Sécurité

CN - Horizon2020

Horizon 2020 Security

Best Practices for Security Proposal Writing

Armand Nachef

Coordinator of the French Security NCP Consortium, CEA

armand.nachef@cea.fr

DE LA RECHERCHE À L'INDUSTRIE cea

Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR, DE LA RECHERCHE ET DE L'INNOVATION

SGDSN

Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR

SAFE CLUSTER by Pegase & Risques

Systematic Paris Region Systems & ICT Cluster

cpu CONFÉRENCE DES PRÉSIDENTS D'UNIVERSITÉ

KEY MESSAGES
FOR PUTTING TOGETHER A HORIZON 2020 PROPOSAL

1. Understand the real political reasons of the call for proposals
   (especially for the security calls)

2. Think at a holistic SYSTEM level

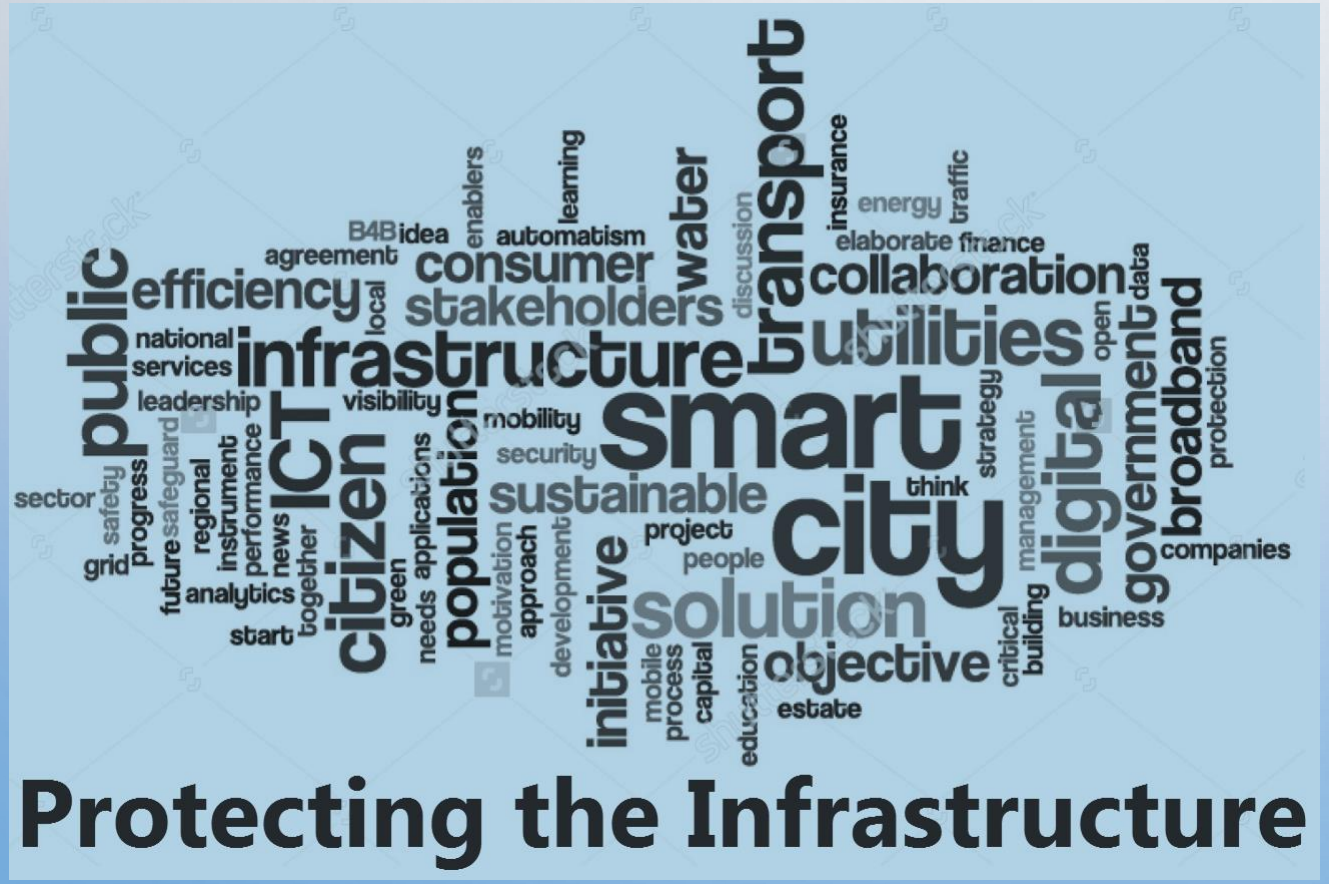
3. Start your proposal by writing the expected impact and after having a very clear idea about “How to impact”.
   The impact part of the proposal should be written by the practitioners

4. Structure your consortium to respond to all expected impacts

“1. Political reasons of the call for proposals”

SU-INFRA

PROTECTING THE INFRASTRUCTURE OF EUROPE AND THE PEOPLE IN THE EUROPEAN SMART CITIES



GENERAL INFORMATION ON THE CALL/TOPIC

Year	Topic (Type of Action)	Title	Budget (M€)	Deadline
2019	SU-INFRA01-2018-2019-2020 (IA) SU-INFRA02-2019 (IA)	Combined physical and cyber threats “Soft" targets in Smart Cities	22,0 16,0	22 Aug 2019

THE REASONING BEHIND THE INFRA CALL

- **Threats** against **crowded areas** and disruptions in the operation of our **countries' infrastructure**.

- **Reducing the vulnerabilities** of critical infrastructure and increasing their **resilience** is one of the major objectives of the EU. An adequate level of protection must be ensured and the detrimental effects of **disruptions on the society and citizens** must be limited as far as possible.

- Recent terrorist attacks have shown a focus on so-called **soft targets**, which may have less long-term physical impact but which may be highly damaging in terms of **victims** and subsequent **psychological and sociological impacts**.

POLICY CONTEXT - CIP

CIP Policy:

- Directive 2008/114/EC – Identification and designation of EU Critical Infrastructure
- European Programme for CI Protection (COM (2006) 786)
- NIS Directive (UE) 2016/1148

- **Main priorities on CIP:**
  - Identification of tools, including indicators, to protect CIs from Hybrid Threats;
  - Methods and tools for addressing insider threats to CI, such as background checks and awareness raising in cooperation with relevant authorities;
  - New challenges to CIP and emerging threats (e.g. cyber, insider threats, drones…)
  - Other: CI Risk assessment methods, transnational cooperation,
    civ-mil cooperation / cooperation with international orgs.

POLICY CONTEXT - PROTECTION PUBLIC SPACES

- **COM(2017) 612 – Action Plan protection of public spaces**
  - Guidance material and Exchange of best practices to support MS.
  - Improving cooperation between local actors and the private sector
  - Increased financial support: €18.5 million from the ISF. Further €100 million from the Urban Innovative Actions.

- **COM(2018) 845 final - SU Progress Report, Dec. 2018 – State of play**
- **Main priorities on Protection of Public Spaces**
  - Focus on known threats but also on emerging threats (e.g. drones, CBRN attacks)
  - Enhance cooperation between public actors, private actors and citizens.
  - New solutions to protect EU cities while maintaining their openness and not creating new vulnerabilities.
  - Consider the human factor.

- **SRE 2018 Panel on Protection of Public Spaces**
  - Take a look at the conference proceedings!!

SU-DS

DIGITAL SECURITY
CYBERSECURITY AND DIGITAL PRIVACY

SU-DS : 2018 → 2020

Year	Topic (Type of Action)	Title	Budget (M€)	Deadline
2019	SU_DS03-2019-2020 (IA) SU-DS05-2018-2019 (RIA) SU-DS05-2018-2019 (IA)	Digital Security and privacy Critical sectors: Privacy Accountability Critical sectors: Privacy Accountability	18,0 10,0 10,0	22 Aug 2019

EVOLVING THREAT LANDSCAPE IN CYBERSECURITY

- Proliferation of (poorly secured) IoT devices
- Blurring lines between state and non-state actors
- Hybrid attacks on western democracies
- Fake news
- Evolving cybercrime business models
- Cyber espionage on the rise
- Dependence on foreign security technologies
- Persisting critical infrastructure vulnerabilities
- Attempts to promote new internet governance model
- Vulnerabilities of third countries

POLICY CONTEXT (1/5)

- **Digital Single Market Strategy – COM(2015) 192;**

- **European Agenda for Security – COM(2015) 185;**

POLICY CONTEXT (2/5)

- **NIS Directive – Directive (EU) 2016/1148 of 6/7/2016 concerning measures for a high common level of security of network and information systems across the Union;**

- **eIDAS – Regulation (EU) 910/2016 of 23.7.2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;**

- **General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679 of 27.4.2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;**

- **Communication on "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry" – COM(2016) 410 of 5.7.2016;**

- **Contractual Public-Private Partnership on Cybersecurity – July 2016;**

POLICY CONTEXT (3/5)

Proposal for an e-Privacy regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - COM(2017) 10 of 10.1.2017;

State of the Union 2017 - speech of the President of the Commission (13/09/2017)

- ✓ **cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks;**
- ✓ **there is a need for a Europe that protects, empowers and defends;**
- ✓ **the priority is to better protect Europe in the digital age;**

Cybersecurity Package 2017 (13/09/2017)

- ✓ **Joint Communication JOIN(2017)450: The Commission announced the intention to create a Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre.**

POLICY CONTEXT (4/5)

Conclusions from the Tallinn Digital Summit (29/09/2017):

- "We should make Europe a leader in cybersecurity by 2025, in order to ensure the trust, confidence, and protection of our citizens, consumers and enterprises online and to enable a free and law-governed internet."

- "Europe needs a common European approach to cybersecurity. Europe has to function as a single European cyberspace and a single cybersecurity market, including in terms of world-class and state-of-the-art security certification and joint standards, operational capacity, and collective crisis response."

POLICY CONTEXT (5/5)

Council Conclusions (20 November 2017)

… "21. WELCOMES the intention to set up a Network of Cybersecurity Competence Centres to stimulate the development and deployment of cybersecurity technologies and to offer an additional impetus to innovation for the EU industry on the global scene in the development of next-generation and breakthrough technologies, such as artificial intelligence, quantum computing, blockchain and secure digital identities;

22. STRESSES the need for the Network of Cybersecurity Competence Centres to be inclusive towards all Member States and their existing centres of excellence and competence and pay special attention to complementarity and with this in mind NOTES the planned European Cybersecurity and Research Centre, which should, as its key role, focus on ensuring complementarity and avoiding duplication within the Network of Cybersecurity Competence Centres and with other EU agencies;" …

“2. Think at a holistic SYSTEM level”

THE 5 PRINCIPLES IN SYSTEM ARCHITECTURE

Every system has a mission

All stakeholders and concerns should be identified

Every system component should have an owner

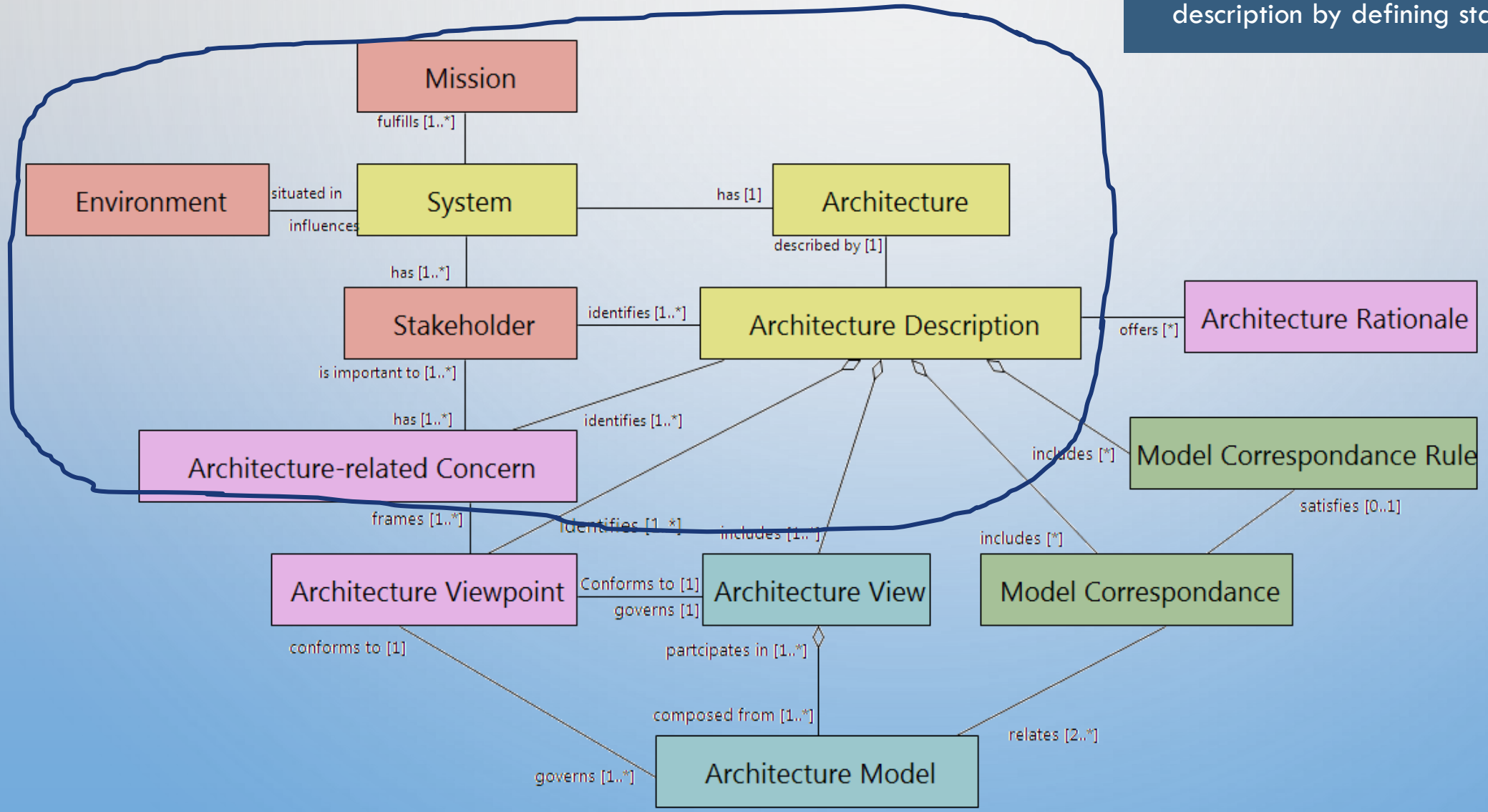
A high-level model should describe the system

Data is important and should be considered

ISO 42012 standard

Requirements for Describing System, Software and Enterprise Architectures

- aims to standardize the practice of architecture description by defining standard terms



MAIN BENEFITS OF USING *ARCHITECTURAL DESCRIPTIONS*

1. Communicate among clients, acquirers, suppliers and developers as a part of contract negotiations;

2. Communicate among parties involved in the development, production, deployment, operation and maintenance of a system;

3. Analyze and evaluate alternative architectures;

4. Establish criteria for certifying implementations for conformance to an architecture

FIVE MAIN ACTORS IN HORIZON 2020 SECURITY PROJETS:

1. Policy makers
   - Define the policy objectives and provide the overall strategic direction
   - Topics in the security research calls are supporting the implementation of the different policies in the different domains

2. Practitioners
   - Define the operational requirements to ensure achievement of intended policy objective

3. Researchers (RTOs and Academia)
   - Understand underlying phenomena
   - Look beyond the state-of-the-art

4. Industry
   - Private and public sector to work hand in hand in developing a vision for tomorrow's security ecosystem
   - Without the commitment of security industry, innovative solutions would remain trapped in endless cycles of research
   - A strong EU security market is fundamental to increase the competitiveness of the industrial base and the level of confidence in the security of supply for strategic technologies

5. Citizens
   - All Calls have a “Human Factor” embedded within.
   - A better integration of the societal dimension means more trust and resilience
   - A better societal consideration into technological requirements means socially compatible solutions.
   - Understanding of causes and societal roots of a an event and of human behavior (anticipation).

THE MAIN ROLES OF PRACTITIONERS IN THE SECURITY PROJECTS

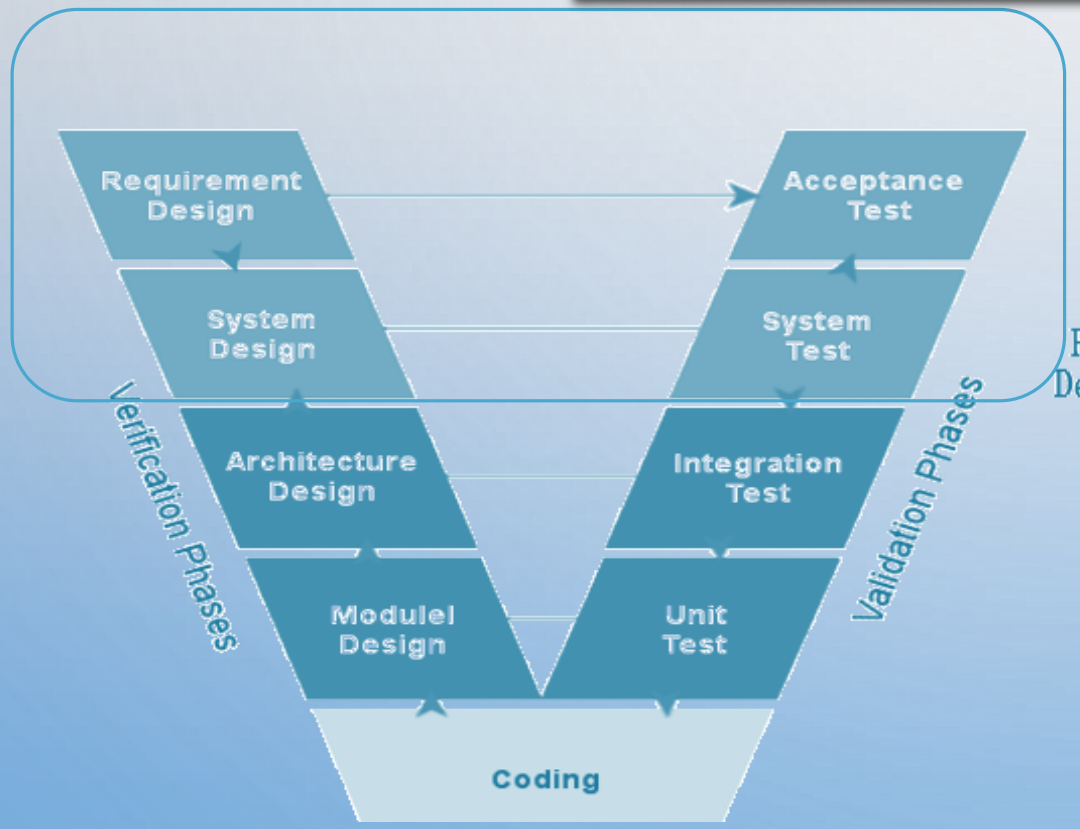
- Identify the innovation needs and requisites:
  - System functional features
  - capabilities, and behaviour
  - Expected operational impact
  - Ethics & legal aspects
- Verify & Validate the requirements and possibly the architecture
- Define use case scenarios
- Provide human and material resources to build Pilots / Demos
- Perform tests:
  - functional testing,
  - smoke and sanity testing,
  - test scenarios
- Validate the solution
- Dissemination activities

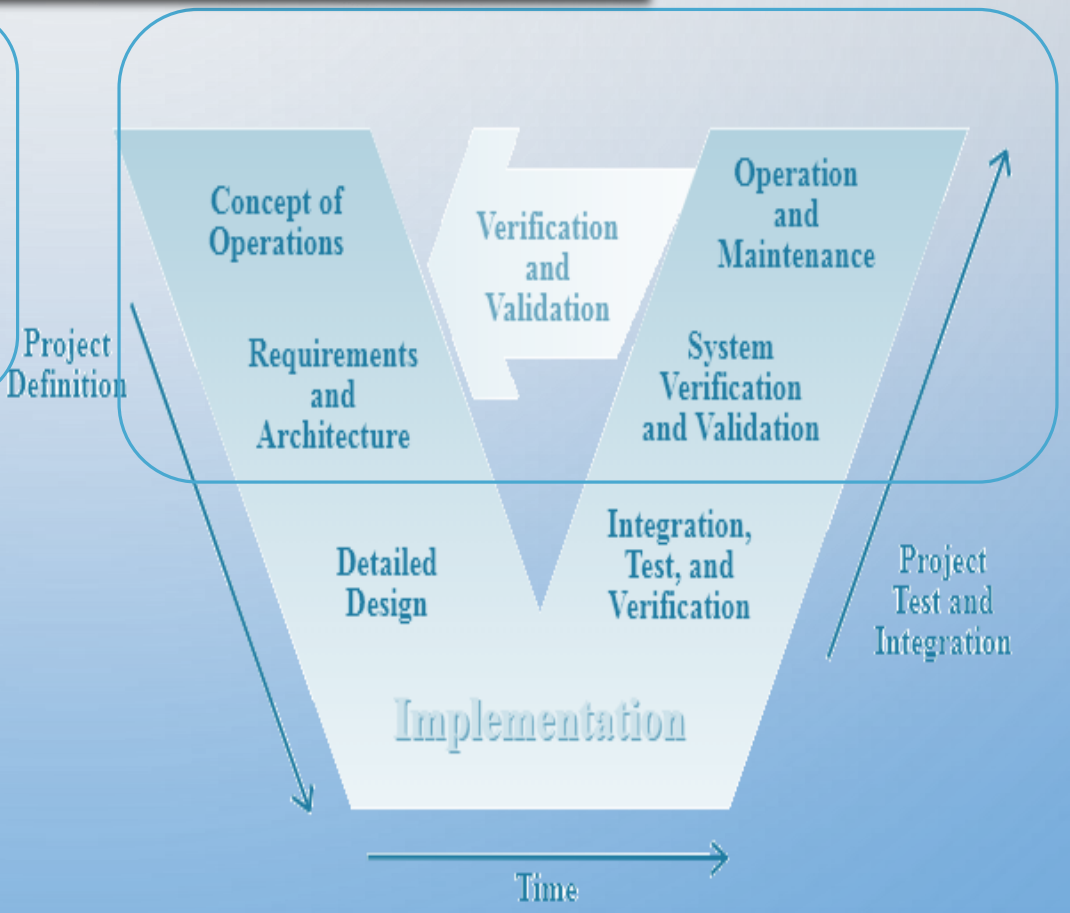
It's very important to know your role in the V-Model

V-MODEL

- V-Models are still pertinent universal graphical representations of a systems development lifecycle
- There are many V-Models
  - 2 examples of V-Models:

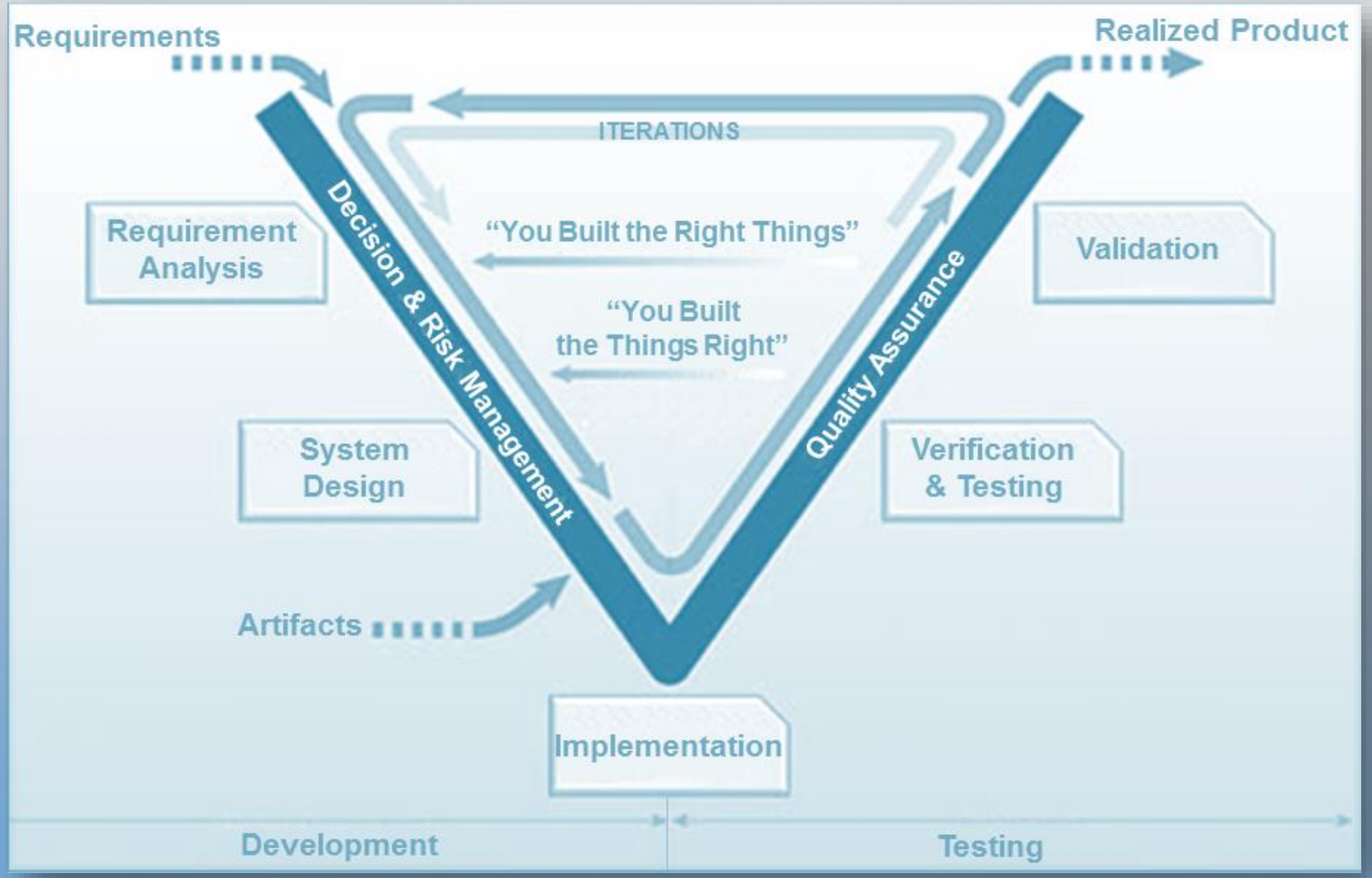
The role of practitioners is on the top of the V-Model





V-MODEL AND METHODOLOGIES

- V-models can fil with all methodologies: agile, formal, semi-formal, traditional, …



“3. The impact part of the proposal should be written **by the practitioners/operators.** **Start your proposal by writing the expected impact and after having a clear idea about how-to-impact** ”

Writing the impact part

- Define the architecture as a whole (high level view)
- Describe the value chain and all stakeholders
- Define how the results will impact each stakeholder
- Describe how the new system will affect its environment
- Define the steps needed to achieve the mid-term and long-term impacts

“4. Structure your consortium to respond to all expected impacts”

Build your consortium

- Choose the most relevant partners in the set that you have described in the “impact part”
- Choose partners according to the TRLs to reach

PARTNER SEARCH

- Your own network
- Annual Security Information Day, Brokerage event, & SMI2G in Brussels
- Events organised by the National Contact Points (NCPs)
- NCP Personalised support & assistance in partner search
- SEREN4 SEREMA
- Enterprise Europe Network (EEN) cooperation opportunities database
- EC Partner search site
- CORDIS partner search platform

STRICTLY FOLLOW THE PROPOSAL TEMPLATE

H2020 Programme

Proposal template 2018-2020

Administrative forms (Part A)
Project proposal (Part B)

Research and Innovation Actions (RIA)
Innovation Actions (IA)