Model-Based Software Design

Results of the Lab 1

MATRICOLA	**LAB 1**					
	Item boundaries (15%)	Estimation matrix (50%)	ASIL (10%)	Safety goals (25%)	**TOTALE**	
289336					***0***	
258729	1	1	1	0,8	**31**	FTTI is not motivated. SG shall be defined in the sake of the item functionality, hence SG1 is not well defined.
289819					***0***	
286850					**0**	
262808					**0**	
240508					**0**	
259408					**0**	
236937	1	1	1	0,8	**31**	FTTI is not motivated
260043	1	0,7	0	0,8	**23**	Controllabilty is overestimated (C2 instead of C1); FTTI is not motivated; The SG shall be defined more precisely in the scope of the item functionality. Ch is safer with respect to Cl.
229445					**0**	
247657	1	0,8	1	0,8	**28**	The Exposure for the evasive manouver is E2. The SG1 shall be defined in terms of a wrong damping coefficient. FTTI is not motivated
260525	1	1	0,5	1	**31**	Some risk parameters are wrongly determined
261432					**0**	
263073					**0**	
260585					**0**	
247757	1	1	1	1	**33**	
246883					**0**	
256855	1	1	1	0,8	**31**	FTTI is not motivated
227500	1	1	1	0,8	**31**	FTTI is not motivated. It is better to directly reach the safe state in a case of a malfunction detection, instead of just allerting the driver expecting an action from he/she.
247447	1	0,7	0	0,8	**23**	Controllabilty is overestimated (C2 instead of C1); FTTI is not motivated; The SG shall be defined more precisely in the scope of the item functionality. Ch is safer with respect to Cl.
263726	0	0,25	0,25	0,8	**12**	The part regarding the item defnitio has not been filled. The ASIL level obtained is too high. The FFTI is not motivated
228969	1	0,8	1	0,5	**26**	Controllabilty is overestimated (C2 instead of C1); FTTI is not motivated; The SG shall be defined more precisely in the scope of the item functionality
257492	1	1	1	0,8	**31**	FTTI is not motivated. It is better to directly reach the safe state in a case of a malfunction detection, instead of just allerting the driver expecting an action from he/she.
250576	1	0,8	0,75	0,8	**27**	The item is safety relevant, so ASIL A. The wors case is S9 S3 E2 and C2 that is ASIL A also in the matrix. FTTI is not motivated
257278					**0**	
263191					**0**	
245206					**0**	
248919	1	1	1	0,8	**31**	FTT is not motivated
304321	0,8	0,5	0	0,5	**16**	No EXT measures; Errors in evaluation of controllability and exposure; wrong definition of SG but table compiled
302968	1	0,5	0,5	0,5	**19**	Risk parameters are wrongly computed; the safety goal refers to a safe state, not properly defined
295829					**0**	
292690					**0**	
290870	1	0	0	0	**5**	The report is incomplete, the ASIL level B is not justified in terms of risk parameters, but only with textual description without formal associations with levels
302192	1	0,8	1	1	**30**	Some puntual errors in severity and controllability in the risk parameters, that are otherwise well motivated. Only SG2 is assessed for this mark
291788	1	1	1	1	**33**	
302215	1	0,75	0,5	0,5	**23**	Controllability is overestimaded (i.e., C2 instead of C1). The SG is well defined. Please note that the FTTI is unique for each SG, since it is the time in which the failure has to be detected and mitigated (so it cannot depends on the situation, but shall be defined at concept time)
304171	1	0,5	0,5	0,5	**19**	Risk parameters are wrongly computed; the safety goal refers to a safe state, not properly defined; the report reports wrong results but it is complete
288903	1	1	1	0,8	**31**	No FTTI is provided

304178	1	0,8	1	1	**30**	Some risk parameters are wrongly computed; FTTI has to be evaluated in terms of impact on drivability (a time sufficiently small to not allow the hazard to harm people)
289832	0,8	0,8	0	0,25	**19**	The ASIL classification obtained is to high definition of the safety goal is wrong
302869	1	0,8	0,5	0,8	**26**	Some risk parameters are wrongly determined Not defined the safe damping factor
288485	1	1	1	1	**33**	
302410	1	1	1	1	**33**	Its better to define as a safe state a fixed damping, but anyway warning the driver is acceptable for such an item
304572	1	0,8	0,5	1	**28**	Some risk parameters are wrongly determined
287462	1	1	1	0,75	**31**	The safe state of SG2 is to force the damping factor to Ch
299300	1	1	1	0,8	**31**	FTTI is not motivated
289798	0,8	1	0,5	1	**30**	No external measures
304373	1	0,5	0,5	0,8	**21**	The risk parameters for F2 are not correct, considering controllability and exposure for the evasive manouver. The ASIL is wrong (D), but the safety goal is well defined. FTTI is not motivated
299582					**0**	
287871	1	0,5	1	0,5	**21**	The controllability is overestimated, the severity is underestimated, and the exposures are E4 and E2 (for the evasive manouver). The ASILs are right, but these values shall be obtained with higher severity and better controllability (C1 and C0). The danping values can be only ch or cl, no intermediate values are possible. The SG is in term of a goal to guarantee the functional safety when the item is operating, not at design time.
243244					**0**	
303498	1	0,8	0,75	0,75	**27**	Some risk parameters are not correct. The SG definition "In case the item is not able to report obstacles it shall transit to the safe state" is not clear. FTTI is not motivated
288756	1	1	1	0,75	**31**	FTTI is not motivated
301881	1	1	1	0,75	**31**	FTTI is not motivated. Attention: the only two damping coefficient are ch and cl: intermediate values are not possible
278073	1	1	1	0,75	**31**	FTTI is not motivated
285913	1	0,75	1	0,75	**27**	FTTI is not motivated
274301					**0**	
304358	0,8	0,5	1	0,75	**22**	No external measures, Severity is underestimadet while controllability is overestimated (i.e., C2 instead of C1)
303007	1	0,9	1	0,75	**29**	Damping factor fixed to Cl is more dangerous with respect to ch; FTTI is not motivated
304235	1	0,75	0,5	0,75	**25**	Risk parameters are wrongly determined (controllability is overestimated); hence ASIL is too high; SG shall be defined in terms of the functionality of the item, hence guarantee handling of the car is too general
289588	1	0,75	0,5	0,5	**23**	Controllability is overestimaded (i.e., C2 instead of C1). The SG is well defined. Please note that the FTTI is unique for each SG, since it is the time in which the failure has to be detected and mitigated (so it cannot depends on the situation, but shall be defined at concept time)
302217	1	1	1	0,8	**31**	FTTI is not motivated
295635	1	0,5	1	0,5	**21**	The controllability is overestimated, the severity is underestimated, and the exposures are E4 and E2 (for the evasive manouver). The ASILs are right, but these values shall be obtained with higher severity and better controllability (C1 and C0). The danping values can be only ch or cl, no intermediate values are possible. The SG is in term of a goal to guarantee the functional safety when the item is operating, not at design time.
303559	1	0,5	1	0,5	**21**	FTTI is not motivated. The SG is a goal that, if violated, lead to exposing the people to the hazard, so it cannot be defined as the functionality of the item
296466	1	0,75	1	0,5	**25**	Controllabilty is overestimated (C2 instead of C1); FTTI is not motivated; The SG shall be defined more precisely in the scope of the item functionality
301202	1	0,8	1	0,75	**28**	Controllability is overestimaded (i.e., C2 instead of C1). FTTI is not motivated
302284	1	0,5	0,5	1	**23**	Severity is overestimate d, while controllabilty is underestimated. FTTI is not motivated.
292624	1	1	1	0,8	**31**	The system can only impose the damping factor equal to ch or cl: no intermediate values are possible.
301494	1	0,75	1	0,8	**27**	FTTI is not motivated
303637	1	0,8	1	0,8	**28**	Controllability is overestimaded (i.e., C2 instead of C1). FTTI is not motivated
303517	1	0,75	0,5	0,9	**26**	The Exposure for the evasive manouver is E2. The SG1 shall be defined in terms of a wrong damping coefficient

303215	1	0,75	1	0,8	**27**	Controllability is overestimanted. FTTI is not motivated
265260					**0**	
265145	0,8	1	1	0,8	**30**	No external measures, F2 is dangerous w.r.t. F1: it is better to define the safe state also imposing the damping to Ch
303593	1	0,75	0,5	0,9	**26**	The Exposure for the evasive manouver is E2. The SG1 shall be defined in terms of a wrong damping coefficient
302893	1	0,8	1	0,8	**28**	The controllability is overestimated. FTTI is not motivated. The damping coneffient can be only Ch or Cl
301330	1	0,5	0,5	0,8	**21**	FTTI is not motivated
287436	1	0,5	0	0,5	**17**	The SG shall be defined in the scope of the item funcionality; FTTI is not motivated
282598	1	0,8	1	0,8	**28**	The Exposure for the evasive manouver is E2. The SG1 shall be defined in terms of a wrong damping coefficient. FTTI is not motivated
303635	1	0,8	1	1	**30**	Controllabilty is overestimated (C3 instead of C1); FTTI motivated from the literature The SG shall be defined more precisely in the scope of the item functionality
295783					**0**	
302177	1	0,5	0,5	1	**23**	Severity is overestimate d, while controllabilty is underestimated. ASIL of F1 == F2; FTTI is not motivated.
301757	1	1	1	1	**33**	
302496					**0**	
287435	1	0,5	0	0,5	**17**	The SG shall be defined in the scope of the item funcionality; FTTI is not motivated
303669					**0**	
302148	1	1	1	0,8	**31**	The SG shall be defined in the scope of the item funcionality; FTTI is not motivated
299955	1	1	1	0,8	**31**	FTTI not motivated
303521					**0**	
296972	1	0,75	1	1	**29**	The controllability is overestimated. FTTI is not motivated.
280037	1	1	1	0,8	**31**	FTTI is not motivated
292706	1	1	1	0,8	**31**	FTTI is not motivated
279928	1	1	0,9	0,8	**31**	The SG is ASIL A, not QM: reading the report it is possible to see that it is just a typo; the FTTI is not motivated
300179	1	0,5	0	0,8	**20**	Risk parameters are wrongly computed; the safety goal refers to a safe state, not properly defined; FTTI is not motivated
298534	1	0,6	0,5	0,8	**23**	FTTI not motivated. Determined ASIL is to high
277538	1	1	1	1	**33**	
295281					**0**	
287639	0,8	1	1	0,8	**30**	No external measures; FTTI is not motivated
302407	1	1	1	0,8	**31**	FTTI is not motivated
296926	0,8	0,6	0,25	0,8	**21**	No external measures; Determined ASIL is to high (controlabilty is overestimated) FTTI is not motivated.
303913	1	1	1	0,8	**31**	FTTI is not motivated
303577	1	0,8	0,75	0,8	**27**	Some risk parameters are not correct. The SG definition "In case the item is not able to report obstacles it shall transit to the safe state" is not clear. FTTI is not motivated
290185	1	1	1	0,8	**31**	FTTI is not motivated
280666	1	1	1	0,8	**31**	FTTI is not motivated
280209	1	0,8	0,5	0,8	**26**	Some risk parameters are not correct. The SG definition "Revert the system to a safe state" is not completely defined. FTTI is not motivated
297788	1	1	1	0,9	**32**	The safety goal cannot be defined as the item functionality, but in terms of what shall not happen to not expose the user to an hazard, causing harms
292825	1	1	1	0,8	**31**	The SG shall be defined in the scope of the item funcionality; FTTI is not motivated
297276	1	1	1	1	**33**	
260291					**0**	
296390	1	1	1	1	**33**	
303922					**0**	
281684					**0**	
301379	1	0,8	1	0,8	**28**	FTTI is not motivated
289371					**0**	
303838	1	1	1	1	**33**	
289549	1	0,8	0,7	0,7	**26**	Some errors in the risk parameters, the ASIL is too high. FTTI is not motivated
302243	1	1	1	1	**33**	
292513					**0**	
303440	1	1	1	0,8	**31**	FTTI is not motivated
294224	1	0,7	0,5	0,7	**24**	The determined ASIL is too high. In the SG, the ASIL is reported as A, but the result from the risk assessment is B
296018	1	1	1	1	**33**	
301256	1	1	1	0,9	**32**	The safety goal cannot be defined as the item functionality, but in terms of what shall not happen to not expose the user to an hazard, causing harms

288086	1	1	1	0,8	**31**	FTTI is not motivated
304003	1	1	1	1	**33**	
296444	0,3	0,6	1	0,5	**19**	Concept phase incomplete. Some risk parameters are wrong. The safety goal has to be defined in terms of an action (alert the driver, disable itself) and not upon the driver. Moreover , it does not describe any useful action in the sake of the functionality of the item.
302415	1	1	1	1	**33**	Its better to define as a safe state a fixed damping, but anyway warning the driver is acceptable for such an item
303840	1	1	1	1	**33**	
302203	1	0,8	1	1	**30**	Some puntual errors in severity and controllability in the risk parameters, that are otherwise well motivated. Only SG2 is assessedù
290511	1	0,75	1	0,8	**27**	FTTI is not motivated
290807					**0**	
260770	1	0,75	1	0,8	**27**	FTTI is not motivated
274180					**0**	
301424	1	1	0,9	0,8	**31**	The SG is ASIL A, not QM: reading the report it is possible to see that it is just a typo; the FTTI is not motivated
295308	1	1	1	0,8	**31**	FTTI is not motivated
304915	1	0,8	0,5	0,7	**26**	The ASIL level is too high. FTTI is notmotivated. It is not completely clear the meaning of activate the passive suspension system: it it needed to define a fallback damping coefficient
290797	1	0,8	0,5	0,8	**26**	Some risk parameters are not correct. The SG definition "Revert the system to a safe state" is not completely defined. FTTI is not motivated
303562					**0**	
292752	1	0,75	1	0,8	**27**	The ASIL classification obtained is to high. The SG for a low ASIL system is usually a disabling of the functionality keeping hte system in a safe state (locking the damping to a fixed value ch). FTTI is not motivated
294427	1	0,7	0,5	0,7	**24**	The determined ASIL is too high. In the SG, the ASIL is reported as A, but the result from the risk assessment is B
275935					**0**	
281255	1	0,5	0,4	0,8	**21**	The controllability is overestimated, leading to an higher ASIL with respect to the expected one. "SHC must be disabled" is not completely defined. FTTI is not motivated
304368	1	0,7	0,5	1	**26**	The controllability is overestimated. The obtaine dASIL is too high
291018	0,8	1	1	0,8	**30**	No external measures; FTTI is not motivated
299497	1	1	1	0,8	**31**	FTTI is not motivated
279445	1	1	1	0,5	**29**	Reduce the speed is an action from the driver and not from the item.
289238					**0**	
274197	1	1	1	0,5	**29**	Reduce the speed is an action from the driver and not from the item.
288732	1	0,5	0,5	0,8	**21**	The ASIL classification obtained is to high. FTTI is not motivated
304173	1	0,5	0,5	0,8	**21**	The risk parameters for F2 are not correct, considering controllability and exposure for the evasive manouver. The ASIL is wrong (D), but the safety goal is well defined. FTTI is not motivated
296224	1	0,5	0,25	0,7	**20**	The controllability is overestimated. FTTI is not motivated.
303615	1	1	1	1	**33**	
290187	0,8	1	1	0,9	**31**	No external measures; There is a typo on the SG: in the table it is reported A, but then is reported B. I just assessed based on the content of the table (C2 is too high). SG texrtual description can be improved by bbetter explaining how to no expose the people to the hazards.
301191	1	1	1	0,8	**31**	FTTI not motivated
300797	1	0,75	1	0,8	**27**	FTTI is not motivated. SG shall be defined in the sake of the item functionality, hence SG1 is not well defined.
274181					**0**	
289606	1	0,8	0,5	0,7	**26**	Exposure of the evasive manouver is E2. FTTI is not motivated. The definition of the safety goals is not sufficiently precise
302509	0,8	1	1	0,8	**30**	No external measures. FTTI is not motivated. The safety goals shall be defined in terms of "prevent the item to.."
302246	1	1	1	1	**33**	
287354	1	1	1	0,8	**31**	FTTI is not motivated. It is not described which is the c value that is safe
296022	1	1	1	0,8	**31**	FTTI is not motivated
302270	1	1	1	1	**33**	
276272	1	0,5	0,25	0,2	**16**	The ASIL classification obtained is to high. The SG are defined, but not analyzed

303867	1	1	1	0,8	**31**	FTTI is not motivated
301840	1	1	1	0,75	**31**	The safe state of SG2 is to force the damping factor to Ch
301107	1	1	1	1	**33**	
292445	1	0,5	0,5	0,8	**21**	FTTI is not motivated
293648	1	1	1	1	**33**	
301039	1	1	1	0,8	**31**	FTTI is not motivated
302896	1	1	1	0,8	**31**	FTTI is not motivated
303627	1	0,75	1	0,75	**27**	FTTI is not motivated. Attention: the only two damping coefficient are ch and cl: intermediate values are not possible
303935	0,8	1	1	0,8	**30**	No external measures. FTTI is not motivated. The safety goals shall be defined in terms of "prevent the item to.."
278898	0,8	0,75	0,75	0,8	**25**	No external measures. The determined ASIL is too high. FTTI is not motivated
293655	1	0,75	0,75	1	**28**	The obtained ASIL is to high (controllability has been overestimanted). FTTI is not motivated
269079	1	0,8	0,7	0,7	**26**	Some errors in the risk parameters, the ASIL is too high. FTTI is not motivated
304502	1	0,7	0,5	1	**26**	The controllability is overestimated. The obtaine dASIL is too high
295298	1	0,9	1	0,75	**29**	Damping factor fixed to Cl is more dangerous with respect to ch; FTTI is not motivated
304976	1	1	1	0,8	**31**	FTTI is not motivated
304798	1	0,8	1	0,75	**28**	Controllability is overestimaded (i.e., C2 instead of C1). FTTI is not motivated
289420					**0**	
290555	1	1	1	0,8	**31**	No FTTI is provided
293550	1	0,75	0,75	0,8	**26**	The ASIL level is to high. No FTTI is provided
303316	1	1	1	0,8	**31**	FTTI is not motivated
288838	1	1	1	1	**33**	
290554					**0**	
297960	0,8	0,75	0,75	0,6	**24**	No external measures; FTTI is not motivated. The controllability is overestimated. The SG are conditions to avoid to expose people to the hazard, so they cannot be defined as the item functionality
296232	1	1	1	0,8	**31**	FTT is not motivated
303262	1	1	1	1	**33**	
302085	1	1	1	0,8	**31**	FTTI is not motivated
287973	1	0,8	0,75	1	**29**	The ASIL classification obtained is to high
294052	1	0,75	0,5	0,75	**25**	Risk parameters are wrongly determined (controllability is overestimated); hence ASIL is too high; SG shall be defined in terms of the functionality of the item, hence guarantee handling of the car is too general
292620					**0**	
295339	1	1	1	0,8	**31**	FTTI is not motivated
300264	1	1	1	0,8	**31**	FTTI is not motivated
305213	1	0,5	0,5	0,8	**21**	The obtained ASIL is to high. FTTI is not motivated
304097	1	1	1	1	**33**	
301033	1	1	1	0,8	**31**	FTTI is not motivated
291961	1	1	1	0,8	**31**	FTTI is not motivated
304928					**0**	
296266	1	0,8	1	0,8	**28**	Controllability is overestimaded (i.e., C2 instead of C1). FTTI is not motivated
290362	1	1	1	0,8	**31**	FTTI is not motivated
290632	1	1	1	0,8	**31**	FTT is not motivated
282858	1	1	1	0,8	**31**	FTTI is not motivated
290020	1	0,75	0,75	1	**28**	The obtained ASIL is to high (controllability has been overestimanted). FTTI is not motivated
305301	0,8	0,6	0,5	0,8	**22**	No external measures. The ASIL obtained is to high (the controllability is overestimated). FTTI is not motivated.
281804	1	0,75	1	0,8	**27**	The ASIL classification obtained is to high. The SG for a low ASIL system is usually a disabling of the functionality keeping hte system in a safe state (locking the damping to a fixed value ch). FTTI is not motivated
290169	1	1	1	0,8	**31**	FTTI is not motivated
279105					**0**	
294596	1	0,75	0,75	1	**28**	The ASIL classification obtained is to high
304263	1	0,5	0,5	0,7	**21**	The ASIL classification obtained is to high. FTTI is not motivated. The SG definition is not clear, in particular the "retro alimentation"
303895					**0**	
292453	1	1	1	0,8	**31**	FTTI not motivated
291532	0,8	1	1	0,9	**31**	No external measures; There is a typo on the SG: in the table it is reported A, but then is reported B. I just assessed based on the content of the table (C2 is too high). SG texrtual description can be improved by bbetter explaining how to no expose the people to the hazards.

300220	1	1	1	0,8	**31**	FTTI is not motivated
279730	1	0,8	0,75	1	**29**	The ASIL classification obtained is to high
289894	0,8	0,8	0	0,25	**19**	The ASIL classification obtained is to high,definition of the safety goal is wrong
295317	1	0,5	1	0,5	**21**	FTTI is not motivated. The SG is a goal that, if violated, lead to exposing the people to the hazard, so it cannot be defined as the functionality of the item
304826	1	0,8	1	0,8	**28**	The controllability is overestimated. FTTI is not motivated. The damping coneffient can be only Ch or Cl
304734	1	0,8	1	1	**30**	Some risk parameters are wrongly computed; FTTI has to be evaluated in terms of impact on drivability (a time sufficiently small to not allow the hazard to harm people)
292480	1	0,75	0,75	1	**28**	The ASIL classification obtained is to high
281772					**0**	
304052	1	1	1	0,8	**31**	FTTI is not motivated
289509	1	1	1	0,8	**31**	FTTI is not motivated
297278	1	1	1	0,8	**31**	FTTI is not motivated
302109	1	1	1	1	**33**	
302565	1	1	1	0,8	**31**	FTTI is not motivated
252890					**0**	
291079	1	1	0,8	0,8	**31**	The considered ASIL in the icy condition is to high: the controllability is little worsened with respect to the same condition without the malfunction.
301100	1	1	1	0,8	**31**	FTTI is not motivated
303394	1	1	1	0,8	**31**	FTTI is not motivated
280004	1	1	1	0,8	**31**	FTT is not motivated
290090	1	1	1	1	**33**	
305577	0,8	0,75	0,75	0,8	**25**	No external measures. The determined ASIL is too high. FTTI is not motivated
286245	1	1	1	0,8	**31**	FTTI is not motivated
300832					**0**	
296445	1	0,75	1	1	**29**	The controllability is overestimated. FTTI is not motivated.
305208	1	1	1	0,8	**31**	FTTI is not motivated
287350	1	1	1	0,8	**31**	FTTI is not motivated. It is not described which is the c value that is safe
303624	1	1	1	0,8	**31**	FTTI is not motivated
292759	1	1	1	0,8	**31**	FTTI is not motivated
294978	1	1	1	0,8	**31**	FTTI is not motivated
296392	1	1	1	1	**33**	
291761	1	0,8	1	0,8	**28**	Controllability is overestimaded (i.e., C3 and C2 instead of C1). FTTI is not motivated
292614	1	1	0,8	0,8	**31**	The considered ASIL in the icy condition is to high: the controllability is little worsened with respect to the same condition without the malfunction.
295409	1	1	1	1	**33**	
302159	1	1	1	1	**33**	
302269	1	0,5	0,25	0,2	**16**	The ASIL classification obtained is to high. The SG are defined, but not analyzed
288434	1	0,8	0,5	0,7	**26**	Exposure of the evasive manouver is E2. FTTI is not motivated. The definition of the safety goals is not sufficiently precise
301250	1	1	1	1	**33**	
302241	1	1	1	0,8	**31**	FTTI is not motivated
290129	1	1	1	0,8	**31**	FTTI is not motivated
300213	1	1	1	0,8	**31**	FTTI is not motivated
299284	1	0,9	1	0,8	**30**	F2 is worst w.r.t. F1. FTTI is not motivated
273733					**0**	
299724	1	0,5	0	0,8	**20**	Risk parameters are wrongly computed; the safety goal refers to a safe state, not properly defined; FTTI is not motivated
305838	1	0,8	0,5	0,75	**26**	Severity not assessed properly;No FTTI
305767	0,8	0,5	1	0,75	**22**	No external measures Severity is underestimadet while controllability is overestimated (i.e., C2 instead of C1)

For any question please write to jacopo.sini@polito.it