Introduzione della ISO26262 in un progetto di veicolo ibrido

Outline

- Il contesto
  - Azienda
  - Prodotto
- Introduzione 26262
- Tool
- Conclusioni

Actua Torino

Actua

- Prototyping
- Electric and hybrid powertrain
- Drive by wire solutions
- Transaxle, differential electrical axle, motor in wheel

- A Polito spin off
  - 10 persone

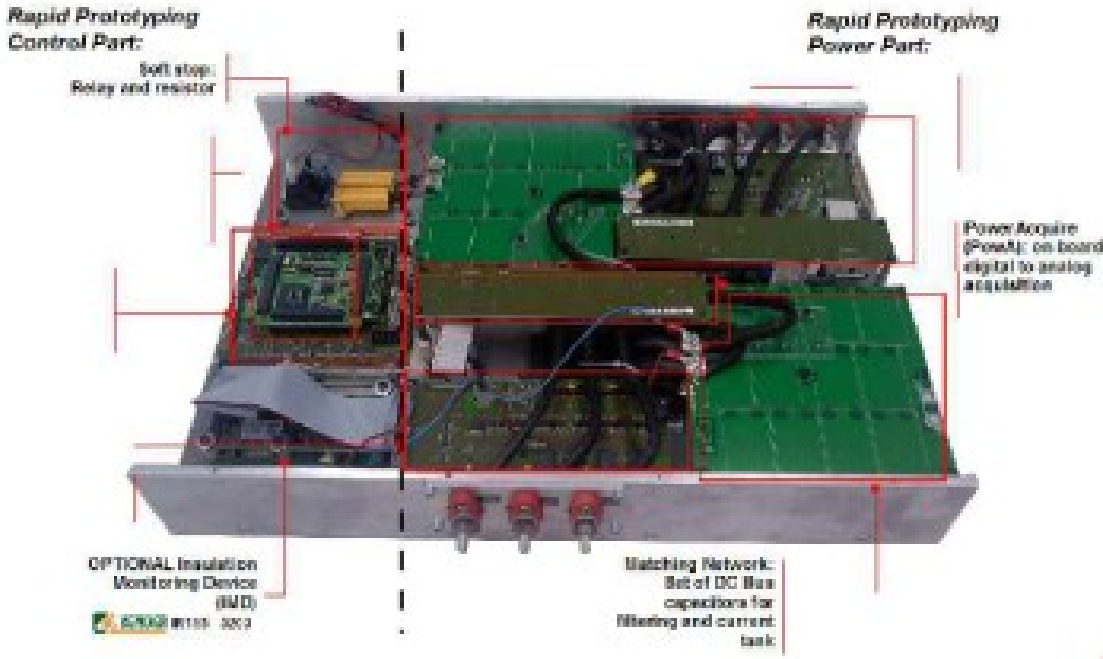
Il contesto: azienda

- Prototipi a vari livelli
  - Non necessitano compliance a standard o norma
- Customer ingegnerizza in prodotto
  - Necessitano compliance a standard

- Strategia aziendale:
  - Prototipi ‘ready to compliance’
  - Tipicamente ASIL B

Il contesto: prodotto

- Automotive actuation control unit
- Unità di controllo per hybrid/elecric powertrains, dual drive
  - Fino a 380V, 600A



Actuation control unit

- 26262 ready in particolare per architettura hw e livelli software intermedi

Introduzione 26262

- Analisi di processo, organizzazione, documenti
  - Word, excel
  - Disegni tecnici
  - Test e piani di test
  - Subversion
- Reengineering
  - Training personale
  - Modifiche organizzative: 26262 owner
  - Modifiche di processo e documentazione

Problematiche

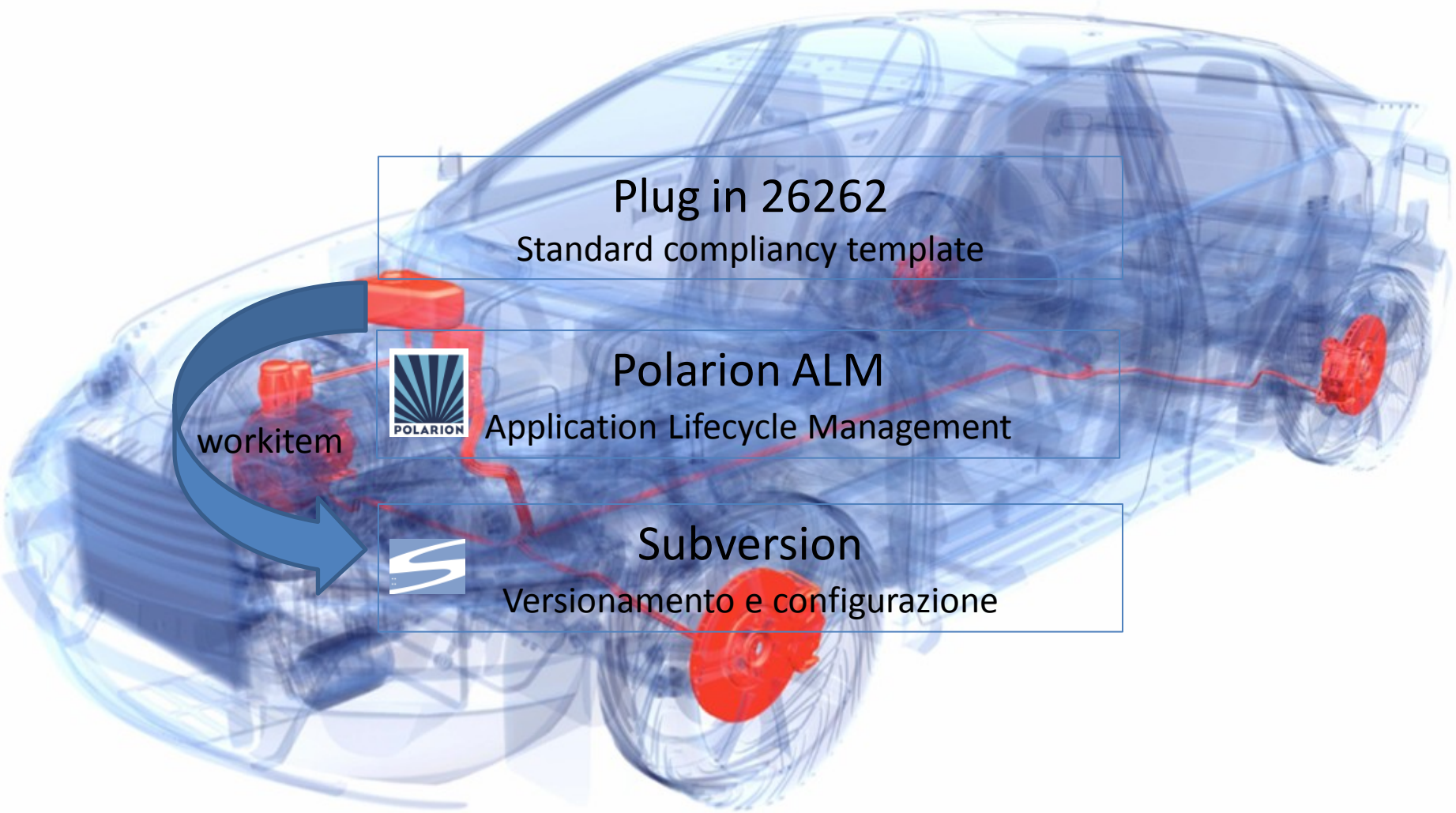
- 26262 è pesante, in particolare in PMI
  - Numero di documenti
  - Dipendenze tra documenti
- 26262 globale
  - Impatta ogni attività e documento

- Necessità di tool di supporto
  - Flessibile
  - Integrabile con tool e documenti attuali

Scelta Polarion

- NOT one more information silos
  - Integrabile e non invasivo
- Integrato con Subversion
- Supporto al processo già in essere
  - Requisiti, normative, rischi
  - Task, test, issue tracking
- Configurabile
- Import export di documenti con Microsoft Office e XML
- Tracciabilità
- Reporting
- Wiki Pages per navigare e descrivere

Tool - concept



Welcome page

Documents

Item definition template
Hazard analysis and risk assestment template
Safety goals template
Functional safety concept template
Verification review report report of the hazard analysis
Verification report of the functional safety concept

Working Tables

Operational Situation Table
Hazard Table
Hazardous Event Table
Safety Goal Table
Safety Requirements Table
Link Hazardous Event
Link Safety Goal
Link Safety Requirement

Standard Documentation

ISO 26262 Overview
How to

Dashboard

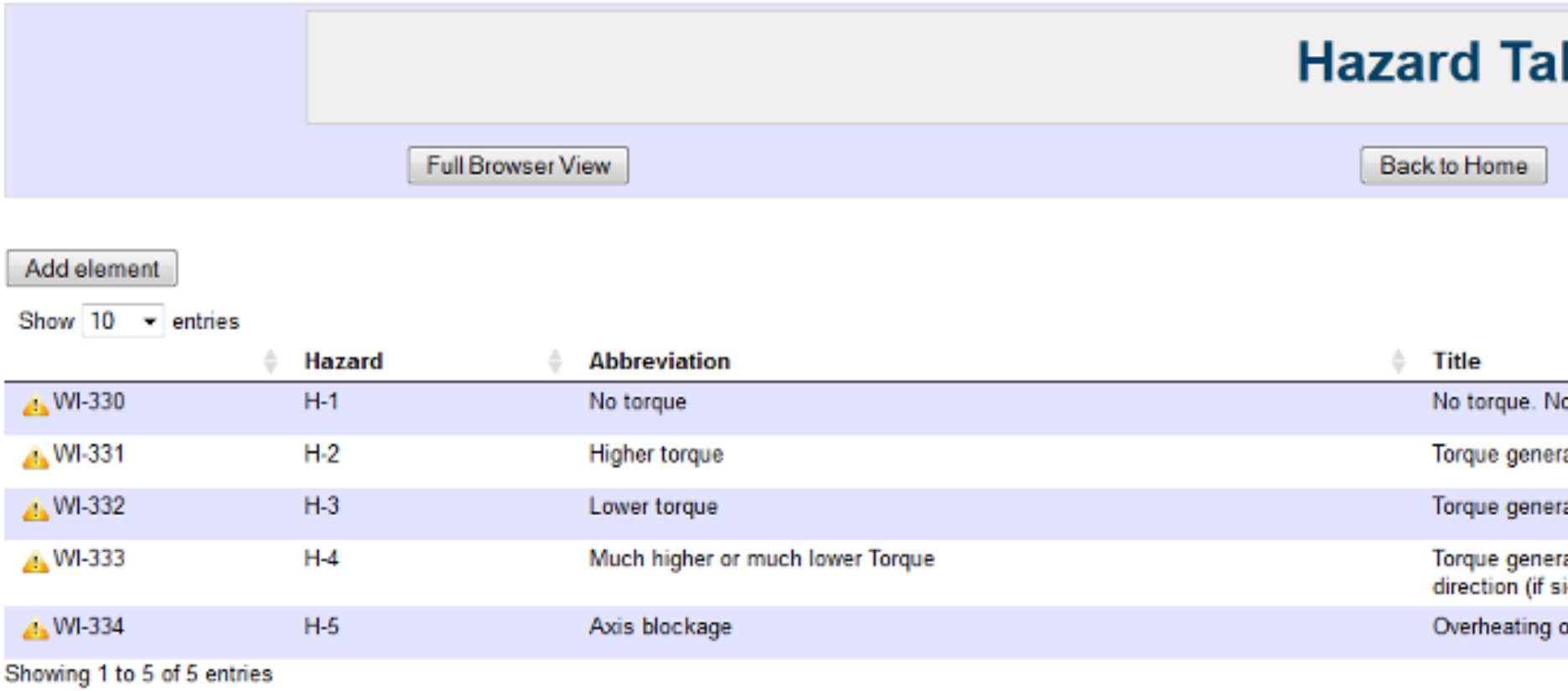
Coverage Analysis

26262 Part 3 nel tool

- Work Item
  - Hazard
  - Operational situation
  - Hazardous event
  - Safety goal

- Tracciabilità e coverage
- Automazione clerical task
  - Tabella Hazardous events come OSxHazard
  - Coverage SG e HE

Hazard table



Hazard Tal

Full Browser View

Back to Home

Add element

Show 10 entries

	Hazard	Abbreviation	Title
WI-330	H-1	No torque	No torque. No
WI-331	H-2	Higher torque	Torque genera
WI-332	H-3	Lower torque	Torque genera
WI-333	H-4	Much higher or much lower Torque	Torque genera direction (if si
WI-334	H-5	Axis blockage	Overheating o

Showing 1 to 5 of 5 entries

Hazardous event table

Hazardous Event Table

Full Browser View | Back to Home

lement | Create link

10 entries

Hazardous	Title	Related H	Related OS	Consequences	Exposure	Severity	Controllability
HE-1	Axis blockage	H-5 - Axis blockage WI-334	OS-1 WI-338 - On parking situation	Overheating of motor. The electric motor can block the rotation of the axle. this can generate loss of friction to the road and instability of the vehicle	E2	S2	C3
HE-2	Axis blockage	H-5 - Axis blockage WI-334	OS-2 WI-339 - On urban road		E2		
HE-4	Axis blockage	H-5 - Axis blockage WI-334	OS-4 WI-341 - On overtaking		E2		

g 1 to 3 of 3 entries (filtered from 10 total entries)

Verification review report example

Coverage Situations

Operational Situation - Coverage

There are **0 Operational Situation** without Hazardous Event.

Operational Situation with H

ID	Title
OS-1	On parking situa
OS-2	On urban road
OS-3	On non urban ro
OS-4	On overtaking
OS-5	On turning
OS-6	On uphill
OS-7	On Downhill

7 iten

Hazard - Coverage

There are **4 Hazard** without Hazardous Event.

Hazard without Hazardou

ID	Title
H-1	No torque. No torque will be ge only with mechanical brake
H-2	Torque generated by the electri greater than expected
H-3	Torque generated by the electri lower than expected
H-4	Torque generated much higher possiblewheels blockage or hig wrong).

Hazard with Hazardous E

ID	Title

Hazardous Event - Coverage

There are **3 Hazardous Event** without Safety Goal.

Hazardous Event without Safety Goal

ID	Title
HE-8	Prova HE senza safety goal assegnati
HE-999	prova asil
HE-888	xxxxxxx

3 items found

Hazardous Event with Safety Goal

ID	Title
HE-1	Axis blockage

Conclusione

- Training
- Applicata 26262 in full a primo prototipo
- Ingegnerizzazione e compliance da parte del customer in 2013
- Tool per part 3

Conclusione

- 26262 possibile anche in PMI
  - Facilitato da aspetto *ready to*
- In PMI ancora piu fondamentale efficienza – senza tool non pensabile
- Plug in 26262 (e 25119 in prospettiva) disponibile
  - Parte 3
  - Parte 4,5,6