L’integrazione della ISO 26262 con le metodologie Agili

11° Workshop on Automotive Software & Systems – Milano, 7 Novembre 2013

Ernesto Viale

Agenda

- Overview
- AIDA Model
- AIDA for Agile

Company overview

Skytechnology è una società di consulenza e ingegneria, con sedi a Torino, Milano e Roma, che fornisce servizi nel mercato dei sistemi embedded:

- Progettazione e collaudo di dispositivi elettronici;
- Applicazione di standard di Functional Safety (i.e. IEC 61508, ISO 26262, IEC 62304, CENELEC 5012x, RTCA DO-178B) e PIMs (i.e. SPICE, ASPICE e CMMI), su:
  - Processi:
    - Gap Analysis e Remediation Plan;
    - Preparazione di Assessments e Appraisals di Terza Parte.
  - Prodotti:
    - Analisi RAMS;
    - V&V e system assurance.

Overview of AIDA Model

- Il Modello **Assistant for an Integrated Development Assessment** (**AIDA**) supporta l'**integrazione** della **ISO 26262** con **ASPICE,** con il **CMMI** e con le metodologie **Agili**.
- Il Modello AIDA organizza e **mantiene** la **maturità** e le **capability** dei processi di progettazione e produzione dell'Item, dell'HW e del SW, **integrando** le attività di **sicurezza funzionale** come richiesto dalla ISO 26262.
- Il Modello AIDA dovrebbe essere applicato inizialmente nella **Gap Analysis** iniziale e nella definizione del **Piano di Adeguamento** alla ISO 26262, nell'implementazione del processo di **continuous improvement** e nell'esecuzione periodica dei **functional safety assessment e audit**.

ISO 26262 Implementation

ISO 26262

AIDA Checklists

ISO 26262 Initial Assessment

Processes/Projects

Methods/Tools

Organization

Work Products

Suppliers/Contracts

Gaps

Corrective actions

AIDA Dashboard

Implementation Plan

Processes/Projects

Methods/Tools

Organization

Work Products

Suppliers/Contracts

ASPICE/CMMI-BASED "AS IS" ORGANIZATION

ISO 26262-EXTENDED "TO BE" ORGANIZATION

ISO 26262 Rollout and Operation

Pilot Projects

Safety-relevant Items

ISO 26262 Rollout

Operation

AIDA Checklists

Functional Safety Assessment

Gaps

Corrective actions

AIDA Dashboard

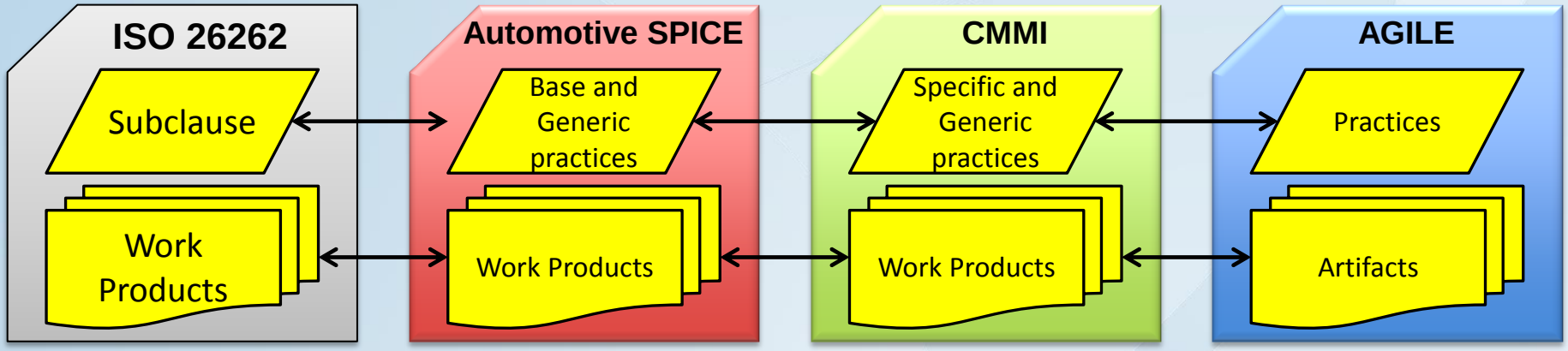
Implementation Plan

Agenda

- Overview
- AIDA Model
- AIDA for Agile

Versioni del Modello AIDA

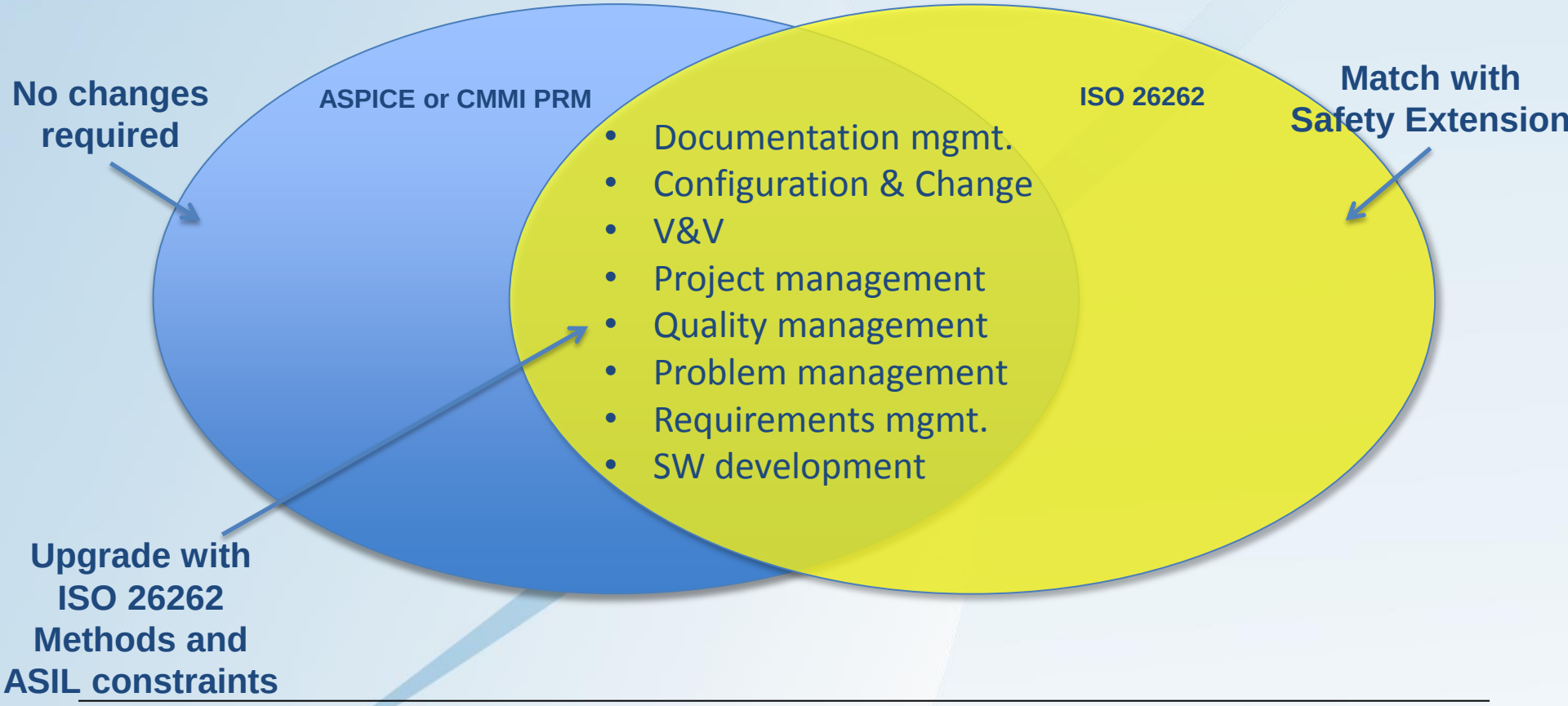
AIDA Version Mapping



ISO 26262	CMMI-DEV	ASPICE	AGILE
-	-	Process Category	-
Parts	Process Category	Process Group	-
Clause	Process Area	Process	-
Subclause «Objectives»	Purpose	Process Purpose	Agile Principles
Subclause «General»	Specific Goals	Process Outcomes	-
Subclause «Requirements»	Specific Practices	Base Practices	Practices
	Subpractices	-	
	Generic Goals	Process Attributes	
	Generic Practices	Generic Practices	
Work Products	Typical Work Products	Output Work Products	Artifacts

AIDA Integrated Reference Model

Il Modello AIDA aiuta a rispondere alla seguente domanda *"Come devo cambiare i miei processi di sviluppo, già conformi ad ASPICE o CMMI, e i miei prodotti per essere compliant alla ISO 26262?"*



AIDA Self-Assessment Toolkit

- Per supportare l'esecuzione della **Gap Analysis iniziale** e dei **Functional Safety Audit e Assessment**, il Modello AIDA fornisce un **Self-Assessment Toolkit**, disponibile gratis richiedendolo su www.aidamodel.org

- **L'AIDA Self-Assessment Toolkit** è costituito da:

  - le **Checklist di Assessment** (1 per ogni parte normativa della ISO 26262) che supportano la valutazione dei processi, metodi e work product rispetto alla ISO 26262.

  - Il **Dashboard** per la generazione dei Report di Assessment, statistiche e trend sull'avanzamento dell'implementazione della ISO 26262.

AIDA Self-Assessment Toolkit

AIDA Assessment Checklist

AIDA Model

<Insert Project Name>

Self-Assessment Checklist

Doc. ID.: <insert document ID>

Version: <insert document Version>

Project: <Insert Project Name>

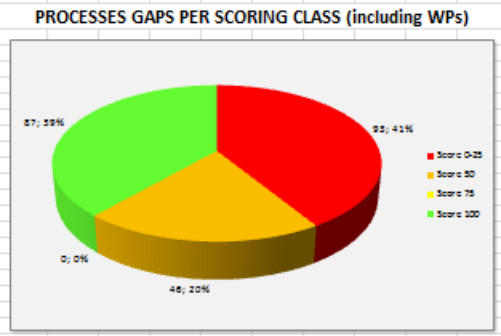
Sub-Project <Insert Sub-Project Name>

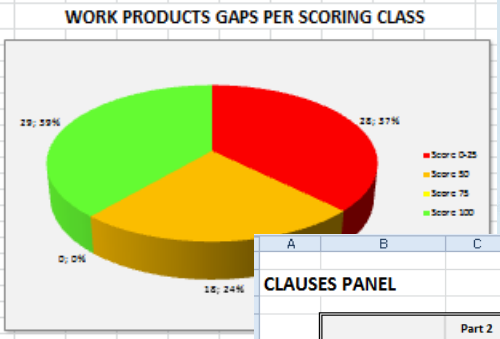
Self-Assessment Checklist Report

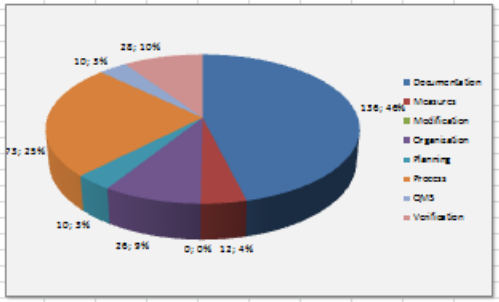
ISO 26262 - Part 4: Product development at the system level

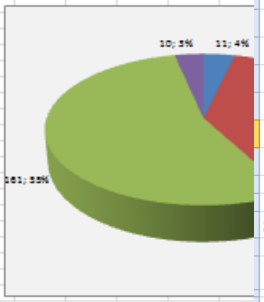
Cover | Work Products | Methods | Corrective Actions | Notes | Vocabulary

Assessment Dashboard









CLAUSES PANEL

	Part 2	Part 3	Part 4	Part 5	Part 6	Part 7	Part 8	Part 9
Clause 5								
Clause 6								
Clause 7								
Clause 8								
Clause 9								
Clause 10								
Clause 11								
Clause 12								
Clause 13								
Clause 14								

Rate	Criteria
100	Fully achieved
85	Largely achieved
50	Partially achieved
0-15	Not achieved
-	Not rated

SUB-CLAUSES PANELS

PART 2 - MANAGEMENT OF FUNCTIONAL SAFETY

Clause 5 Overall safety management	5.3.1	5.3.2	5.4.2	5.4.3	5.4.4	5.4.5	5.5.1	5.5.2	5.5.3						
management during the concept phase and the product development	6.3.1	6.3.2	6.4.2	6.4.3	6.4.4	6.4.5	6.4.6	6.4.7	6.4.8	6.4.9	6.5.1	6.5.2	6.5.3	6.5.4	6.5.5
Clause 7 Safety management after	7.3.1	7.3.2	7.4.2	7.5.1											

Cover | Gaps Synoptics | Gaps Metrics | Processes | Work Products | Methods | Corrective Actions | Metrics Database

CORRECTIVE ACTIONS ON SAFETY LIFECYCLE PROCESSES		C. A. CHARACTERIZATION	
C.A. ID	Corrective Action	C. A. Area	C. A. Priority
PART 2	MANAGEMENT OF FUNCTIONAL SAFETY		
P2-CA01	Develop and institutionalize a Quality Management System compliant with ISO 9001 for the primary and supporting processes involved in the functional safety management of vehicle electronics. The main phases are the following: a) define the scope and objectives of the QMS and update the existing Quality Manual b) develop/update the procedures, work instructions and work products templates c) train involved persons on QMS processes and procedures d) apply procedures and track quality records e) perform audits and a management review at the end of 2012 See the following files for the evaluation of the applicability of the production QMS: - ISO9001-Work.xls - Valutazione Procedure SIS Quality 161111.xls This corrective action should be furtherly detailed with operative steps.	QMS	Medium High

Agenda

- Overview
- AIDA Model
- AIDA for Agile

L'approccio Agile

- Le metodologie Agili sono basate sui principi delle **CONTINUOUS CHANGES** e del **DELIVERING VALUE**
- L'obiettivo è di incrementare la qualità dei prodotti e dei processi di sviluppo.

Che non implica caos o mancanza di formalizzazione!

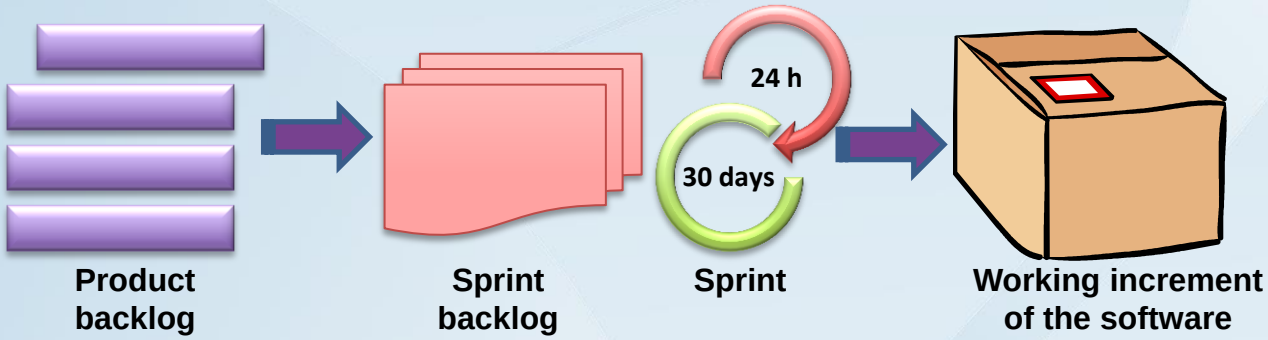
- I prodotti safety-relevant devono fornire evidenza dell'implementazione dei requisiti di sicurezza ("…*provide evidence that all reasonable system safety objectives are satisfied.*").

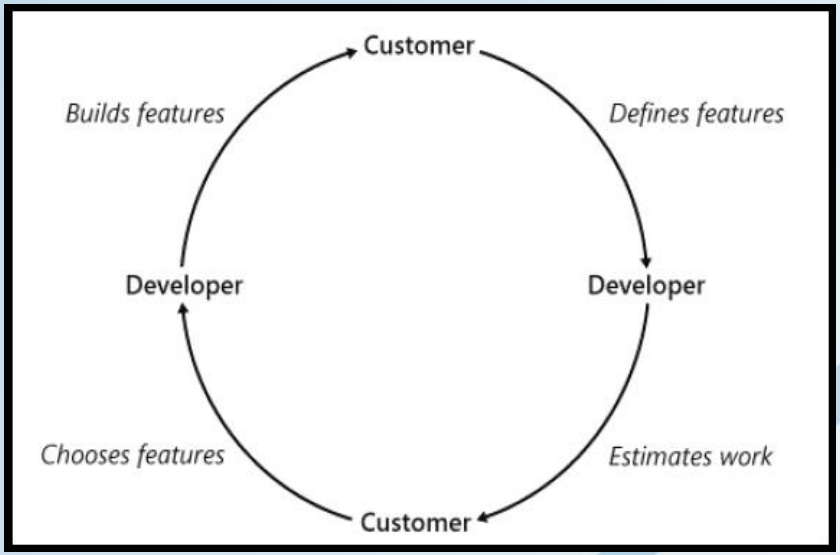
Che non implica mancanza di agilità!

- La progettazione di un prodotto sicuro può essere eseguita con un approccio agile.

Agile Development

Scrum





XP – Extreme Programming

Lean Development

Agile applicato al software safety-critical

Agile e IEC 61508

- Vuori, M.; “Agile development of safety-critical software ”

Agile e Avionics DO-178C

- Douglass, B. P.; “Agile analysis practices for safety-critical software development”

Agile e Railways EN 50128

- Gardner, P.; “Agile methods and safety-critical software ”

Agile e le FDA regulation

- Morsicato, R. and Shoemaker B.; “Agile Methods in Regulated and Safety-Critical Environments”
- Van Schooenderwoert, N.; “Safety-Critical Applications Built via Agile Discipline”

Altri

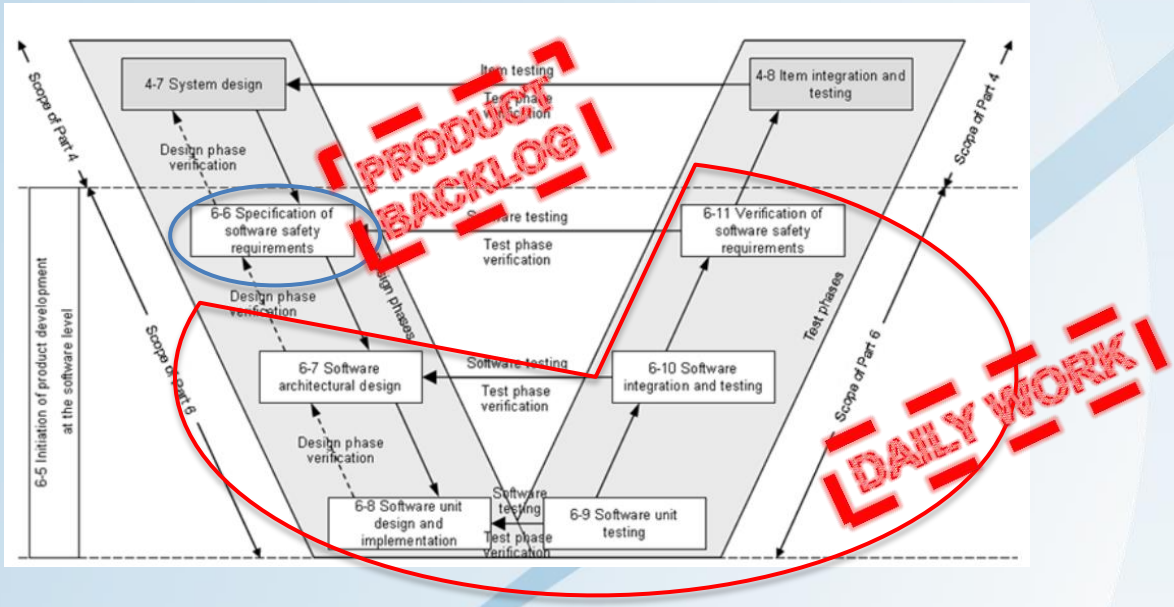
- Wolff, S.; “Scrum goes formal: Agile methods for safety-critical systems”

BASATO su Agile Project Management e il Lean Manufacturing

- Fornisce gli elementi per rendere agile l'implementazione della ISO 26262;
- Identifica le pratiche da integrare nei processi di progettazione della sicurezza;

PREVEDE LO SVILUPPO DEL SOFTWARE (ISO 26262-6) SU SCRUM

- Fa riferimento a roatche, principi e artifact della metodologia SCRUM.



L'integrazione tra SCRUM e ISO 26262 non intende essere "fully agile", ma fornisce indicazioni per un approccio snello e rapido per implementare la sicurezza funzionale

I PRINCIPI SU CUI SI BASA IL MODELLO SONO:

- Tailoring
- Automation
- Iterations
- Inspection
- Adaption
- Embedded compliance

*"The organization may **tailor** the safety lifecycle for application across item developments, …, but only if such a tailoring is limited to applying one or more of the following permissions:*

*a) subphases, activities or tasks may be **combined** or split, or*

b) an activity or task may be performed in a different phase or subphase, or

c) an activity or task may be performed in an added phase or subphase, or

*d) phases or subphases may be **iterated**."*

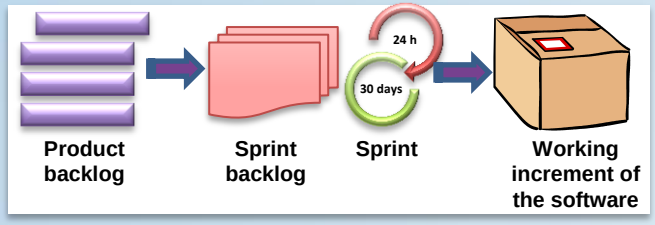
[1] ISO 26262-2:2011

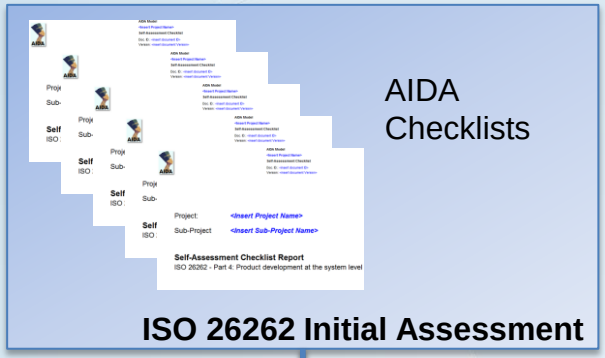
ISO 26262 Implementation

ISO 26262

AIDA for AGILE

Processes/Projects



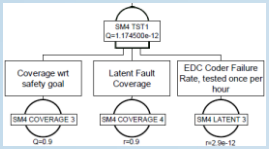


AIDA Checklists

ISO 26262 Initial Assessment

Processes/Projects

Methods/Tools

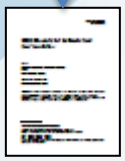


Organization

Gaps

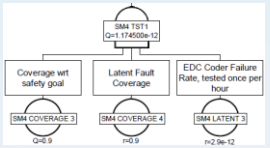
Corrective actions

AIDA Dashboard

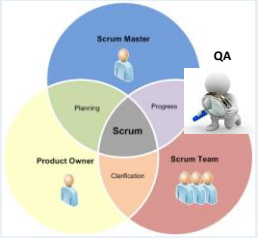


Implementation Plan

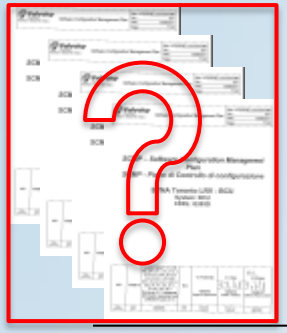
Methods/Tools



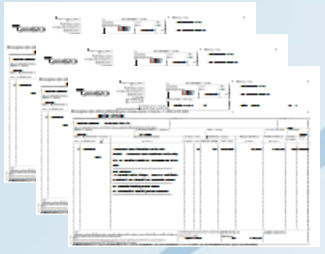
Organization



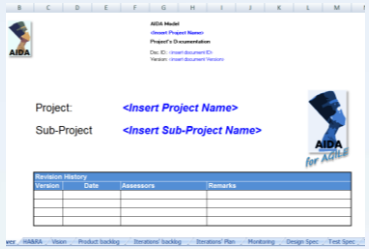
Work Products



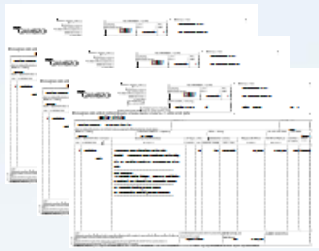
Suppliers/Contracts



Work Products



Suppliers/Contracts

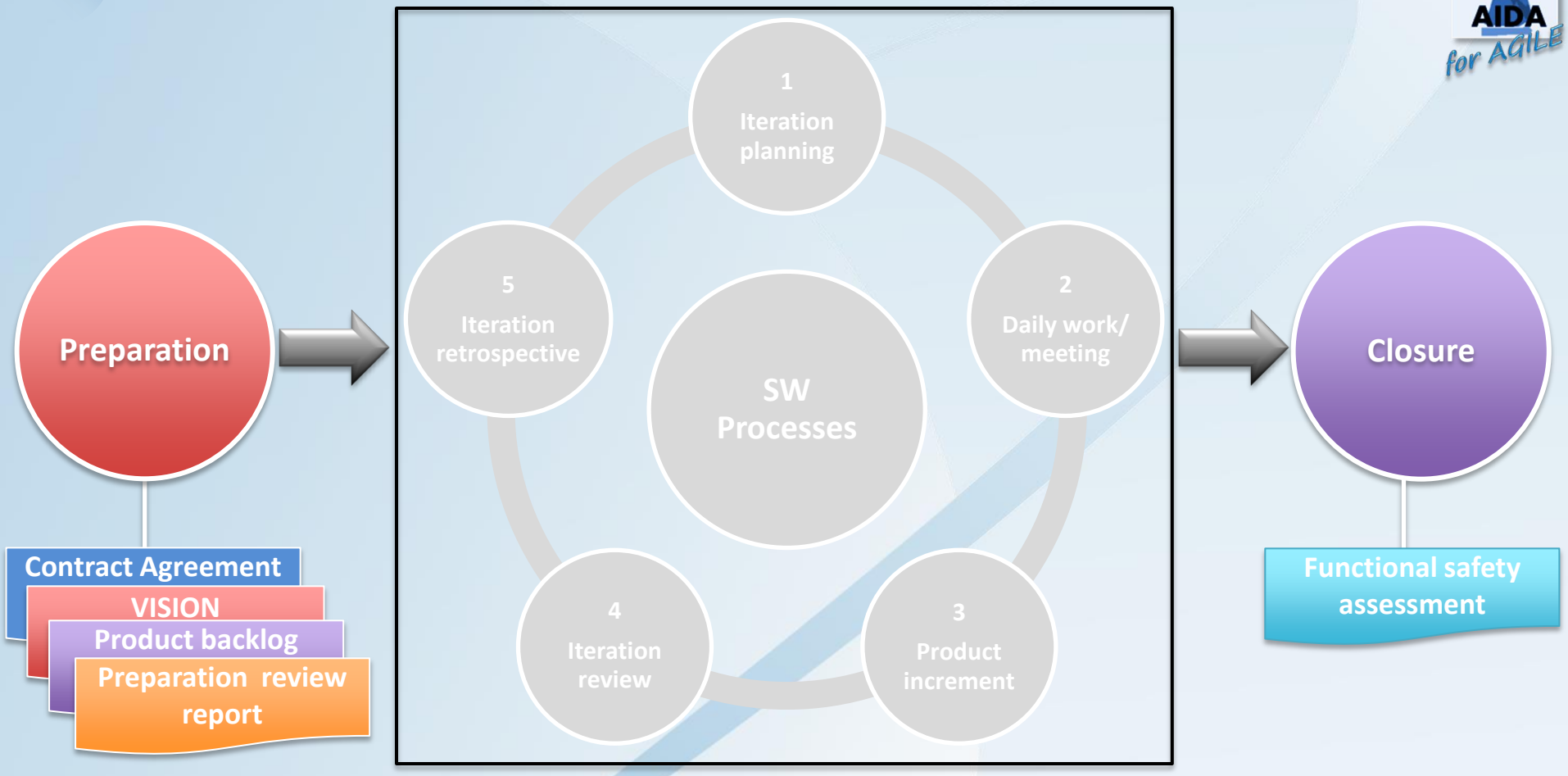


AGILE-BASED "AS IS" ORGANIZATION

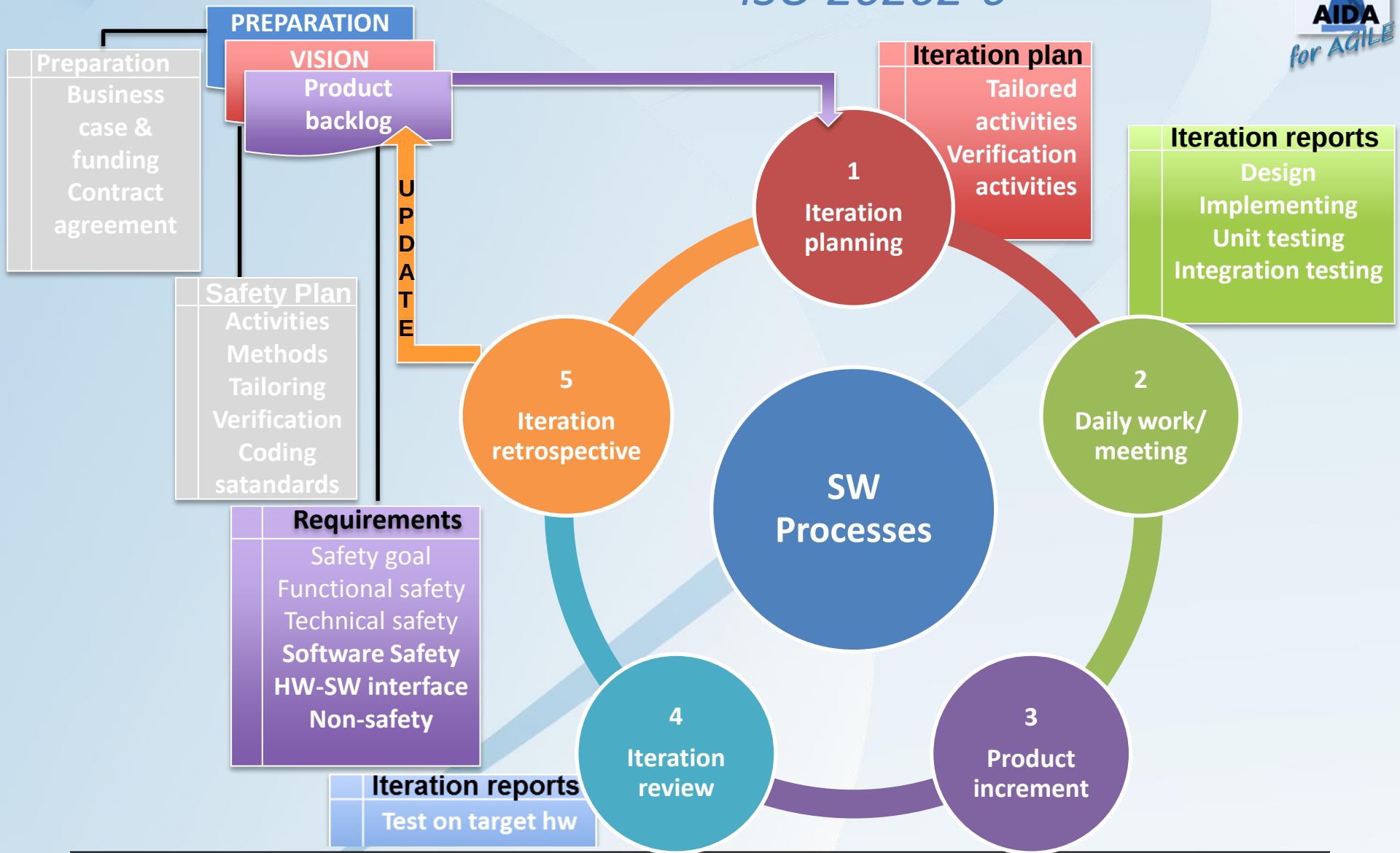
ISO 26262-EXTENDED "TO BE" ORGANIZATION

AIDA for Agile Development Process

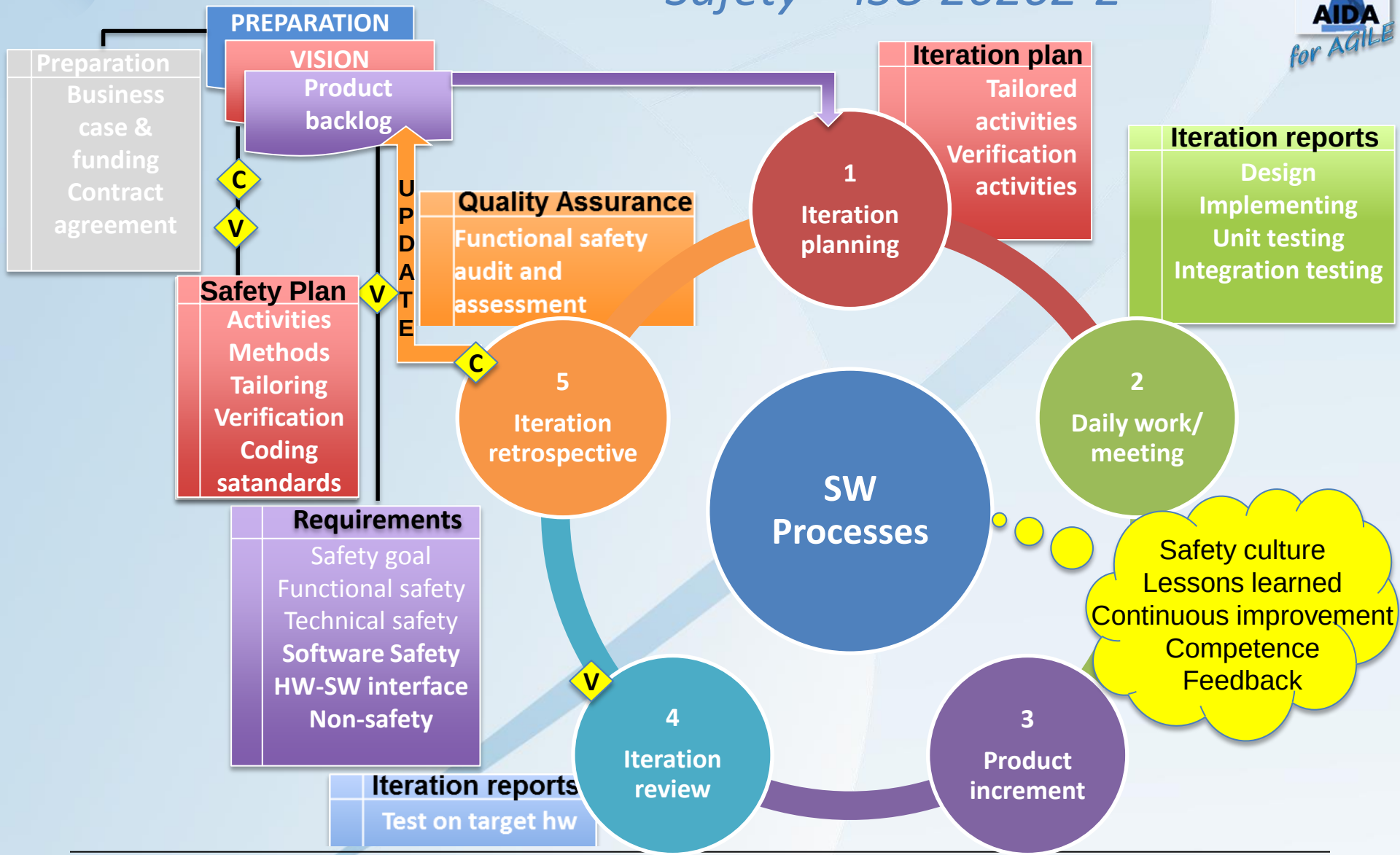
Preparation and closure Artifacts



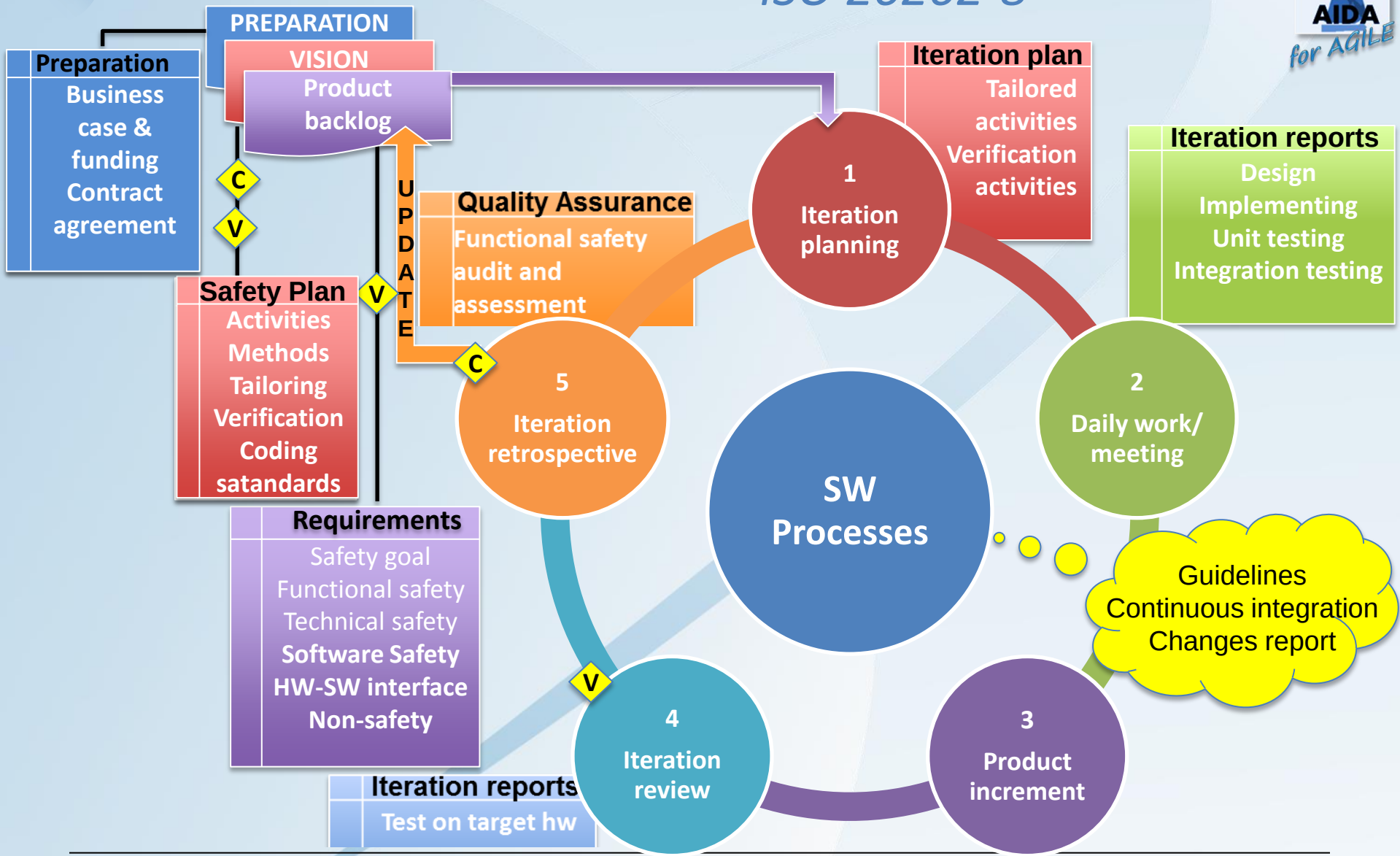
Developing safety Sofware with Scrum ISO 26262-6



Adding Management of Functional Safety – ISO 26262-2



Adding Supporting Processes ISO 26262-8



Safety Sofware Development
ISO 26262-6 versus Agile

ISO 26262-6 Clause	ISO 26262 Work products	Agile Artifact/Practice	When
5 - Initiation of product development at the software level	5.5.1 Safety plan (refined) 5.5.2 Software verification plan 5.5.3 Design and coding guidelines for modeling and programming languages 5.5.4 Tool application guidelines	**VISION** **ITERATION PLAN**	Iteration planning meeting
6 - Specification of software safety requirements	6.5.1 Software safety requirements specification 6.5.2 Hardware-software interface specification (refined) 6.5.3 Software verification plan (refined) 6.5.4 Software verification report	**PRODUCT BACKLOG**	Daily work Daily meetings
7 - Software architectural design	7.5.1 Software architectural design specification 7.5.2 Safety plan (refined) 7.5.3 Software safety requirements specification (refined) 7.5.4 Safety analysis report 7.5.5 Dependent failures analysis report 7.5.6 Software verification report (refined)	**METAPHORS**	Daily work Daily meetings
8 - Software unit design and implementation	8.5.1 Software unit design specification 8.5.2 Software unit implementation 8.5.3 Software verification report (refined)	**CODING**	Daily work Daily meetings
9 - Software unit testing	9.5.1 Software verification plan (refined) 9.5.2 Software verification specification 9.5.3 Software verification report (refined)	**ITERATION REVIEW REPORT**	Daily work Daily meetings

AIDA Model

www.aidamodel.org

MEDDEV AUTOMOTIVE LASTAMPA.it Info Toro Google Tube Sky Go OPENCOSS Tale Home - Fondazione ... noma Sito LabVIEW LabVIEW Community LabV

Search this site

AIDA Model

- Home
- AIDA Model
  - Integrated Assessment Model
  - Integrated Reference Model
  - Self-Assessment Toolkit
- Publications
- News & Events
- About Us
- Gallery
- Contact Us
- Skytechnology

Blog

SAFER WITH ISO 26262

Within the increasing complexity trend in electric and electronic (E/E) systems embedded in vehicles, associated with customers demand for efficiency, comfort and safety, are implicit many product liability issues. The ability to prove that delivered products are safe and reliable has become mandatory for manufacturers and suppliers. ISO 26262 is the **state-of-the-art standard** for functional safety in the automotive field.

INTEGRATION AND REUSE

The Assistant for Integrated Development and Assessment (AIDA) is a model that **integrates ISO 26262** and the requirements of a given de-facto standard(**Automotive SPICE®, CMMI or Lean Development**) supported by a safety extension process framework (**ISO/IEC 15504-10 or +Safe**).

AIDA MODEL WILL DRIVE THE CHANGE

News

We are improving AIDA model! *AIDA team is working to improve AIDA model by updating its current version (AIDA for Automotive SPICE) and by soon releasing two new versions: AIDA for Agile and AIDA for ...*
Posted Feb 13, 2013, 2:51 AM by Maria Antonieta Garcia

AIDA Model has been released!
Aida Model version 1.1 has been released. To get a free copy, please fill the form in the Contact Us page.
Posted Nov 22, 2012, 6:13 AM by Maria Antonieta Garcia

Showing posts 1 - 2 of 2. View more »

ernesto.viale@sky-team.it
Consulting B.U. Manager.