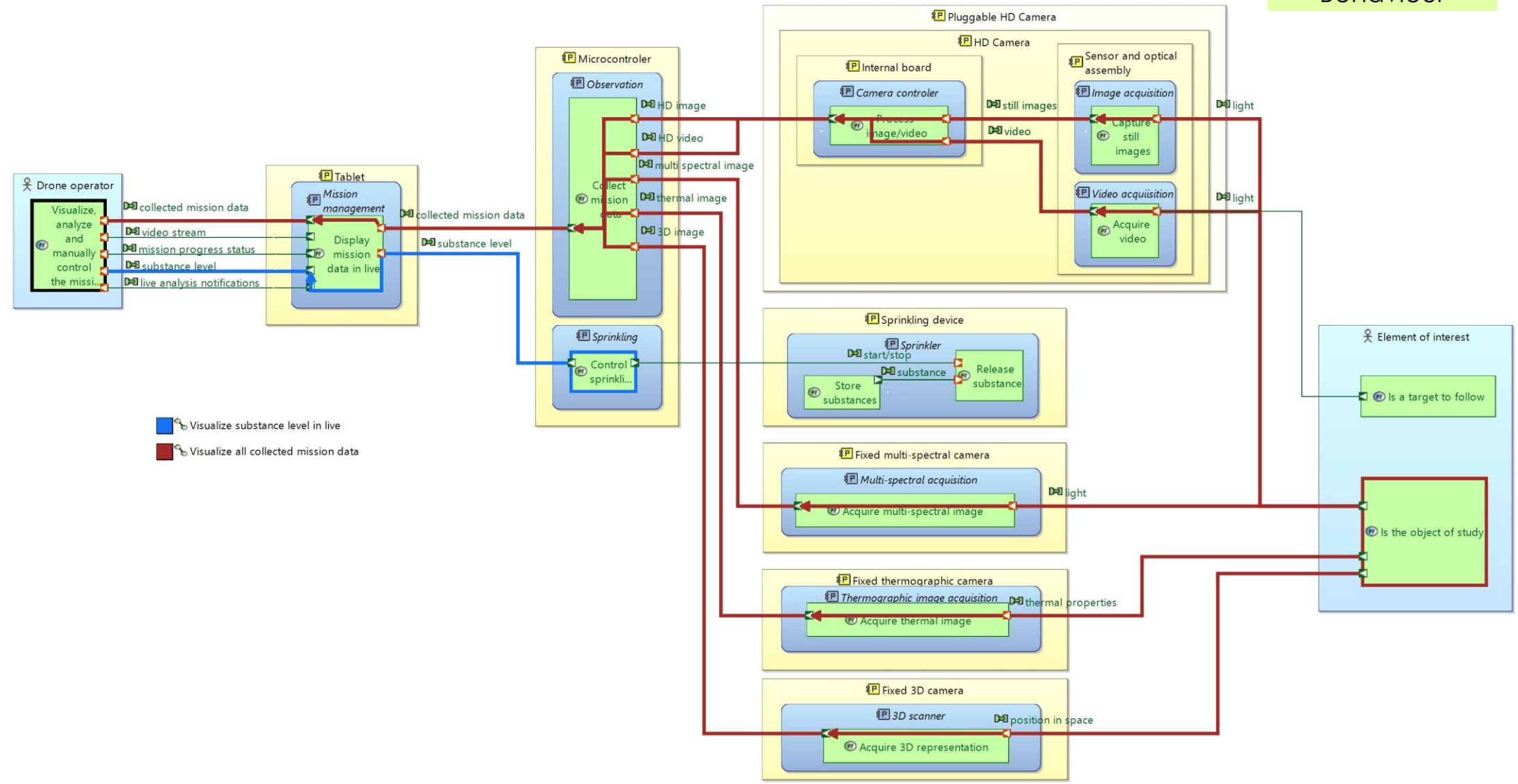


# [PAB] Visualize data in live during navigation

## PAB: Architecture view (in Physical Architecture perspective)

Purpose
Structure
Behaviour

NEED PERSPECTIVES
OA
SA
SOLUTION PERSPECTIVES
LA
PA



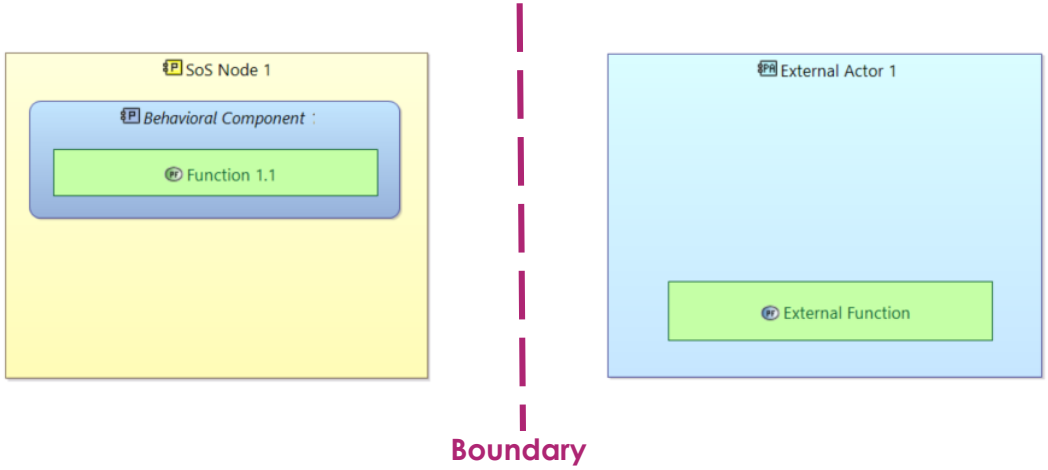



THALES
Building a future we can all trust

# System Boundaries in SoS

## > System

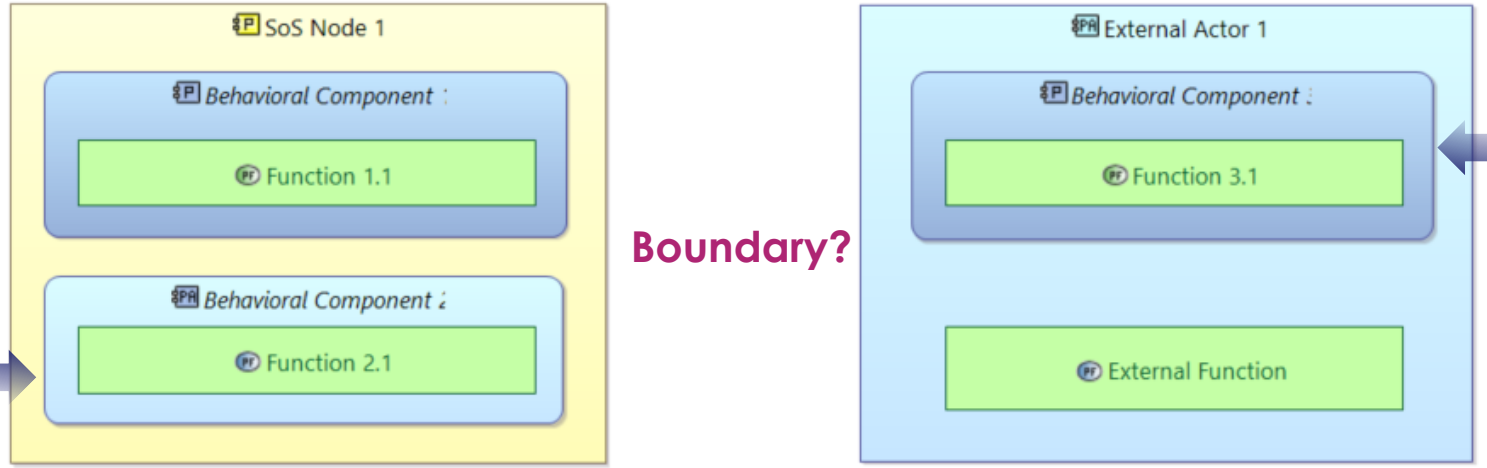
A BC and Function allocated to a physical node that is designed, built and delivered by the system provider




An entity external to the system under design that is in charge of a specified function

## > System of Systems

A Behavioral Component (e.g. a software application) that is developed and delivered by an entity external to the system, and that is deployed in the SoS (e.g. SoS = cloud platform)

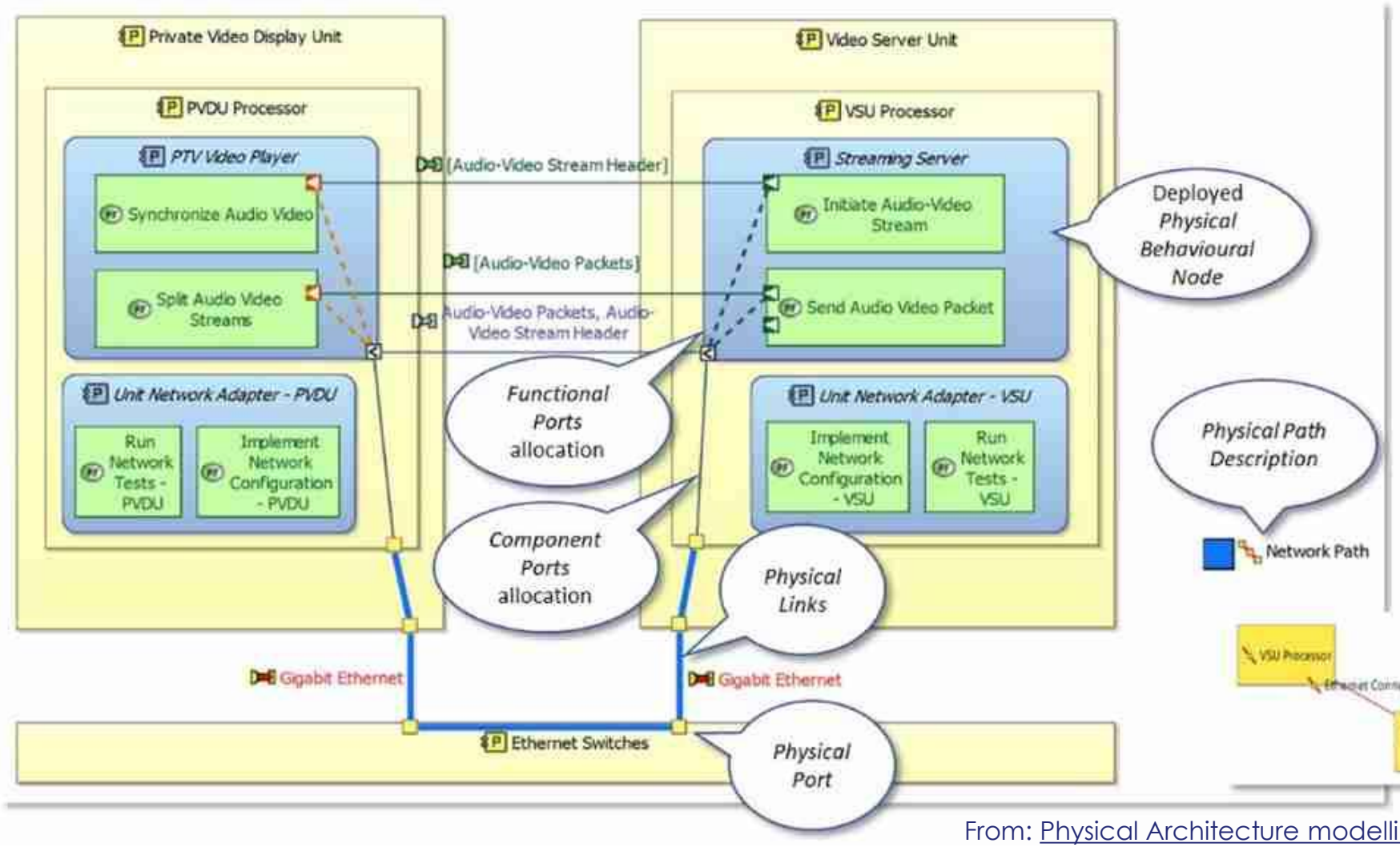



A Behavioral Component that is developed and delivered by the SoS provider, and that is deployed elsewhere



REF xxxxxxxxxxxx rev xxx – date Name of the company / Template: 87211168-DOC-GRP-EN-007

# Reminder: Physical Architecture Views (PAB)

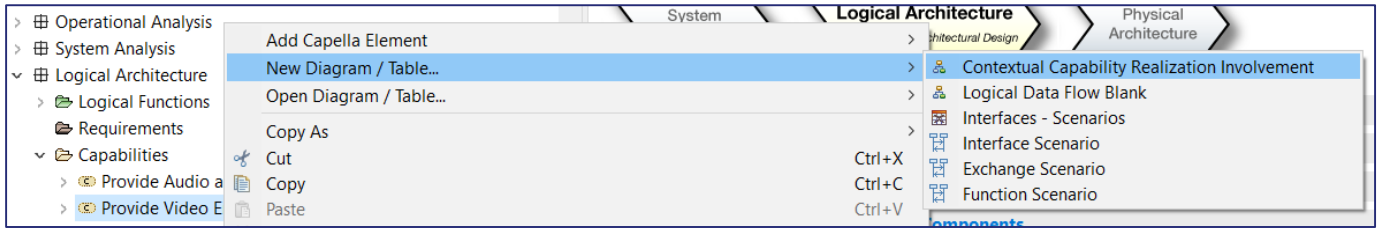



## Don't forget the deployment interfaces!

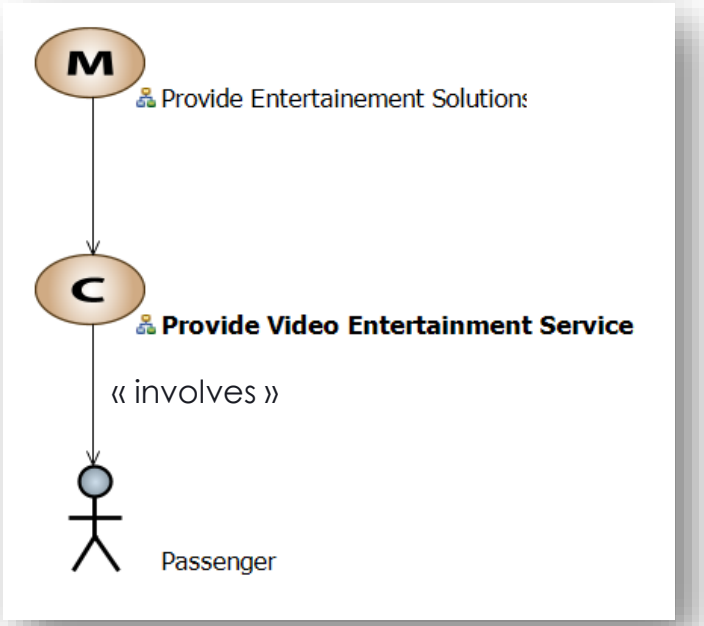
Examples: a pump « deployed » in a room (size, position, …); a software application « deployed » in an OS (version, APIs, …), …

From: Physical Architecture modelling steps and concepts - Home (iexcelarc.com)

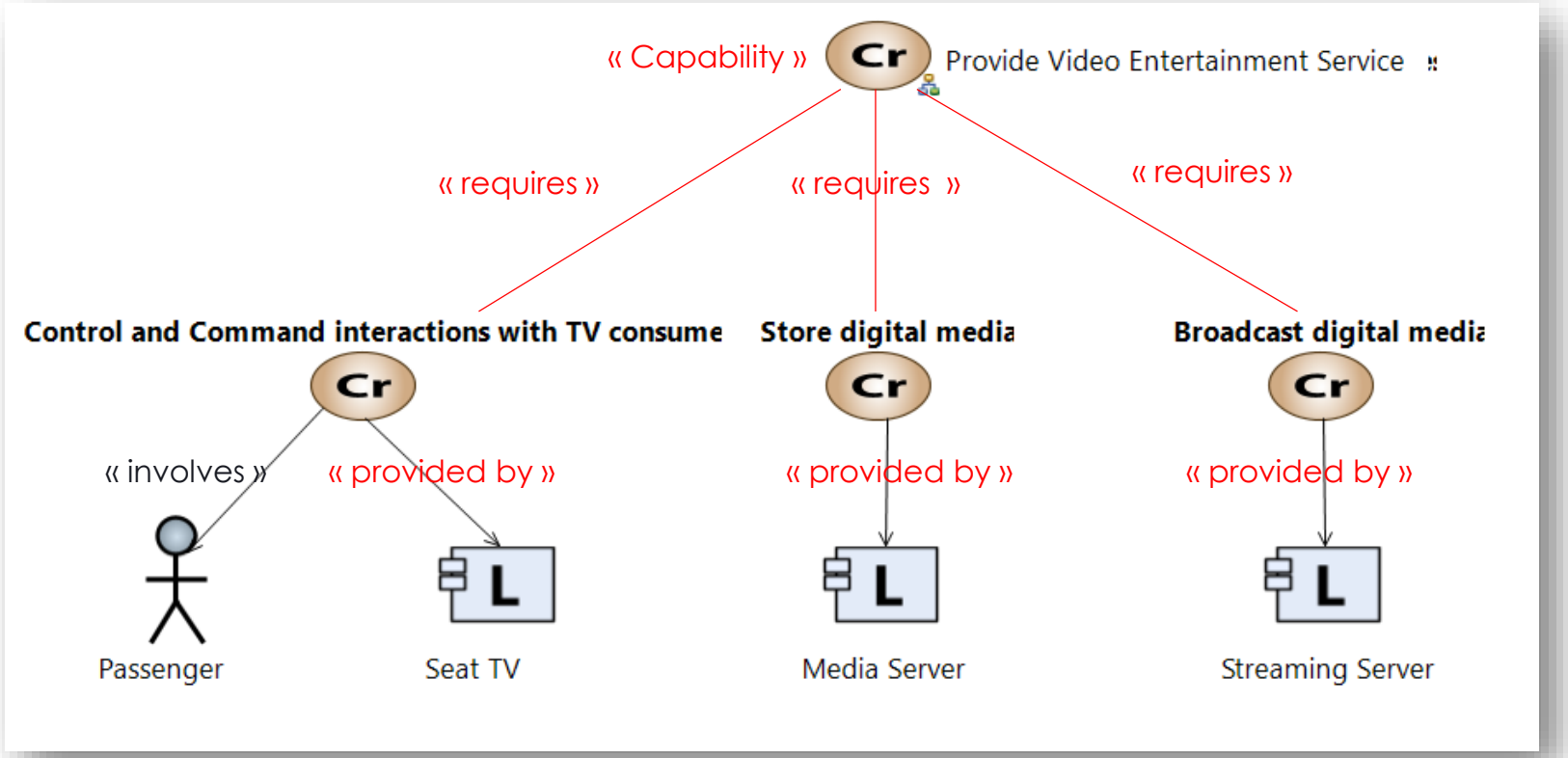
# Capability Realizations




## > In Systems Analysis:

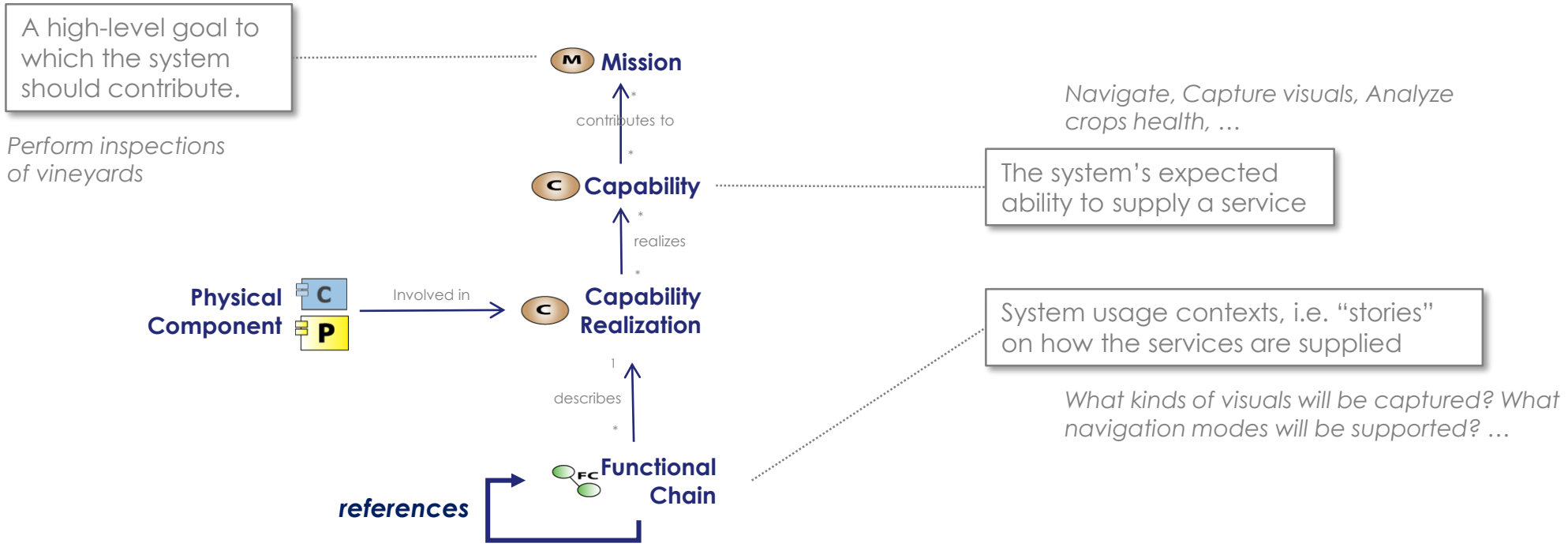



## > In Logical Architecture and Physical Architecture (CRI views):




Red relations are added to adapt Arcadia to SoS architecting

# Orchestration of Functional Chains to specify Mission Threads




**Webinar on orchestration of Functional Chains:**
**https://youtu.be/ZqvfSURUpIY?si=gVs1FSZObqyz2GnU&t=795**

# (Emerging) System lifecycle properties

# « -ilities »

> **System properties that specify the degree to which systems are able to maintain or even improve function in the presence of change**

- Often manifest after the system has been put to initial use
- Not the primary purpose of the system
- But typically concern wider system impacts with respect to time and stakeholders

| Ility Name | Definition ("ability of a system…") |
|---|---|
| adaptability | to be changed by a system-internal change agent with intent |
| agility | to change in a timely fashion |
| changeability | to alter its operations or form, and consequently possibly its function, at an acceptable level of resources |
| evolvability | design to be inherited and changed across generations (over time) |
| extensibility | to accommodate new features after design |
| flexibility | to be changed by a system-external change agent with intent |
| interoperability | to effectively interact with other systems |
| modifiability | to change the current set of specified system parameters |
| modularity | degree to which a system is composed of modules (not an ability-type ility) |
| reconfigurability | to change its component arrangement and links reversibly |
| robustness | to maintain its level and/or set of specified parameters in the context of changing system external and internal forces |
| scalability | to change the current level of a specified system parameter |
| survivability | to minimize the impact of a finite duration disturbance on value delivery |
| value robustness | to maintain value delivery in spite of changes in needs or context |
| versatility | to satisfy diverse needs for the system without having to change form (measure of latent value) |

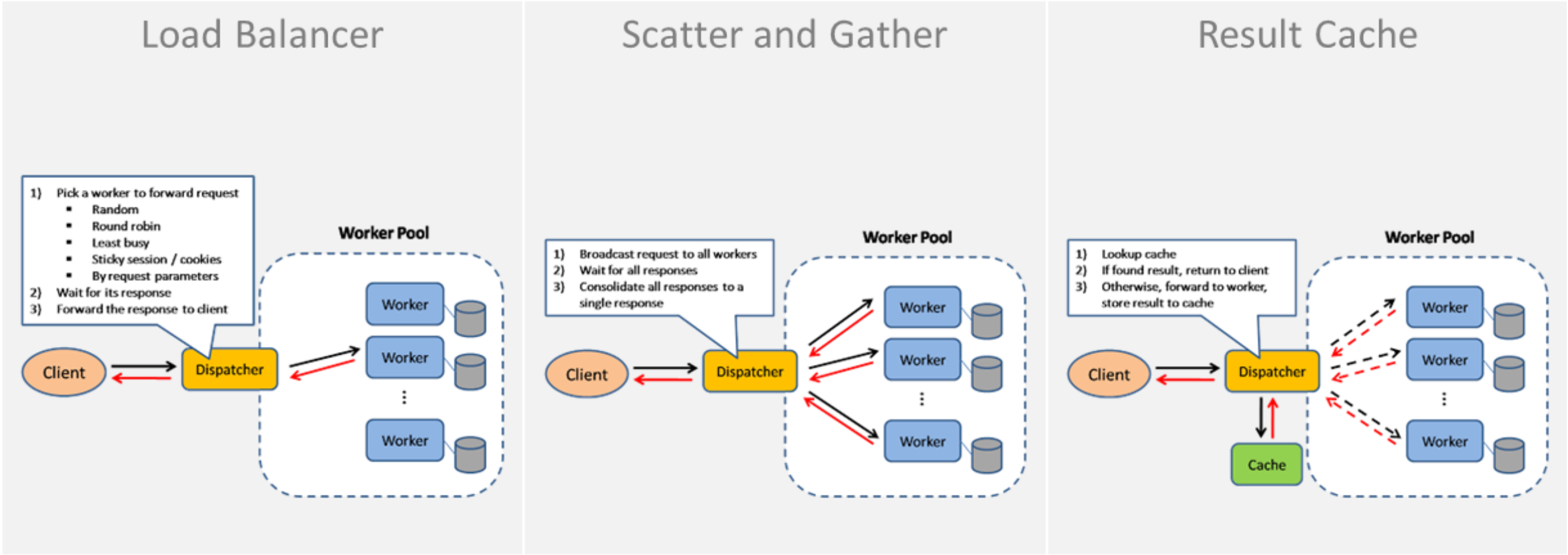
# More system lifecycle properties

- Accessibility
- Accountability
- Adaptability
- Administrability
- Affordability
- Agility
- Availability
- Capability
- Composability
- Configurability
- Compatibility
- Demonstrability
- Deployability
- Durability
- Executability
- Extensibility
- Evolvability
- Fidelity
- Flexibility
- Functionality
- Integratability
- Interoperability
- Interpretability
- Maintainability
- Manageability
- Mobility
- Modifiability
- Operability
- Performability
- Portability
- Practibilty
- Practicality
- Predictability
- Producibility
- Recoverability
- Reliability
- Repeatability
- Responsibility
- Reusability
- Scalability
- Serviceability
- Stability
- Supportability
- Suitability
- Survivability
- Tailorability
- Testability
- Traceability
- Trainability
- Transportability
- Trustability
- Understandability
- Upgradability
- Usability
- Verifiability
- Vulnerability
- …

**+ all those that don't finish by « ility »: human factors, resilience, cybersecurity, cost, weight, …**

# Ex: software scalability patterns (Ricky Ho)

Scalability is about **reducing the adverse impact due to growth** on performance, cost, maintainability and many other aspects

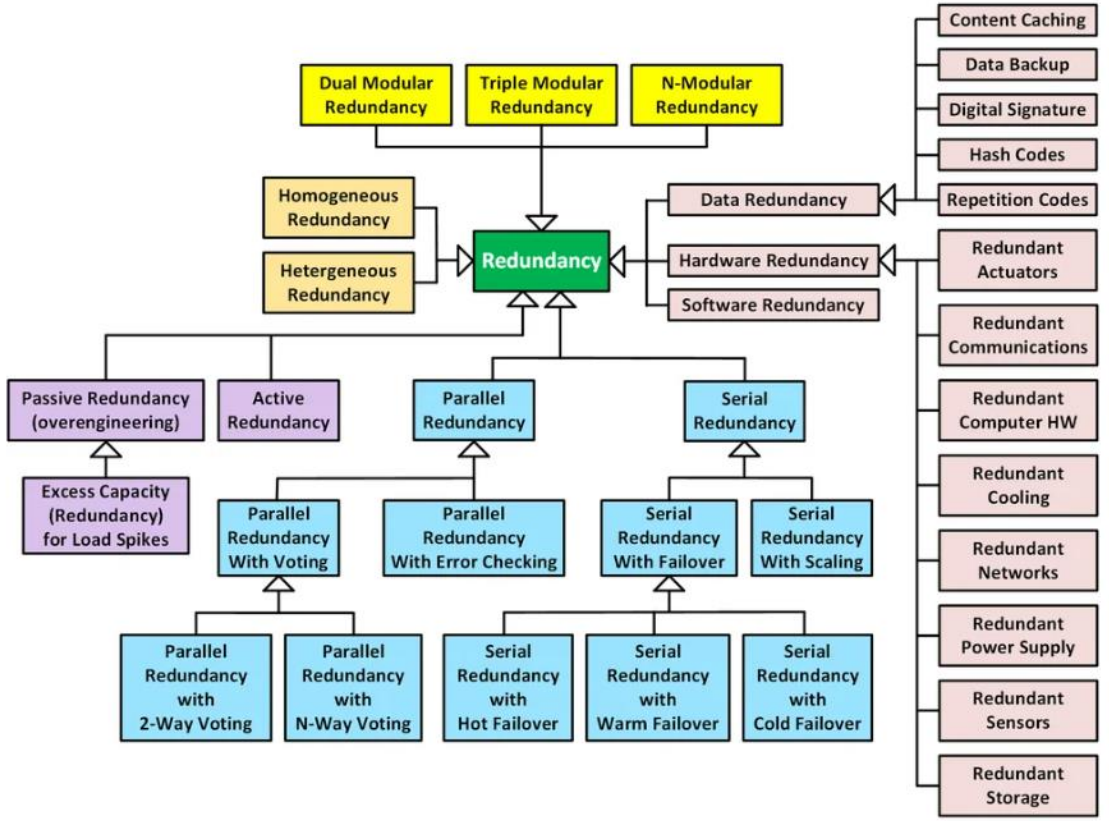


# Ex: System Resilience

Source; Software Engineering Institute, "System Resilience", DONALD FIRESMITH. System Resilience: What Exactly is it? (cmu.edu)

A system is resilient to the degree to which it rapidly and effectively **protects its critical capabilities from disruption** caused by adverse events and conditions.

| Quality Attribute | Example Adversities | |
|---|---|---|
| | Adverse Events | Adverse Conditions |
| Robustness | Input Errors Failures | Adverse Environments and Faults (HW/SW/Data Defects) |
| Safety | Accidents | Hazards and Vulnerabilities |
| Cybersecurity | Cyber Attacks | Cyber Threats and Vulnerabilities |
| Anti-Tamper | Attempted Tampering | AT Threats and Vulnerabilities |
| Survivability | Kinetic Attacks | Military Threats and Vulnerabilities |
| Capacity | Load Spikes Load-Related Failures | Excessive Loads |
| Longevity | Age-Related Failures | Excessive Age and Age-Related Defects |
| Interoperability | Lost Communications | Degraded Communications |





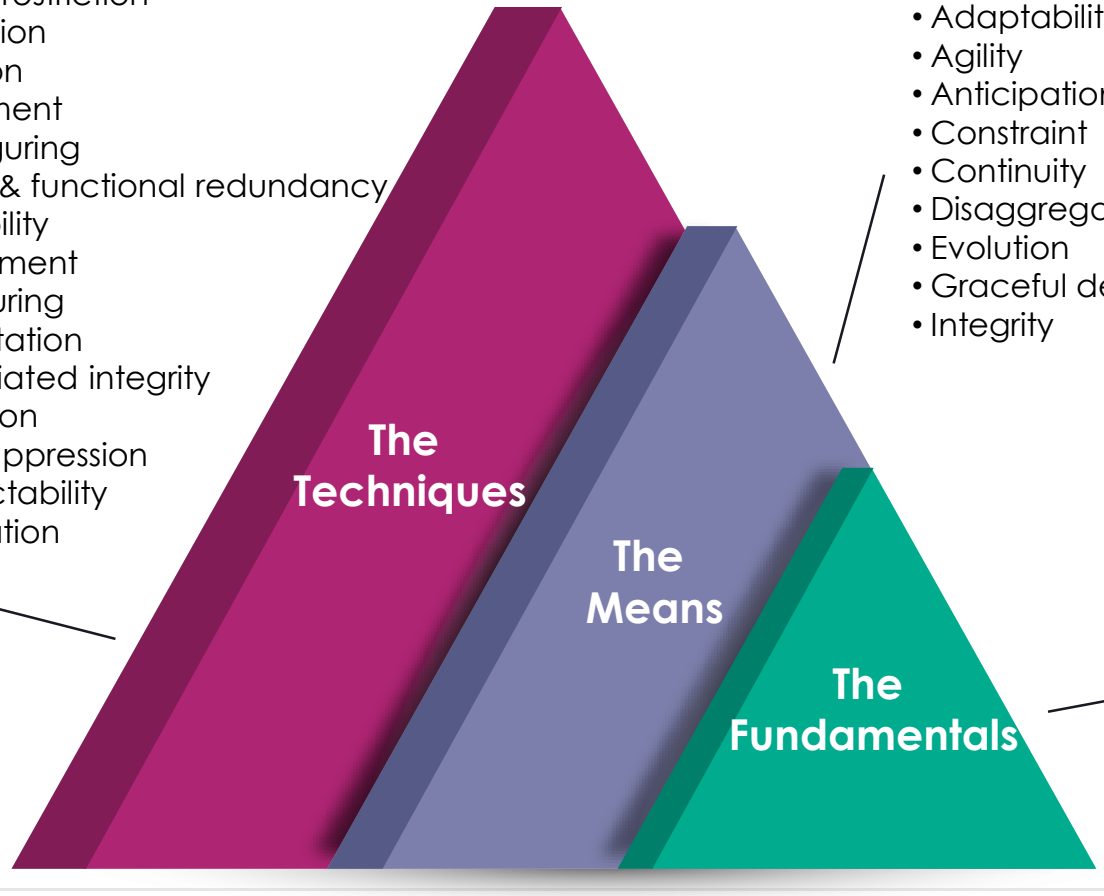

REF xxxxxxxxxxxx rev xxx – date Name of the company / Template: 87211168-DOC-GRP-EN-007

# Ex: System Resilience

Source; SEBoK, "System Resilience", Brtis, Jackson, Cureton
https://www.sebokwiki.org/wiki/System_Resilience

- Absorption
- Adaptive response
- Analytic monitoring & modelling
- Boundary enforcement
- Buffering
- Coordinated defence
- Complexity avoidance
- Deception
- Defence in depth
- Distribution
- Detection avoidance
- Diversification
- Drift correction
- Dynamic positioning
- Dynamic representation
- Effect tolerance
- Human participation
- Internode interaction & interfaces
- Least privilege

- Loose coupling
- Modularity
- Neutral state or safe state
- Non-persistence
- Privilege restriction
- Proliferation
- Protection
- Realignment
- Reconfiguring
- Physical & functional redundancy
- Reparability
- Replacement
- Restructuring
- Segmentation
- Substantiated integrity
- Substitution
- Threat suppression
- Unpredictability
- Virtualization



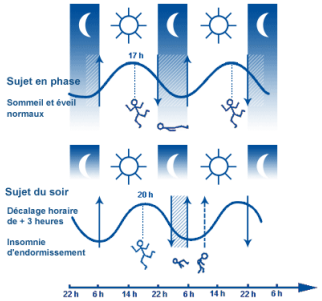

- Adaptability/flexibility
- Agility
- Anticipation
- Constraint
- Continuity
- Disaggregation
- Evolution
- Graceful degradation
- Integrity

- Preparation
- Prevention
- Re-architecting
- Redeployment
- Robustness
- Situational awareness
- Tolerance
- Transformation
- understanding

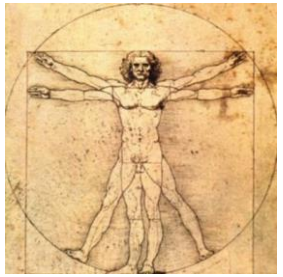
- Avoid adversity
- Withstand adversity
- Recover from adversity
- Evolve & adapt

# Ex: Human Factors

**Favor Human centered approach**




**Anticipate Variability**



**Respect Humans limits**


**Expect Shortcuts**

**Expect Creativity**

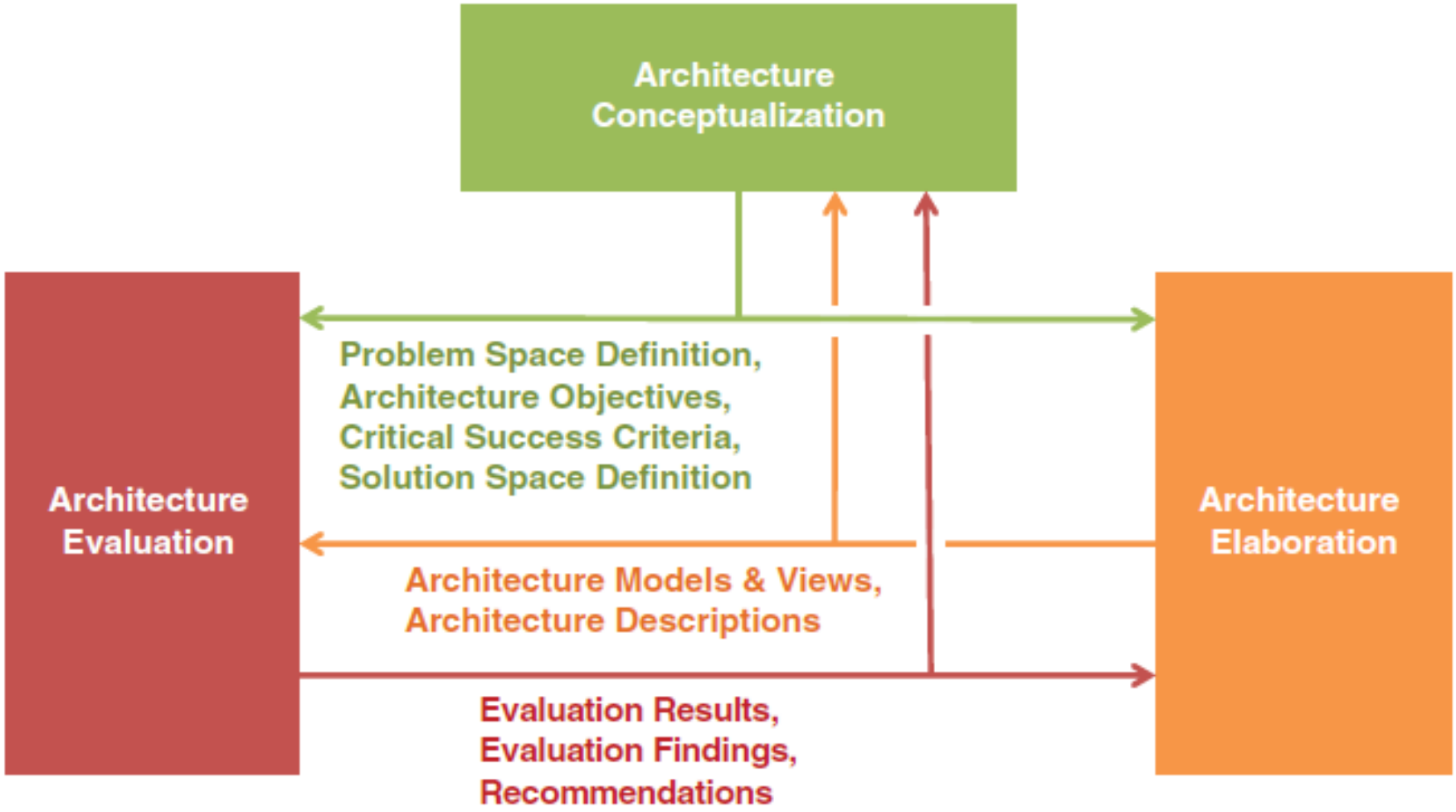

**Emotions will interfere**

# Architecture evaluation




REF xxxxxxxxxxxx rev xxx – date Name of the company / Template: 87211168-DOC-GRP-EN-007

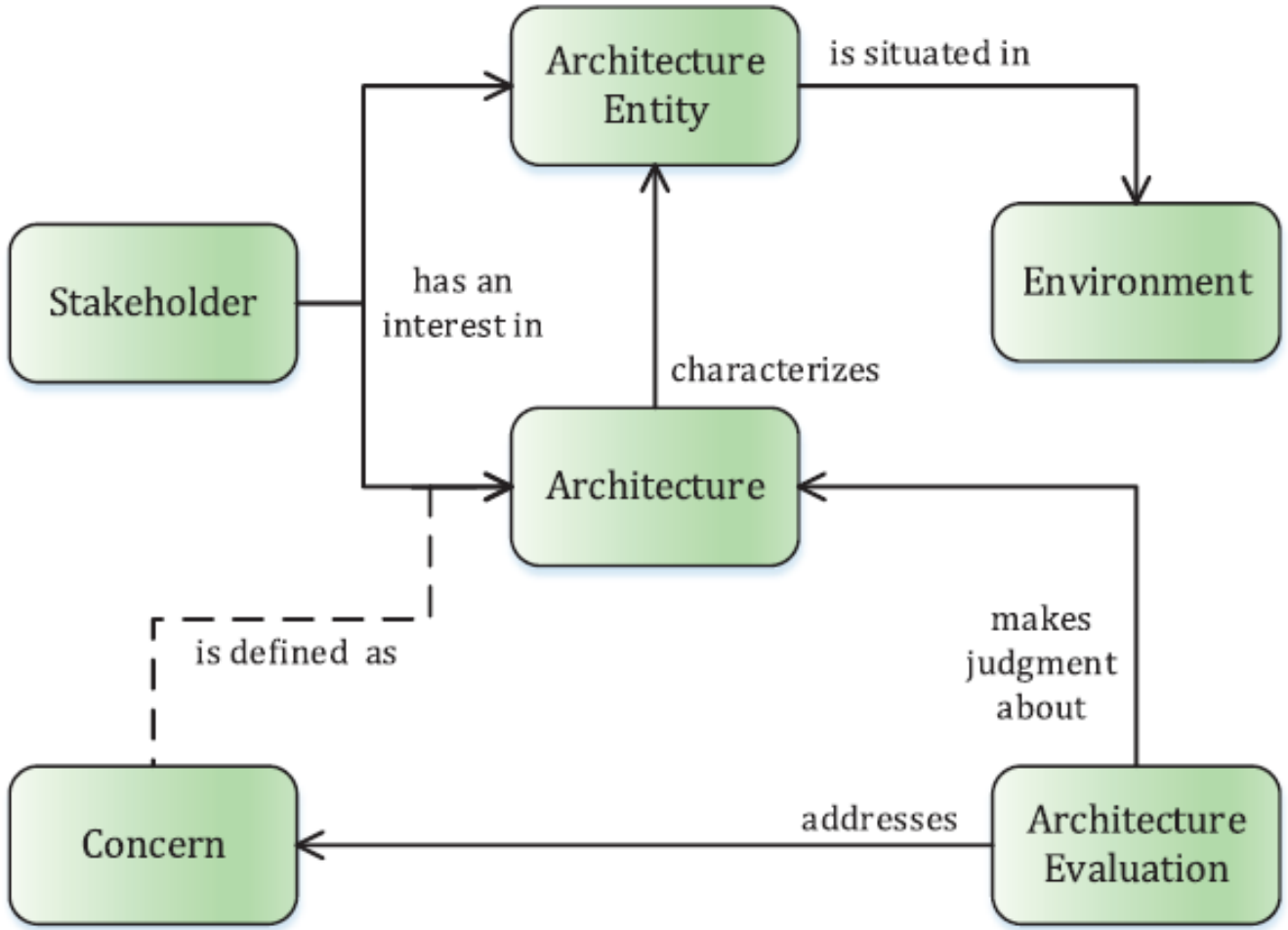
# Architecture Evaluation in the Architecting process



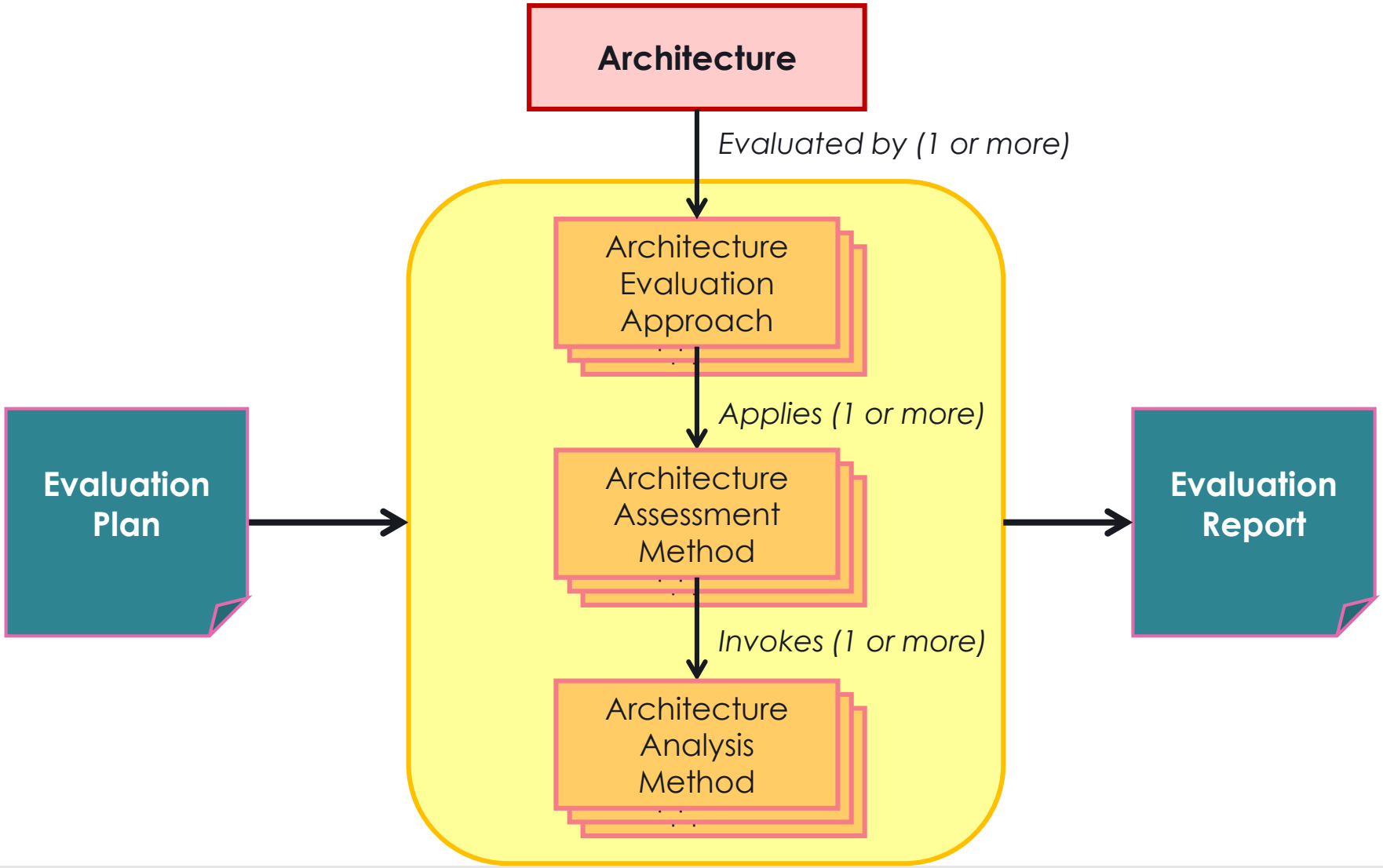
# ISO/IEC/IEEE 42030 – Architecture Evaluation

## > Stakeholders concerns drive Architecture Evaluation

- Concerns are about the system itself, and not about the architecture, neither about the quality of the architecting process



# ISO/IEC/IEEE 42030 – Architecture Evaluation Framework






REF xxxxxxxxxxxx rev xxx – date Name of the company / Template: 87211168-DOC-GRP-EN-007

# ISO/IEC/IEEE 42030 – Architecture Evaluation Framework

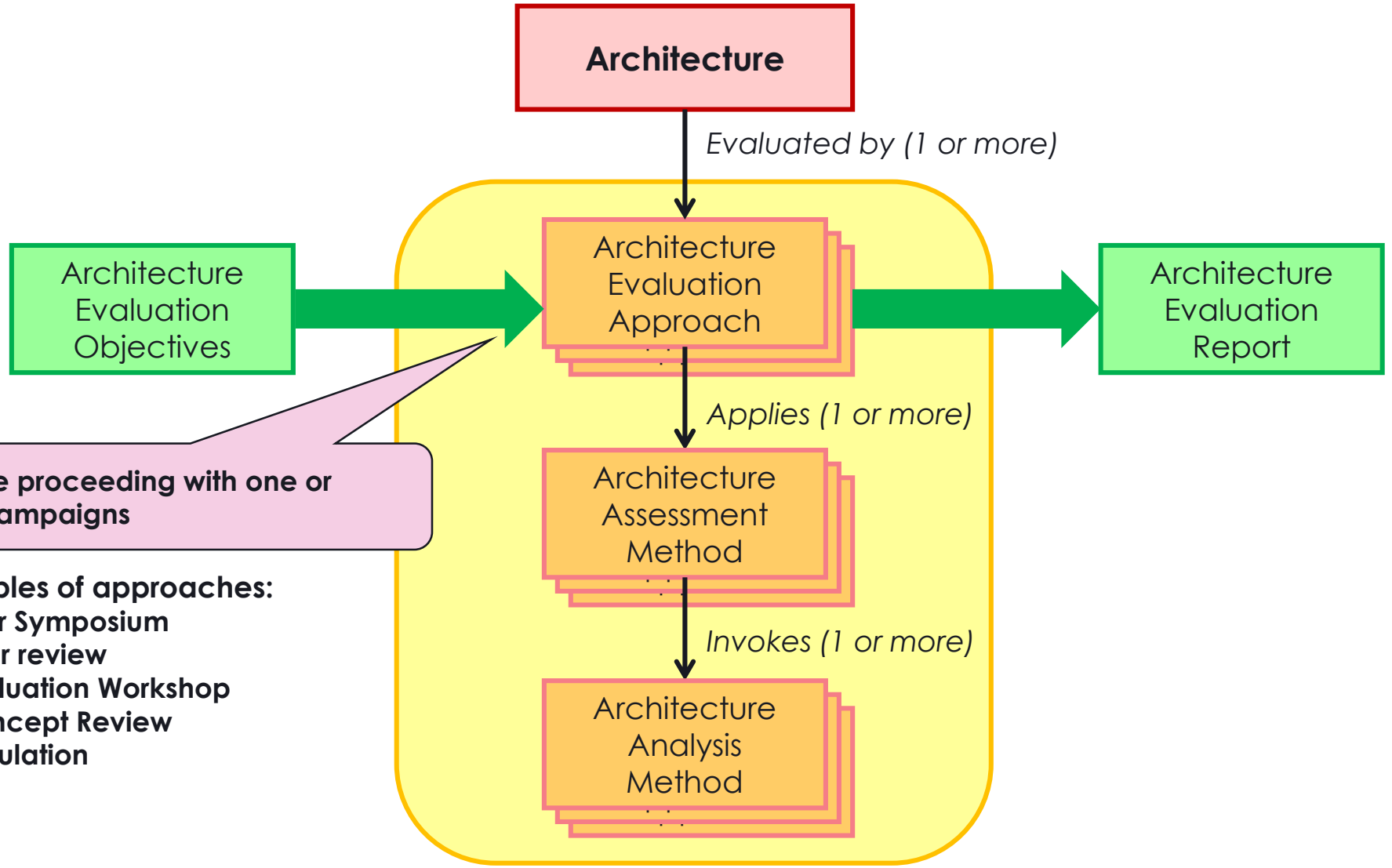
## > Evaluation Plan

- Purpose & scope
- Evaluation objectives, constraints, criteria, priorities
- Schedule & required resources
- Evaluation framework(s) to be used
- Evaluation approach(es) & method(s) to be used
- Roles & responsibilities of evaluators
- Required inputs & reference materials
- Expected outputs & deliverables

## > Evaluation Report

- Purpose, scope & objectives
- Participants in the effort (either directly or indirectly)
- Inputs used
- Frameworks used
- Approaches & methods used
- Method results & rationale
- Observations & findings
- Risks & opportunities identified
- Recommendations & regrets

# ISO/IEC/IEEE 42030 – Architecture Evaluation Framework



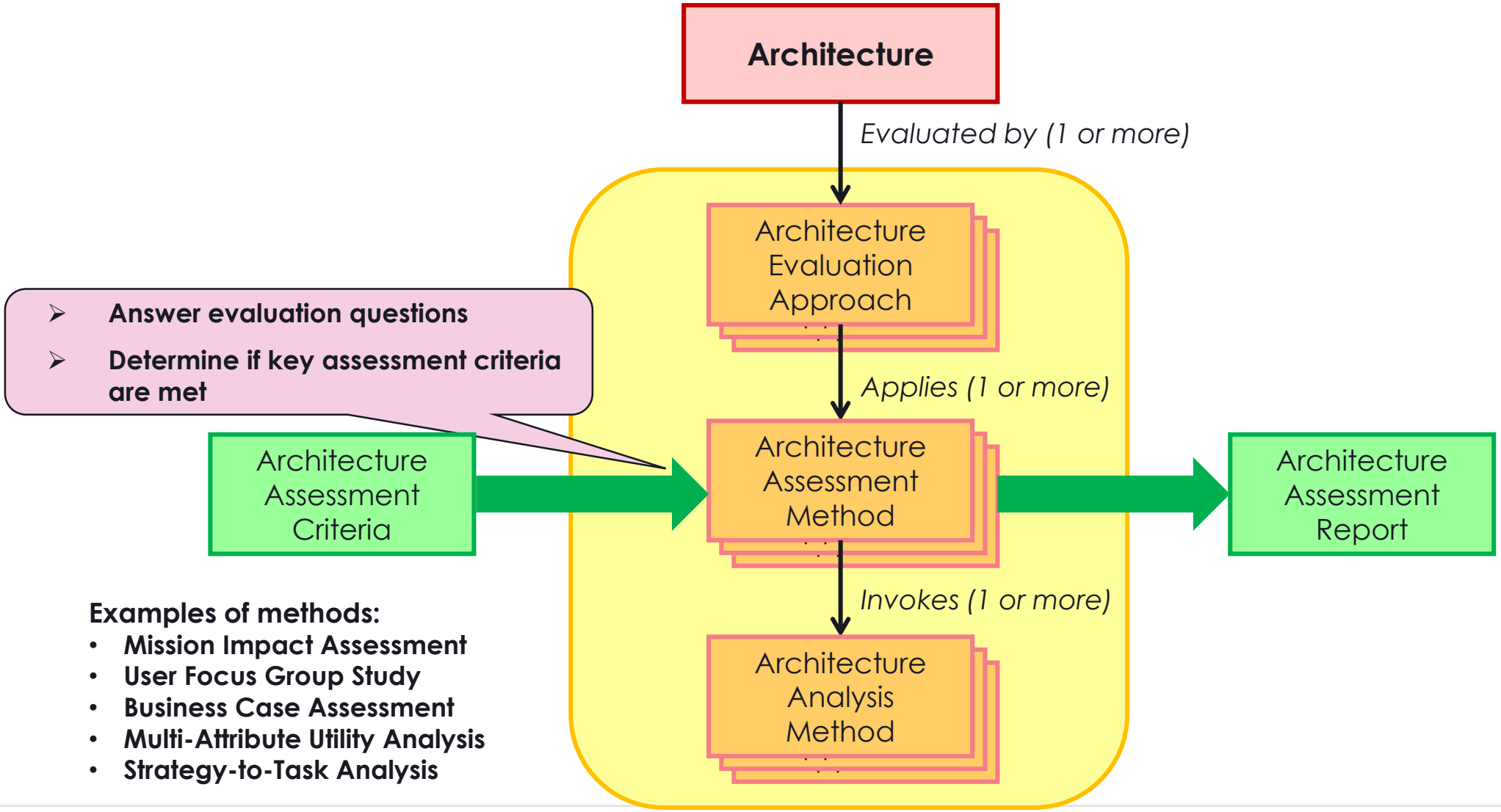

**Examples of approaches:**

- **User Symposium**
- **Peer review**
- **Evaluation Workshop**
- **Concept Review**
- **Simulation**



REF xxxxxxxxxxxx rev xxx – date Name of the company / Template: 87211168-DOC-GRP-EN-007

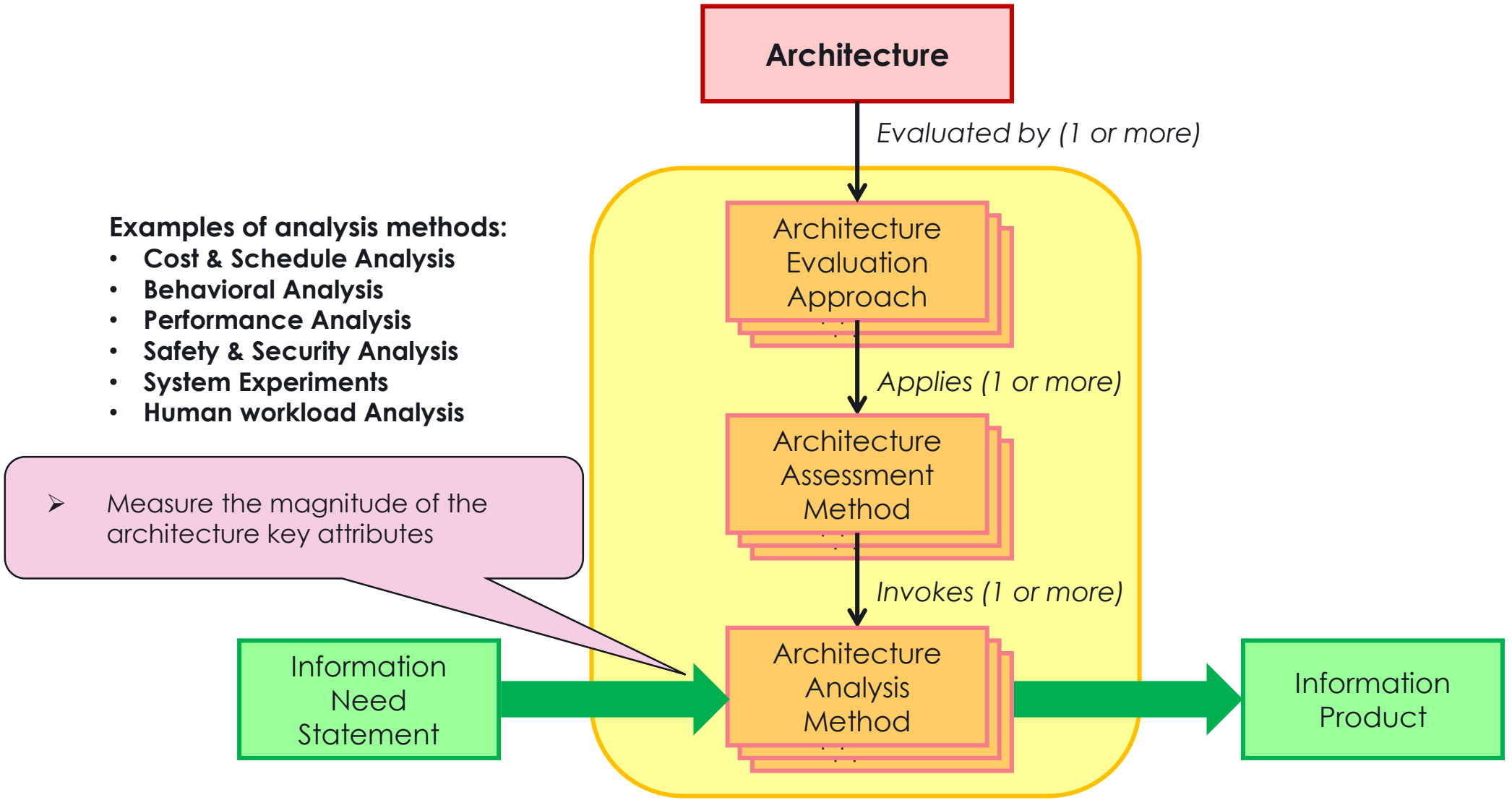
# ISO/IEC/IEEE 42030 – Architecture Evaluation Framework



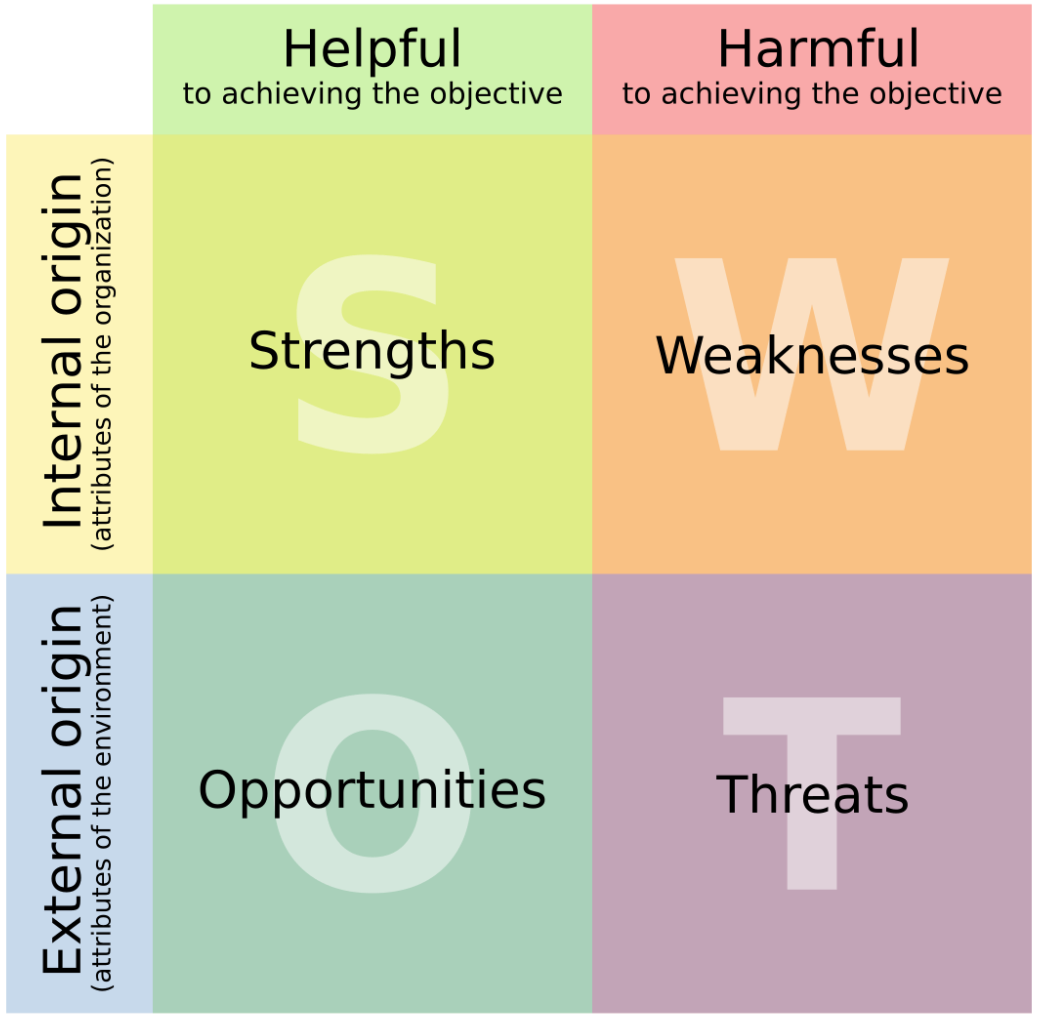

**Examples of methods:**

- **Mission Impact Assessment**
- **User Focus Group Study**
- **Business Case Assessment**
- **Multi-Attribute Utility Analysis**
- **Strategy-to-Task Analysis**

# ISO/IEC/IEEE 42030 – Architecture Evaluation Framework



# SWOT: a simple analysis method



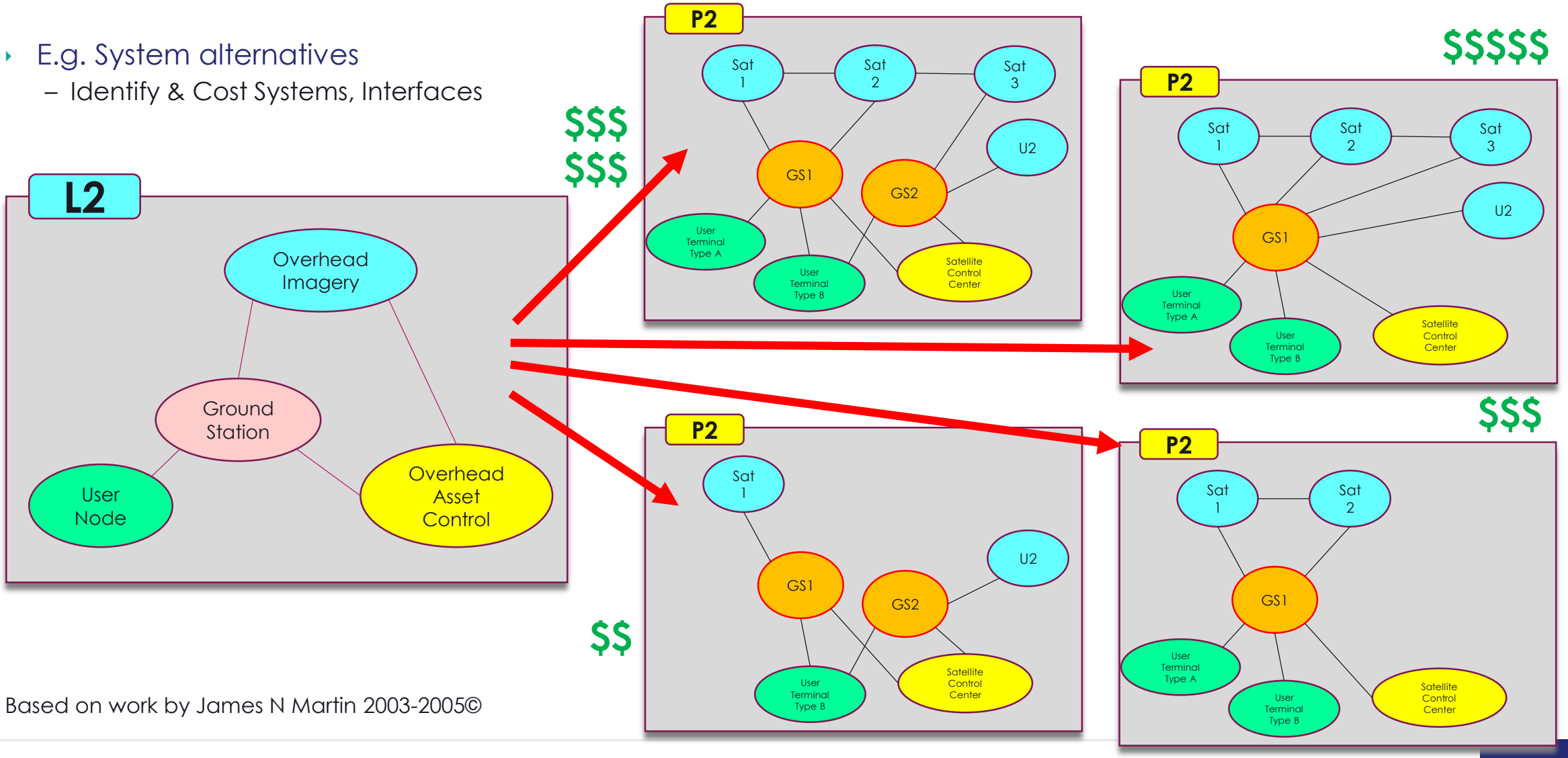

## > Example:

- Strenghts
  - **Modularity**: The architecture is designed to be modular, enabling the easy addition of new features without affecting the entire system
- Weakness
  - **Management Complexity**: While modularity is beneficial, it has led to high complexity in the daily management and operation of the system.
- Opportunities
  - **Emerging Technologies**: The integration of emerging technologies like artificial intelligence to enhance product recommendations and data analysis.
- Threats
  - **Increasing Cyber Threats**: Rising risk of cyberattacks targeting customer data, necessitating constant updates to security measures.

# Architecture Tradeoffs

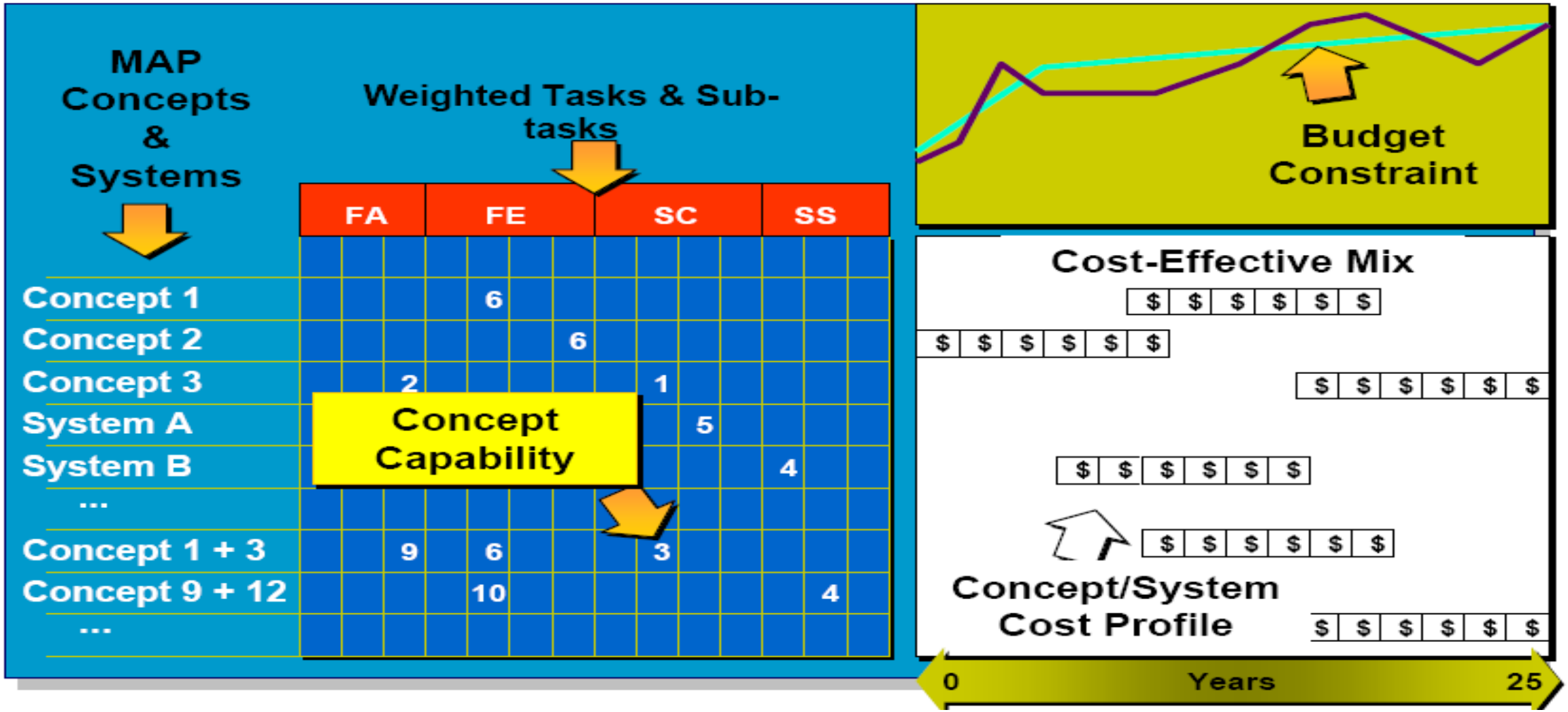
# Exploring Trade Space Using Views

- E.g. System alternatives
  - Identify & Cost Systems, Interfaces



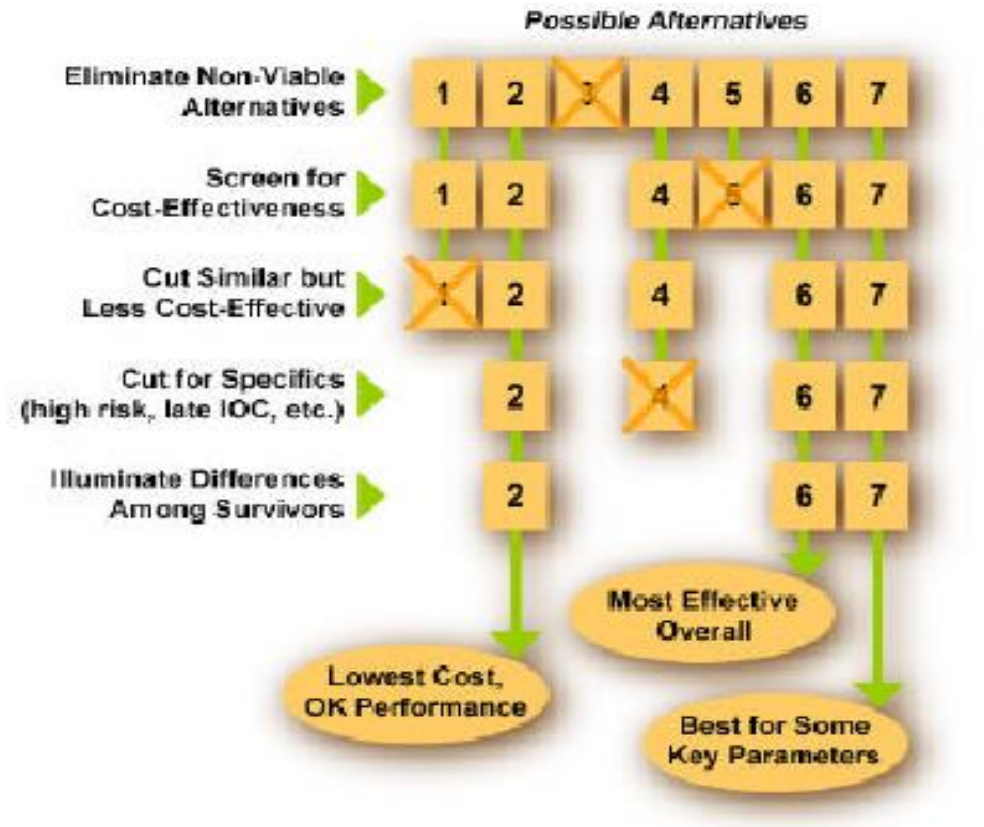

Based on work by James N Martin 2003-2005©

# Evaluate System Fit to Concept



# Early Elimination of Alternatives

- Selecting most cost-effective alternative
- Multiple drivers




Ref. US Aerospace Agency Architecture Methodology

## > Eliminate

- Non viable
- Expensive
- Similar, less cost effective
- Risky (delivery, security)
- ….

## > Highlight

- Lowest Cost,
- Most effective,
- Best for identified set of  key drivers

# Exercise 3

# Exercise 3.1 – SoS Architecture

## Based on the results of Exercise 2 and the following Mission Thread:

### Ensure law enforcement in the event zone at D-Day

- This Mission Thread is a subset of the one studied last time with a new scope: focusing on the day of the event

## 1. Consolidate the Mission Thread

- Extract the Mission Thread Steps and the Capabilities that are exploited to achieve this **new scope (« to-be » instead of « as-is »)** of the Mission Thread
  - Document this in a table, not in a diagram (cf. Day 2)
- Some guidance
  - Make sure you include a capability of detecting suspects from video stream (drones, CCTV, …)
  - Leverage on FRESUS capabilities presented above
  - Document this in the Document section of the System Analysis perspective

## 2. Develop Physical Architecture View

- In the same model, and focusing on the elements concerned by the Mission Thread (Step 1), produce a PAB view of the Physical Architecture
- Define Functional Chains
  - At least 3 per capability, show them in the PAB
  - Make sure you include Functional Chains for Detection capability

## 3. Define the Capability Realizations

- Identify the Capabilities of the Physical Components (CapabilityRealizations) that are needed to perform the FRESUS Capabilities included in the Mission Thread
  - Produce a Capability Realization Blank (CRB) view in the Physical Architecture Perspective



REF xxxxxxxxxxxx rev xxx – date Name of the company / Template: 87211168-DOC-GRP-EN-007

# Exercise 3.2 – Evaluation of Architectures

## 4. Perform a SWOT analysis of the following architecture alternatives:

**Drones or Drone swarms have suspects recognition capabilities**

**vs.**

**Suspects recognition is only done by humans and machines in the Police Mobile Command and Control Center**

- Consider the following criteria:
  - Cybersecurity
  - Communications (latency, bandwidth, …)
  - Resilience
  - Others (pick yours)

# Mission Thread: Example

**Mission Thread Template: Header**

| | |
|---|---|
| **Name** | Protect Fleet Assets Against Cruise Missile Attacks |
| **Vignette (Summary Description)** | Two ships (Alpha and Beta) are assigned to air defense (AD) to protect a fleet containing two high-value assets (HVA). A surveillance aircraft (SA) and 4 UAVs (2 pairs) are assigned to the fleet and controlled by the ships (Alpha and Beta). A pair of UAVs flying as a constellation can provide fire-control quality (FCQ) tracks directly to the two ships. A two-pronged attack on the fleet occurs:<br>• 5 aircraft launch missiles from the southeast<br>• 3 minutes later, 7 submarines launch missiles from the southwest<br><br>The fleet is protected with no battle damage. |
| **Nodes and Actors** | Two ships (Alpha and Beta), 4 UAVs, 2 HVAs, 1 SA, 5 enemy aircraft and their missiles, and 7 enemy submarines and their missiles |
| **Assumptions** | Enemy aircraft are flying along a route normally used for training, and suddenly change direction and head for the fleet. They are being tracked.<br>The submarines are undetectable until they fire their missiles.<br>• *No sonobouys are deployed, but they could be in a new vignette.*<br>The vignette is not concerned with counterattacking the enemy aircraft or submarines.<br>It is not a wartime situation.<br>Sea State 3.<br>Ships readiness condition is YOKE.<br>Alpha controls 2 UAVs and Beta 2 other UAVs.<br>• *Each ship has two organic UAVs.*<br>During normal operations, the UAVs have separate, non-overlapping areas of regard (AoRs).<br>*Alpha ship's helo is in the air.*<br>*The SA has an area of regard that will detect both the launched missiles.*<br>*The Air Defense Commander (ADC) is on board Alpha.*<br>*Both ships are aware that a potentially hostile country has some fighter aircraft conducting training missions nearby.* |

**Mission Thread Template: Steps**

| Steps | Description | Quality Attribute, Capability, and Engineering Considerations |
|---|---|---|
| 1 | Alpha develops the air defense plan (ADP) and Rules of Engagement (ROE) and sends them to Beta. The plan assigns to Alpha the AoR to the west, and Beta the AoR to the east. Alpha configures surveillance and weapons systems to support eastern engagements. | 1. *How much is predefined and how much is done manually?*<br>2. *ROE dictates a "Shoot-Look-Shoot" defense.*<br>3. *How is this communicated to Beta? Using the fleets NRTC: near-real-time communications.* |
| 2 | The SA aircraft detects that the 5 enemy aircraft have changed course and are heading toward the fleet at low altitude. | 1. *The enemy aircraft are within the AoR of the SA sensors. The SA has been tracking these aircraft and sending tracks to Alpha and Beta.*<br>2. *Need a "fleet" SA use case.* |
| 3 | SA informs both Alpha and Beta of the change. | 1. *Within X seconds of detecting the change*<br>2. *Using the GIG. Is the GIG usable for tactical near-real-time data? Probably not!*<br>3. *Need a use case on assigning the UAVs to track the aircraft at this point.* |
| 4 | Alpha (and Beta) go to General Quarters. | 1. *ADC informs the captain, who orders general quarters.*<br>2. *Using Internal Comms.* |
| 5 | SA detects that missiles have separated from the enemy aircraft and informs Alpha and Beta. | 1. *Within X seconds.* |
| 6 | Alpha assigns its 2 UAVs to track the missiles. | 1. *The legacy Defensive Engagement System (DES) cannot use external tracks to form a FCQ track.*<br>2. *Within X seconds.*<br>3. *Does the ADC have to do this manually?*<br>4. *Would they start tracking automatically if the missiles were within their AoR?*<br>5. *Would they have been tracking the aircraft?* |
| 7 | The 2 Alpha-controlled UAVs send FCQ tracks for the 5 missiles to both Alpha and Beta. | 1. *The 2 UAVs can redirect their payload to do this within YY seconds. (use case)*<br>2. *Takes XX seconds for the FCQ tracks to stabilize.*<br>3. *What is the comms between UAVs and ships for maneuver and payload control?* |

From: Introduction to the Mission Thread Workshop.
Carnegie Mellon University. 2013.

THALES
Building a future we can all trust

# Thank you

www.thalesgroup.com