D'APPOLONIA

Process Improvement and Emerging Risk Management

The CMMI +SAFE Approach

SEVENTH FRAMEWORK PROGRAMME

iNTeg-Risk

Early Recognition, Monitoring and Integrated Management of Emerging, New Technology Related, Risks

EU-VRi

Grant agreement number: CP-IP 213345-2

Fabio Bagnoli

Stuttgart – 3 June 2009

CMMI & +SAFE MODEL

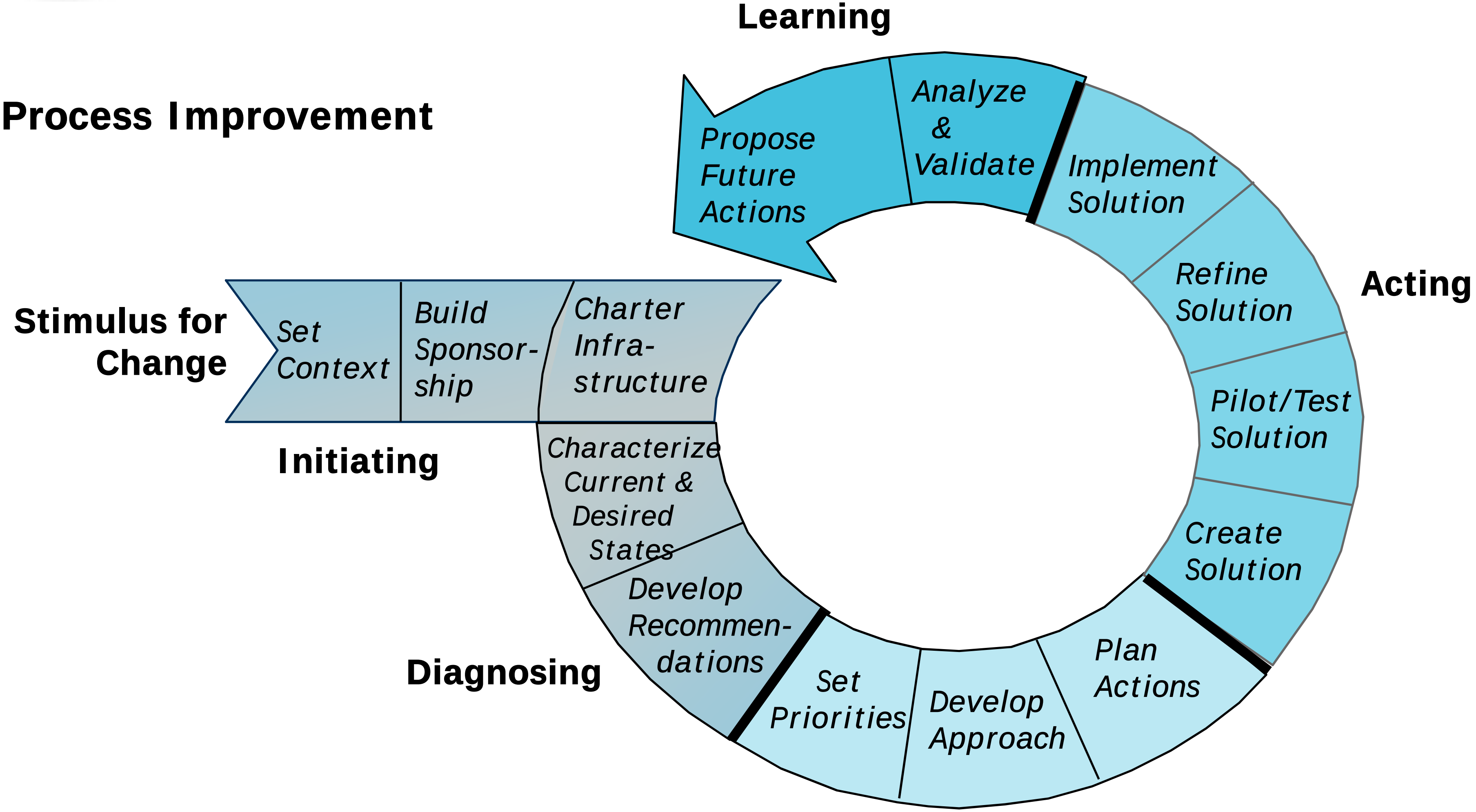
- CMMI®, Capability Maturity Model for Integration, has been developed by the Software Engineering Institute (SEI) at Carnegie Mellon University, Pittsburgh USA, to improve organisational practices in the use and development of technology. CMMI® presents successful practices for improving development, sustainment and maintenance, and management of software-intensive systems.

- Although CMMI® provides a framework in which safety activities can take place, the model is not focused on safety. In order to fill the gap of including Safety Processes within a common CMMI® framework, the +SAFE approach has been developed by the Australian Defence Material Organisation (DMO).

- +SAFE is, an extension of the CMMI® for the safety of software and systems engineering. The extension consists of two additional process areas to the CMMI® model, providing a basis for process improvement and appraising of Safety related issues of any organization.

THE CMMI MODEL

Process Improvement



Establishing

http://www.sei.cmu.edu/ideal/ideal.htMl

CMMI PROCESS AREAS

- A Key Process Area (KPA) is a cluster of related practices in an area that, when implemented collectively, satisfy a set of goals considered important for making significant improvement in that area.

- The CMMI Process Areas (22) can be grouped into the following four categories to understand their interactions and links with one another regardless of their defined level:
  - Process Management
  - Project Management
  - Engineering
  - Support

- Each process area is defined by a set of goals and practices. There are two categories of goals and practices:
  - Generic goals and practices: They are part of every process area.
  - Specific goals and practices: They are specific to a given process area.

CMMI MATURITY LEVELS

- There are five levels defined along the continuum of the CMMI
  - Level 1 - Ad hoc (Chaotic)
  - Level 2 - Repeatable
  - Level 3 - Defined
  - Level 4 - Managed
  - Level 5 – Optimizing
- According to the SEI: "Predictability, effectiveness, and control of an organization's software processes are believed to improve as the organization moves up these five levels.”
- Since +SAFE is not currently integrated in the CMMI model, its Process Areas are not foreseen in the scheme of the maturity levels definition.
- However +SAFE Specific Goals may be integrated in the implementation and appraisal within the acquisition of the Maturity Levels where the CMMI Process Area belongs to.

THE SCENARIO FOR THE +SAFE IMPLEMENTATION

- Innovative technologies introduce new Safety Risks that sometimes may not been foreseen by traditional safety risk management approaches dealing with generic field of application → Unlike others, +SAFE is focused on Software and Systems Engineering, thus more addressed, by its nature, to the development of new technologies.

- The intrinsic flexibility and integrability of the +SAFE model allows strong synergies with most of the safety standards, tailoring the high level definition of the +SAFE model on the needs and requirements of the specific application.

- The +SAFE model can be adapted to create common guidelines for emerging risks that could support the definition of a common Safety Paradigm, considering the emerging risk throughout the whole life-cycle of the system or of the process involved in the emerging risk.

A KEY QUESTION OF THE INTEG-RISK PROJECT

Is it possible to address all emerging risks within a same management framework?

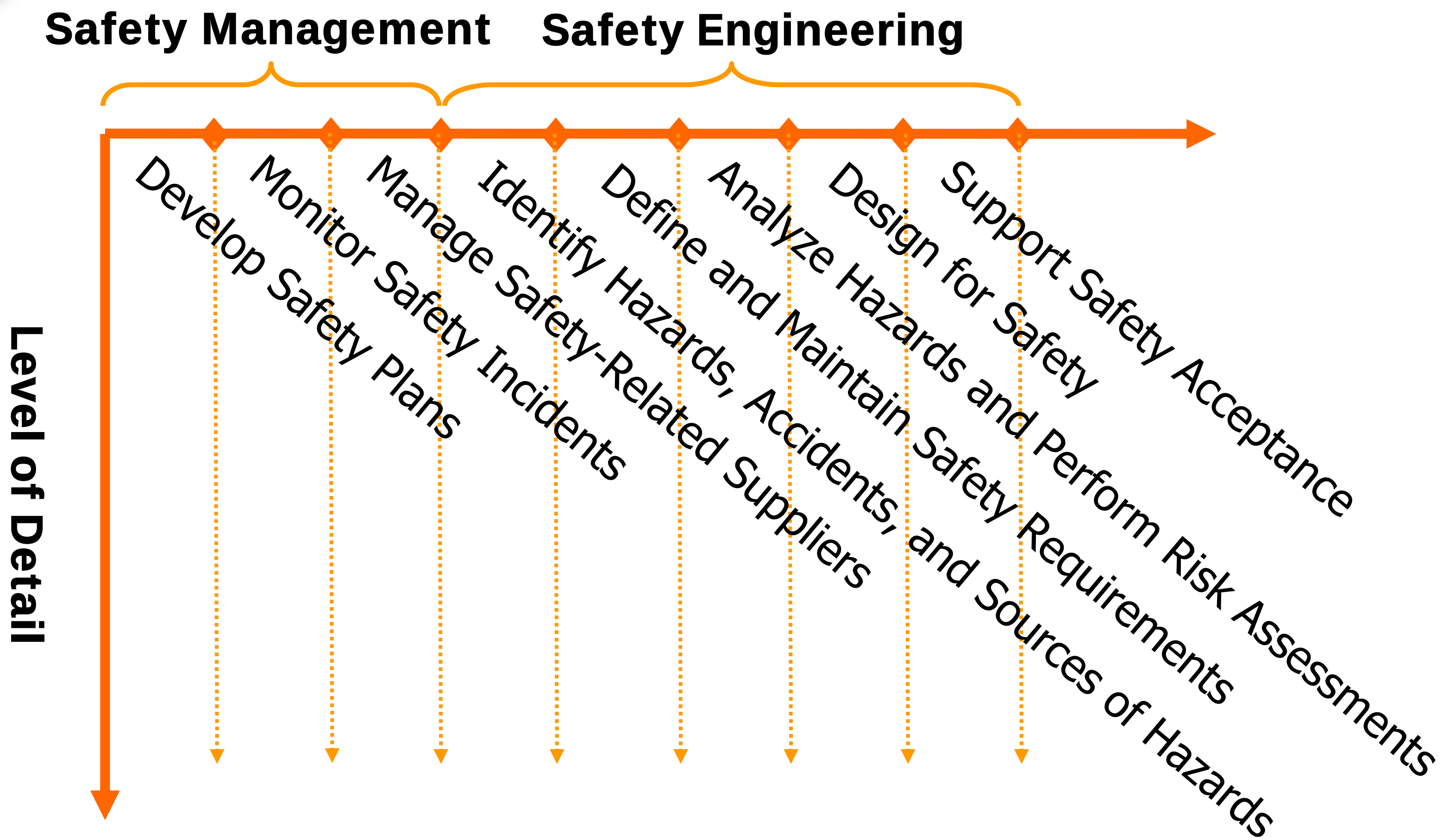
- Objective of the Integ-Risk project is to define a new safety paradigm, based on a common framework for integrated risk management.
- Integrated Safety Management includes the risk management along the whole life-cycle of the system or of the process involved in the emerging risk them selves.
- Moreover, capabilities of integration within wider scenarios should be foreseen.
- The INTEG-Risk project should start by focusing on the identification of already defined methodologies for risk analysis and management to be integrated within a Safety Model on which basing the Safety Paradigm.
- +SAFE Model can be proposed as an approach to emerging risks management.
- +SAFE is focused on Software and Systems Engineering, thus more addressed, by its nature, to the development of new technologies.
- +SAFE can be adapted to create common guidelines for emerging risks that could support the definition of the paradigm, considering the emerging risk throughout the whole life-cycle of the system or of the process involved in the emerging risk.

+SAFE PROCESS AREAS AND RELATED SPECIFIC GOAL

Since +SAFE is an extension of CMMI, it uses the same assumptions, model, structure and taxonomy of CMMI and it involves the general process-area and capability-level interactions as CMMI.

CMMI PA Category	Safety Process Area	Specific Goals
Project Management	Safety Management	SG1 Develop Safety Plans
		SG2 Monitor Safety Incidents
		SG3 Manage Safety-Related Suppliers
Engineering	Safety Engineering	SG1 Identify Hazards, Accidents, and Sources of Hazards
		SG2 Analyze Hazards and Perform Risk Assessments
		SG3 Define and Maintain Safety Requirements
		SG4 Design for Safety
		SG5 Support Safety Acceptance

+SAFE TAILORING APPROACH


Safety Management
Safety Engineering
Level of Detail
Develop Safety Plans
Monitor Safety Incidents
Manage Safety-Related Suppliers
Identify Hazards, Accidents, and Sources of Hazards
Define and Maintain Safety Requirements
Analyze Hazards and Perform Risk Assessments
Design for Safety
Support Safety Acceptance

- The first feature to be tailored is the number of Specific Goals that will be considered within the implementation of +SAFE Model.

TAILORING OF THE +SAFE SPECIFIC GOALS

- As an extension to CMMI, +SAFE is a process model defining goals to be achieved and increasing levels of performance capability. The model provides indicators on how goals can be achieved, but these are not prescriptive and an organization is able to select the approaches it wishes to adopt to achieve the goals.
- Normally, not all the Safety Areas and not all the Specific Goal are applicable or required by a project.
- Tailoring +SAFE means choosing which features will be addressed by the implementation.
- Parameters on which basing the tailoring can be:
  - ✓ Implementation environment
  - ✓ Customer requirements
  - ✓ Customer needs
  - ✓ External relationships
  - ✓ Safety standard chosen (if any)
  - ✓ Country laws and regulations

CUSTOMIZATION OF THE LEVEL OF DETAIL IN INNOVATIVE FIELDS AND APPLICATIONS

- **The implementation of a Safety Management System requires an initial definition of the level of detail the implementation will deal with.**
  - “level of detail” refers to the distance between the Safety Processes being defined and the concrete daily activity of the system or organization.
  - Safety Processes may:
    - Deal with high level policies → Low level of detail
    - Be designed as work procedures → High level of detail
  - **The level of detail is according to:**
    - Information available about the system at a certain stage
    - Implementation environment needs and requirements
- **The lower the level of detail required by the implementation, the more the information needed about the system or organization.**
  - Starting from this point, innovative fields and the related emerging risks introduce a further difficulty in being managed, since the background information is limited compared to well-known fields.

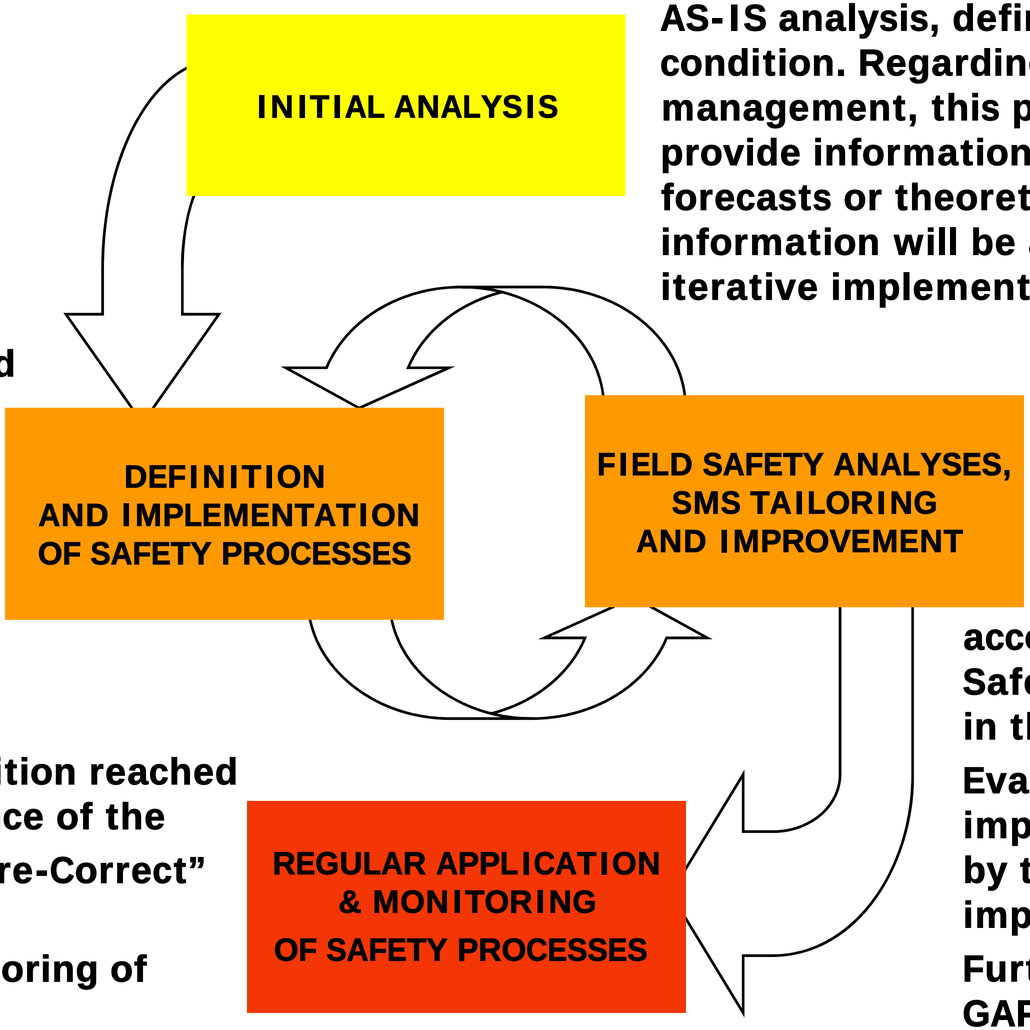
ITERATIVE APPROACH

- Safety Management in Innovative Fields is challenging
- There are no benchmark to evaluate the efficacy of the defined Safety Processes.
- The Safety Management process must be designed considering iterative steps: feedback from the field are collected and used to retrieve information about the implementation environment, efficacy of the Safety Processes, etc.
- The Safety Processes is defined according to the following steps:
  - Initial analysis
  - Safety Processes definition and implementation
  - Safety Processes application and monitoring
  - Iteration until convergence to an acceptable residual risk threshold

ITERATIVE APPROACH

- Initial Analyses, collection about the as-is conditions of the system under evaluation still remain a fundamental step.
- Definition and implementation of a preliminary set of Safety Processes. These processes will then be tuned according to feedback collected during the implementation phase.
- Application in the daily operations of these Safety Processes and monitoring though Safety analyses in order to evaluate the Safety conditions of the system and give feedback to the process with information for the improvement of the Safety Management System.
- Iterations has to be performed until the System reach an acceptable Risk level. Then the System can be considered “stable” according to this approach and normal application and monitoring can be performed.

ITERATIVE INFORMATION ACQUISITION


INITIAL ANALYSIS
DEFINITION AND IMPLEMENTATION OF SAFETY PROCESSES
FIELD SAFETY ANALYSES, SMS TAILORING AND IMPROVEMENT
REGULAR APPLICATION & MONITORING OF SAFETY PROCESSES

AS-IS analysis, defining the initial safety condition. Regarding emerging risks management, this phase normally provide information coming from forecasts or theoretical models. Real information will be acquired along the iterative implementation.

Implementation of Safety Processes as defined in a GAP analysis aiming at reaching an assessed TO-BE situation.

Evaluation of the level of accomplishment of the Safety Objectives defined in the TO-BE analysis.

Evaluation of the improvements achieved by the processes implementation.

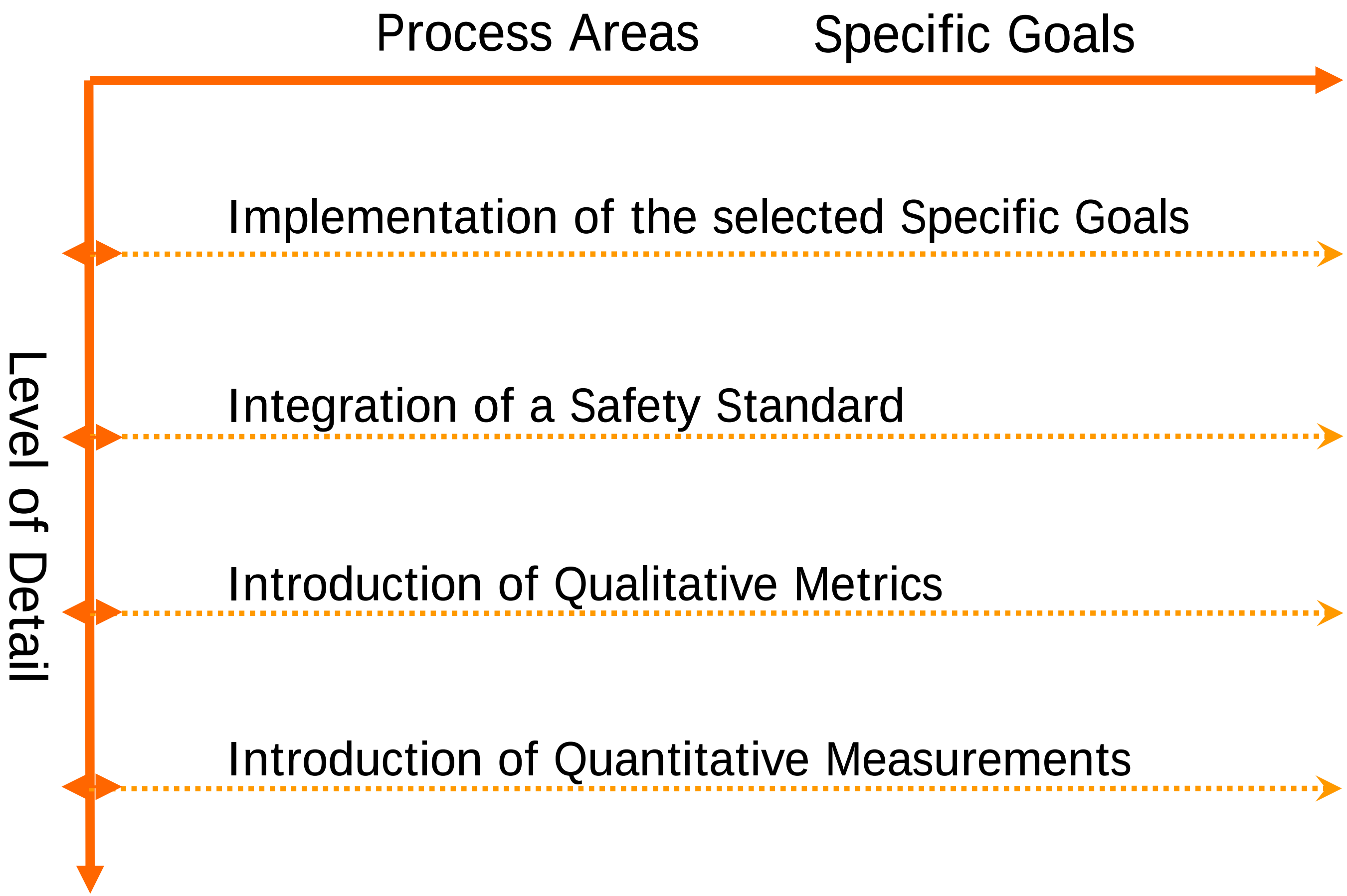
Further refining of the GAP towards the desired condition basing on the feedback from the field measurement.

Steady Safety condition reached after the convergence of the "Implement-Measure-Correct" Cycle.

Application & Monitoring of Safety Processes.

Verification of the correct implementation of the processes.

DETAIL LAYERS REACHED IN THE +SAFE IMPLEMENTATION



Process Areas

Specific Goals

Level of Detail

Implementation of the selected Specific Goals

Integration of a Safety Standard

Introduction of Qualitative Metrics

Introduction of Quantitative Measurements

- The second feature to be tailored is the Level of detail that the implementation of +SAFE Model will reach.

A POSSIBLE STP-BY-STEP APPROACH

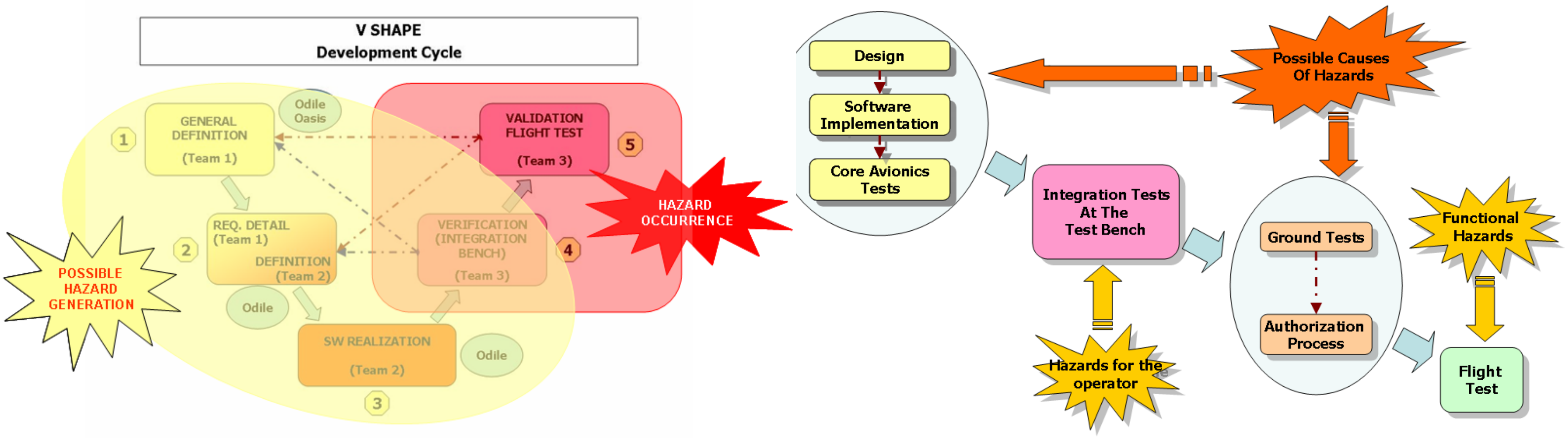
1. Implementation of the selected Safety Goals
   - ➢ It consists in the implementation of a Safety Management System applying the identified Process Areas and Specific Goals.
2. Integration of a Safety Standard
   - ➢ +SAFE model allows strong synergies with most of the safety standards that are usually focused on specific applications.
3. Introduction of Qualitative Metrics
   - ➢ Qualitative Metrics support the evaluation of the criticality of the risks or at the definition of risk categories (e.g. Impact-Occurrence matrix).
4. Introduction of Quantitative Measurements
   - ➢ Quantitative Measurement aims at the estimation of the risk with concrete input. Software tools implementing different kind of analyses can be exploited.
   - ➢ Integration with the KPI definition in Integ-Risk is CRUCIAL at this stage.

IMPLEMENTATION OF THIS APPROACH

- Initial implementation of the selected Specific Goals.
- The implementation of the Specific Goals should be performed according to the +SAFE Model specifications.
- The design of the Safety Processes should overcome the intrinsic lack of knowledge typical of a innovative field of application where emerging risks are being managed.
- Iterative implementation where analysis and measurements of the previous implementation cycle provides additional information about the system being managed.
- Safety standards are focused on specific application. The Safety Management System built on the +SAFE model, can be modulated according to the level of details that needs to be achieved. This allows to tailor the high level definition of the +SAFE model on the specific needs and requirements of each application.

USE CASE

- D’Appolonia worked for a Flight Test and Development Center, a specialized department of the United Arab Emirates Air Force involved the software integration, development and testing.
- The aim of our task was to establish and Organisational Safety System to define and maintain the relevant processes and procedures to be undertaken by the Organisation personnel and within each project of the Organization. Safety is in fact a critic issue for any Defence Organisation, particularly for Air Forces
- Safety processes have been defined according to MIL-STD-882C
- We propose to adopt this best practice to map the Safety process defined in WP2 in a common CMMI® framework. MIL-STD-882 Tasks have been applied to the CMMIQS Safety project



USE CASE

MIL 882C TAKS	*+SAFE v1.2 SPECIFIC GOALS*
Task 101 – System Safety Program	SGM1 Develop Safety Plan
Task 102 – System Safety Program Plan	SGM1 Develop Safety Plan
Task 103 – Integration/Management of Associate Contractors, Subcontractors, and Architect and Engineering Firms	SGM3 Manage Safety Related Supplier
Task 104 – System Safety Program Reviews/Audits	SGE3 Define and Maintain Safety Requirements
Task 106 – Hazard Tracking And Risk Resolution	SGE1 Identify Hazards, Accidents, and Sources of Hazards SGE2 Analyze Hazards and Perform Risk Assessments
Task 201 – Preliminary Hazard List	SGE1 Identify Hazards, Accidents, and Sources of Hazards
Task 202 – Preliminary Hazard Analysis	SGE2 Analyze Hazards and Perform Risk Assessments
Task 205 – System Hazard Analysis	SGE4 Design for Safety
Task 206 – Operating and Support Hazard Analysis	SGM2 Monitor Safety Incidents
Task 301 – Safety Assessment	SGE5 Support Safety Acceptance
Task 401 – Safety Verification	SGE3 Define and Maintain Safety Requirements

THE PRESENT GAP TOWARDS AN INTEGRATED APPROACH

The main gaps to be filled towards an integrated approach in emerging risks management implementing +SAFE includes the definition of:

- A common procedure for the selection of the Specific Goals to be selected for the implementation.
- Standardized methods for definition of the proper level of detail of the implementation:
  - Selection of Safety standards to be applied to specific field of application;
  - Common Qualitative Metrics;
  - Identification of suitable Safety Analyses for the Quantitative Measurements and related software tools implementing the safety analyses (including KPI)
- A common Taxonomy.

CONCLUSIONS – INTEG-RISK OBJECTIVES

- During the iNTeg-Risk project the +SAFE model will be tailored according to the definition of the emerging risks.
- Customized Safety Processes modeling will be proposed to assure that +SAFE is followed in the management of emerging risks.
- To integrate this approach already defined methodologies will be evaluated in terms of compliance with this approach.
- A gap analysis including specific recommendations will be provided.

Thank You
for the Attention!

Fabio Bagnoli
fabio.bagnoli@dappolonia.it