

AF3 Phoenix - Change Request #2873

Safety level information is a complete mess

03/09/2017 11:35 AM - Anonymous

Status:	New	Start date:	03/09/2017
Priority:	Normal	Due date:	
Assignee:	Florian Hölzl	% Done:	0%
Category:	Hackathon	Estimated time:	0.00 hour
Target version:	Backlog		

Description

Safety levels ("DO178C-Level A/B/C/D/E, ISO26262 1/2/3/4") are implemented twice:

- once in mira (model element "SafetyLevel") which is used in scheduling but is actually not even editable by the user at the moment...
- once in the safety plugin (model element "SafetyIntegrityLevel") which is the only one really editable by the user

Question is: do we need both? Why are there even two implementations?

Gut feeling: we can remove the one in mira completely and just remove the dependency on it in scheduling (I guess it's in practice not used since the property is not even definable through the UI...).

We could then use only the one in safety.

This one could also be improved in the future, as a second iteration:

- the metamodel allows in the same class SIL and DAL levels...
- the implementation is a little bit too annotation-oriented in my opinion. Meaning a developer discovering this package spontaneously thinks that it's an "only-annotation" thing, but it can be used anywhere.

History

#1 - 03/09/2017 11:36 AM - Anonymous

@Flo: I assign to you so that we discuss it in the JF

#2 - 03/09/2017 11:45 AM - Simon Barner

Some comments:

- If I remember correctly, the MIRA model element SafetyLevel was supposed to be removed after the introduction of org.fortiss.af3.safety. See [#2171](#) and its sub-issues.
- However, there is / was a link from MIRA to the org.fortiss.af3.safety SIL annotation.
- Being able to defined safety levels based on the terms defined in different domain-specific standards was a required at the time the annotation has been introduced. Switching between the standards is currently implemented in a sub-optimal fashion (annotation of the top-level component)

#3 - 03/09/2017 11:51 AM - Anonymous

- Ok. From my own searches, it's not used anymore except by the scheduling plugin. But as I said I suspect it's useless now. Who's in charge of scheduling?
- Regarding a possible usage in the safety plugin, I didn't see any, but I might have overlooked (I'm in a meeting right now so my observation skills might be a little be low, sorry if so...)
- Mmh. This is however also allowed by the mira implementation. I must say at the moment, when looking at both models, it just really looks redundant, with slightly different implementations of the model.

#4 - 03/09/2017 01:12 PM - Simon Barner

Regarding scheduling: The mira SafetyLevel was supposed to be replaced by the one in org.fortiss.af3.safety, and it might be that the remaining occurrences of SafetyLevel can be removed without any further refactoring. Sergey or Johannes shown know the code.

#5 - 03/09/2017 01:26 PM - Anonymous

Ok I add both of them as watchers then

#6 - 03/01/2018 01:59 PM - Florian Hölzl

- Category set to Hackathon

- Target version changed from AF3 2.11 Post-release to AF3 2.13 RC1 (Feature Freeze)

I will bring this up in hackathon.

#7 - 04/23/2018 10:23 AM - Florian Hölzl

- Target version changed from AF3 2.13 RC1 (Feature Freeze) to AF3 2.14 RC1 (Feature Freeze)

#8 - 05/13/2019 02:08 PM - Johannes Eder

- Target version changed from AF3 2.14 RC1 (Feature Freeze) to Backlog