ACAS Adaptive Cruise Control System

Critical Systems Labs has prepared public demonstration safety case argument for a hypothetical adaptive cruise control (ACC) system. This safety case argument uses a dialectical approach known as “Eliminative Argumentation” (EA) [1]. EA involves the explicit representation and reasoning about potential doubts within the argument, in order to effectively eliminate or address them.

The argument contains 300 nodes in total, roughly following the Positive Trust Balance [2] approach to autonomous vehicle safety by arguing that the design, implementation, testing and monitoring of the ACC system are all done correctly.The ACC system discussed is modelled for use in a serial-production road vehicle, for highway use only (60-120 km/h), to have authority over both acceleration and braking, and to receive sensory information from a forward-facing radar unit.

This safety case is made publicly available for researchers in EA methodology and practitioners interested in applying safety case methods to complex systems. A representation of the argument has been automatically generated by Socrates and is displayed in the following pages. There is a video describing this safety case here: https://www.youtube.com/watch?v=ZH5LijuTfF4

[1] J. B. Goodenough, C. B. Weinstock and A. Z. Klein, "Eliminative Argumentation: A Basis for Arguing Confidence in System Properties," Carnegie Mellon University - Software Engineering Institute, Pittsburgh, United States, 2015.

[2] P. Koopman and M. Wagner, "Positive Trust Balance for Self-driving Car Deployment," in *SAFECOMP 2020*, 2020.

DEMO Adaptive Cruise Control - Redone

This file was generated by Socrates.

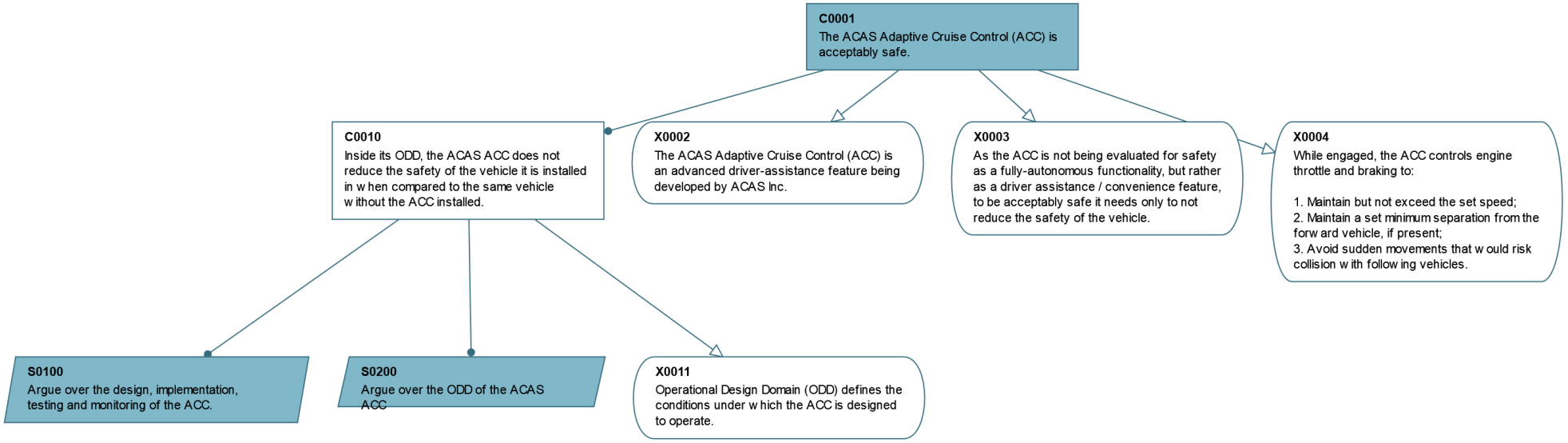
Argument Created: 2022-04-04T19:59:39.000+00:00

Last Modified: 2023-07-31T20:37:20.000+00:00

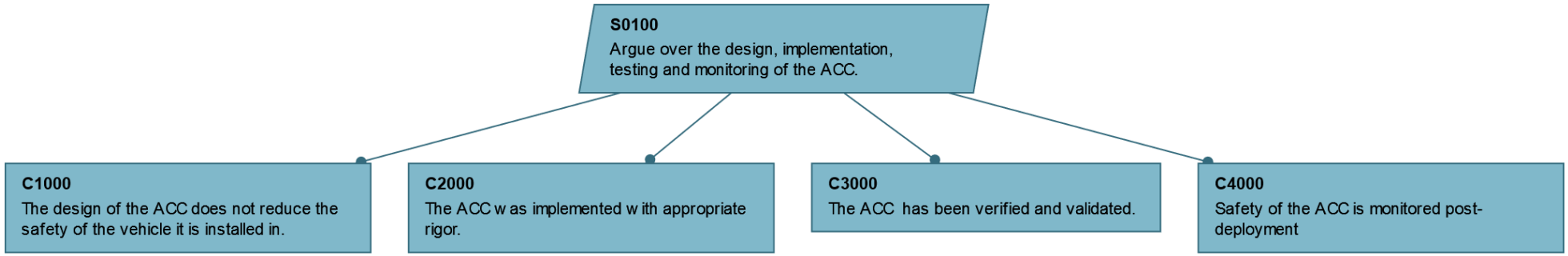
Owner: Critical Systems Labs

Argument

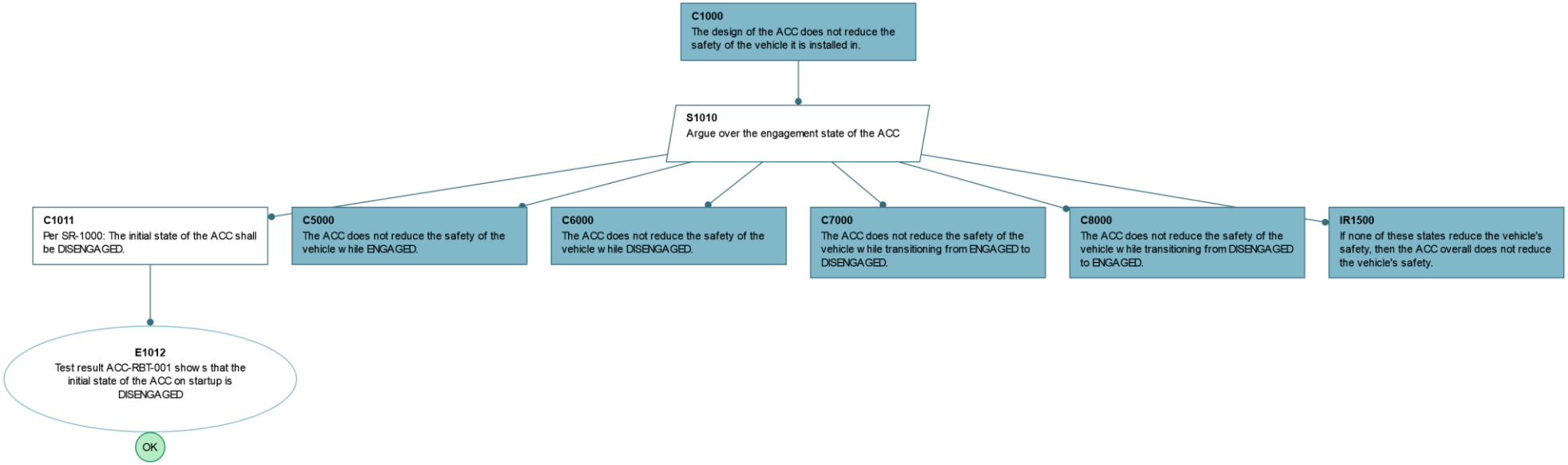
C0001 - The ACAS Adaptive Cruise Control (ACC) is acceptably safe.			
Parent subtree(s)	None	**Descendant subtree(s)**	S0100, S0200
Description	The ACAS Adaptive Cruise Control (ACC) is a COTS software-only product to provide speed control and following-distance control to road vehicles. This argument is structured around the claim that that ACC is not guaranteed to be available at all times, but when active, does not make the vehicle unsafe.		
Artifacts	None	**Glossary Terms**	None



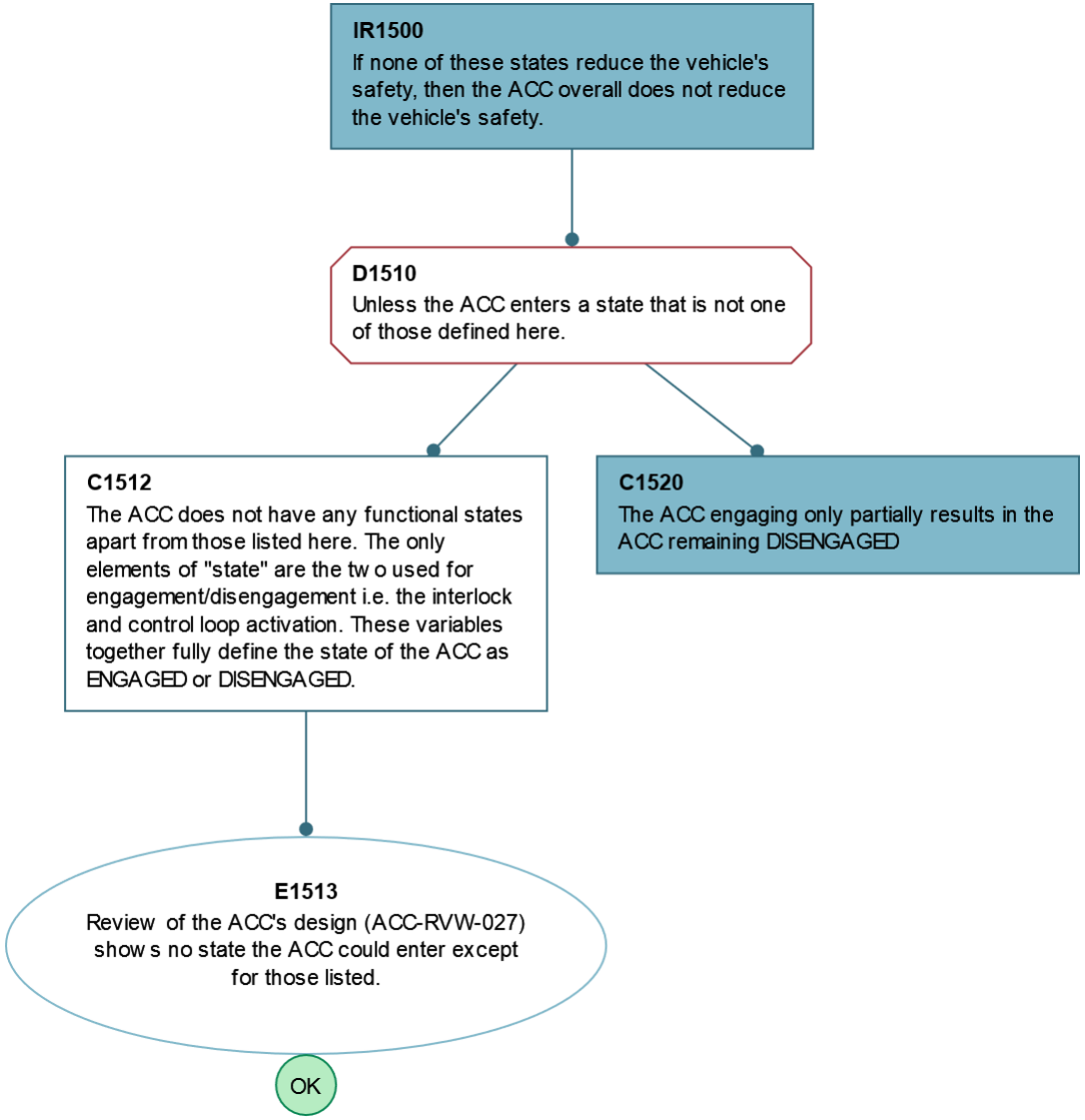
S0100 - Argue over the design, implementation, testing and monitoring of the ACC.			
Parent subtree(s)	C0001	**Descendant subtree(s)**	C1000, C2000, C3000, C4000
Description			
Artifacts	None	**Glossary Terms**	None



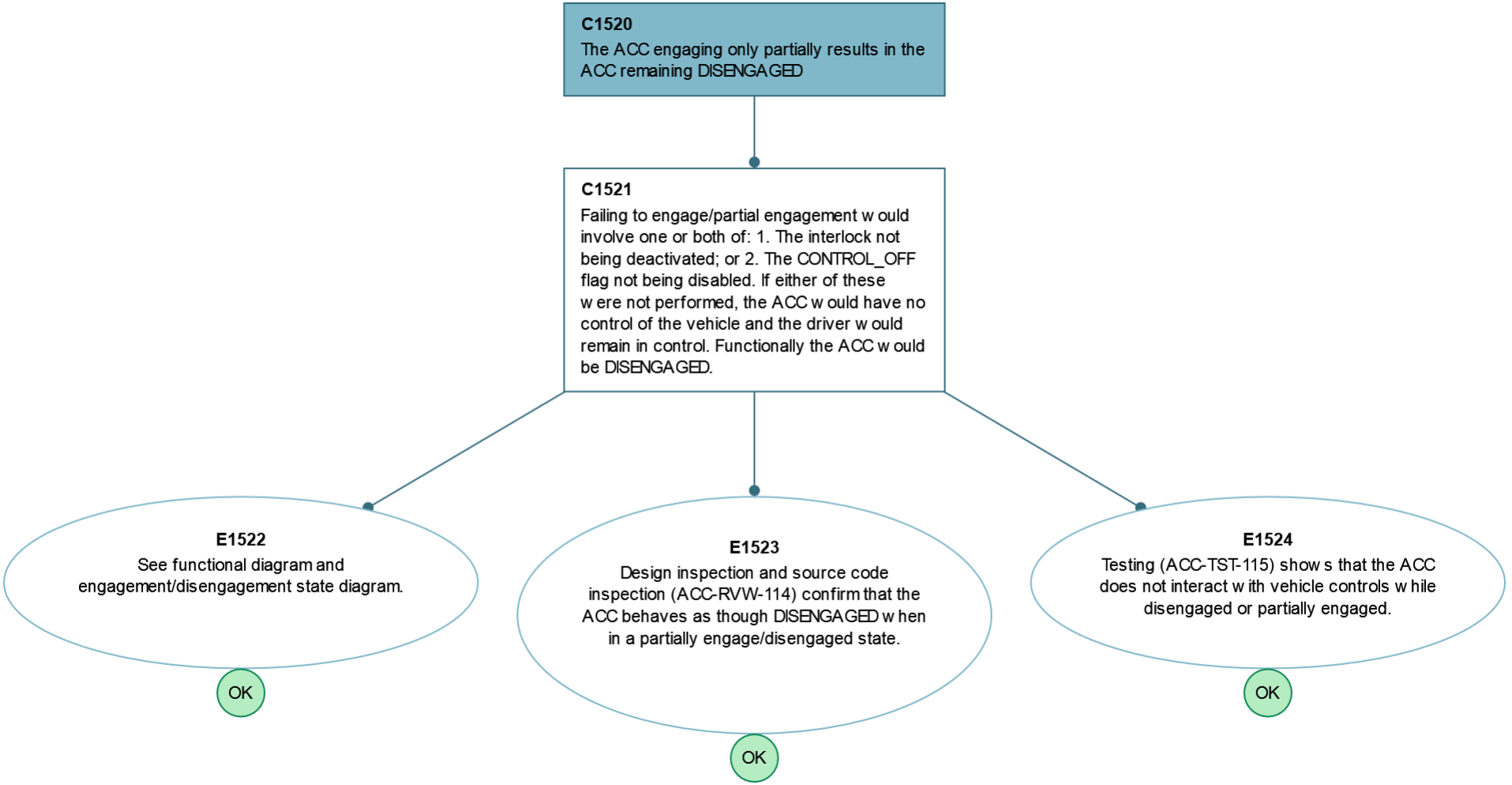
C1000 - The design of the ACC does not reduce the safety of the vehicle it is installed in.			
Parent subtree(s)	S0100	**Descendant subtree(s)**	IR1500, C5000, C6000, C7000, C8000
Description			
Artifacts	IR1500: Engagement-Disengagement State Diagram	**Glossary Terms**	None



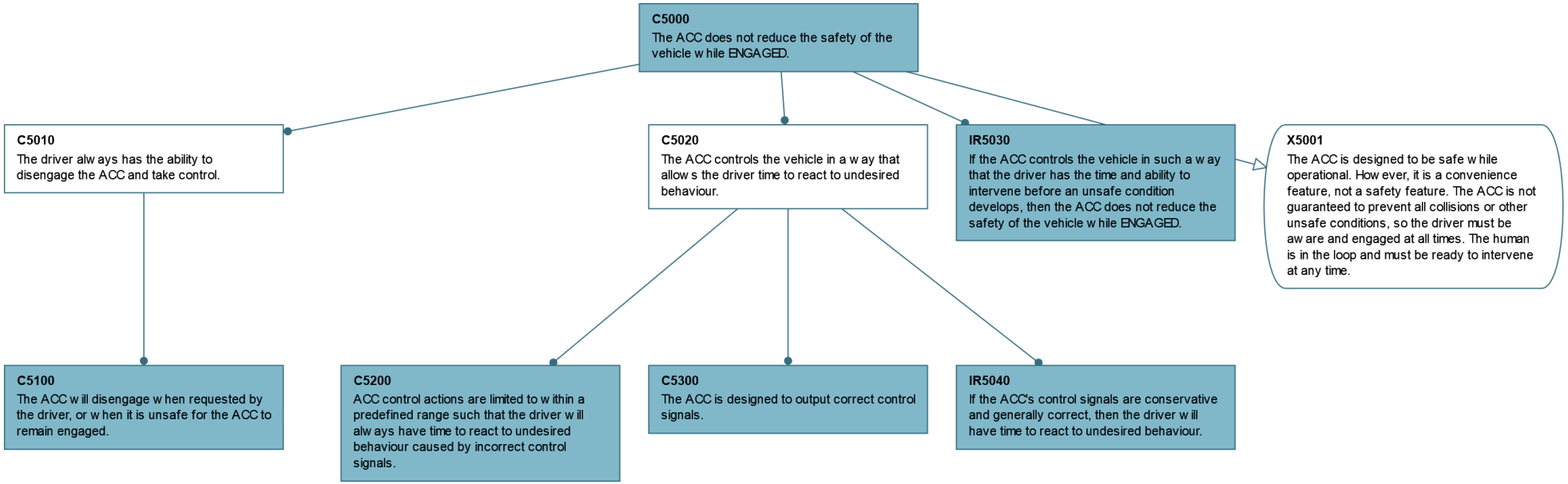
IR1500 - If none of these states reduce the vehicle's safety, then the ACC overall does not reduce the vehicle's safety.			
Parent subtree(s)	C1000	**Descendant subtree(s)**	C1520
Description			
Artifacts	IR1500: Engagement-Disengagement State Diagram	**Glossary Terms**	None



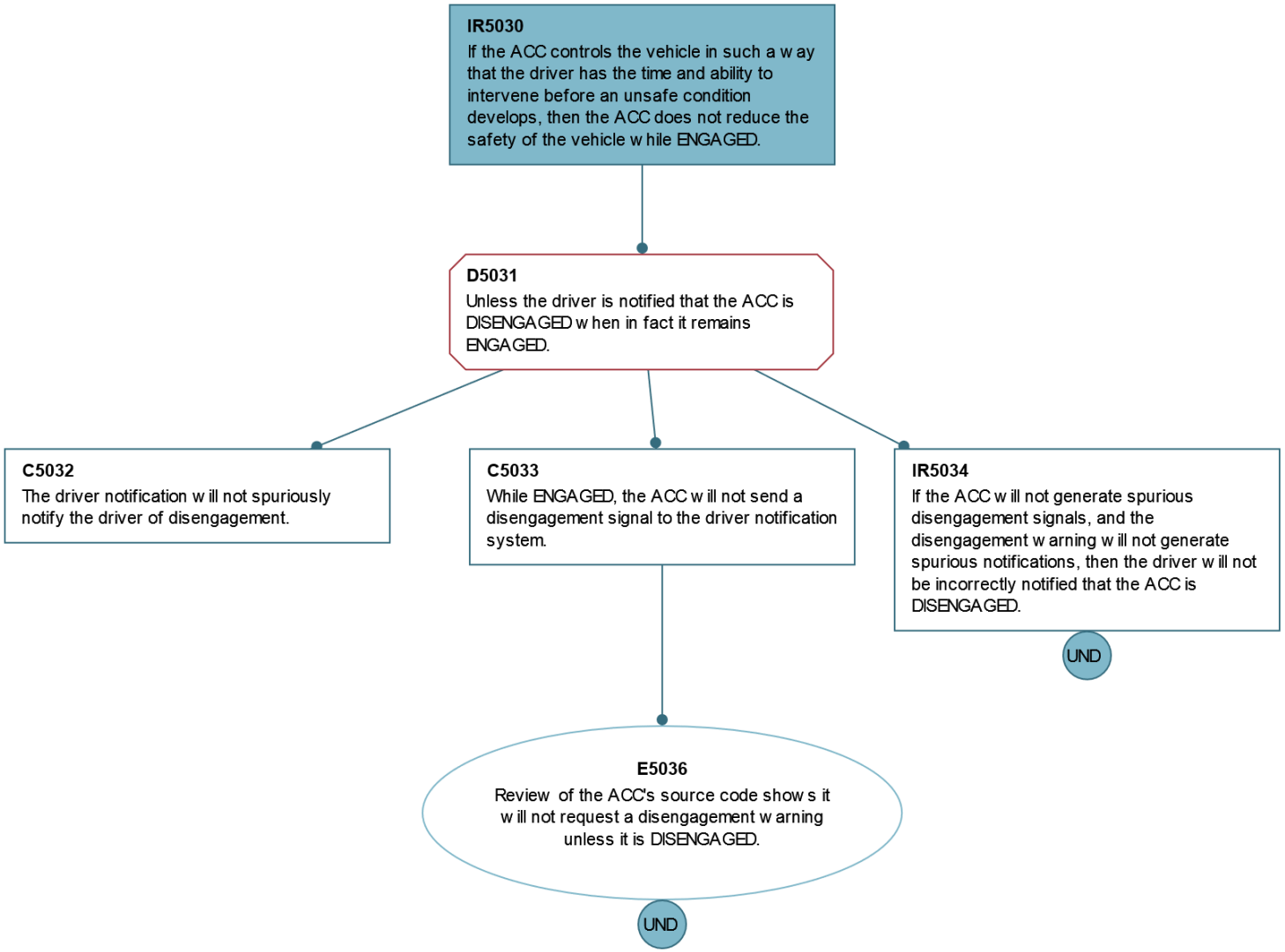
C1520 - The ACC engaging only partially results in the ACC remaining DISENGAGED			
Parent subtree(s)	C7100, IR1500, C8330	**Descendant subtree(s)**	None
Description			
Artifacts	E1524: Test Results	**Glossary Terms**	None



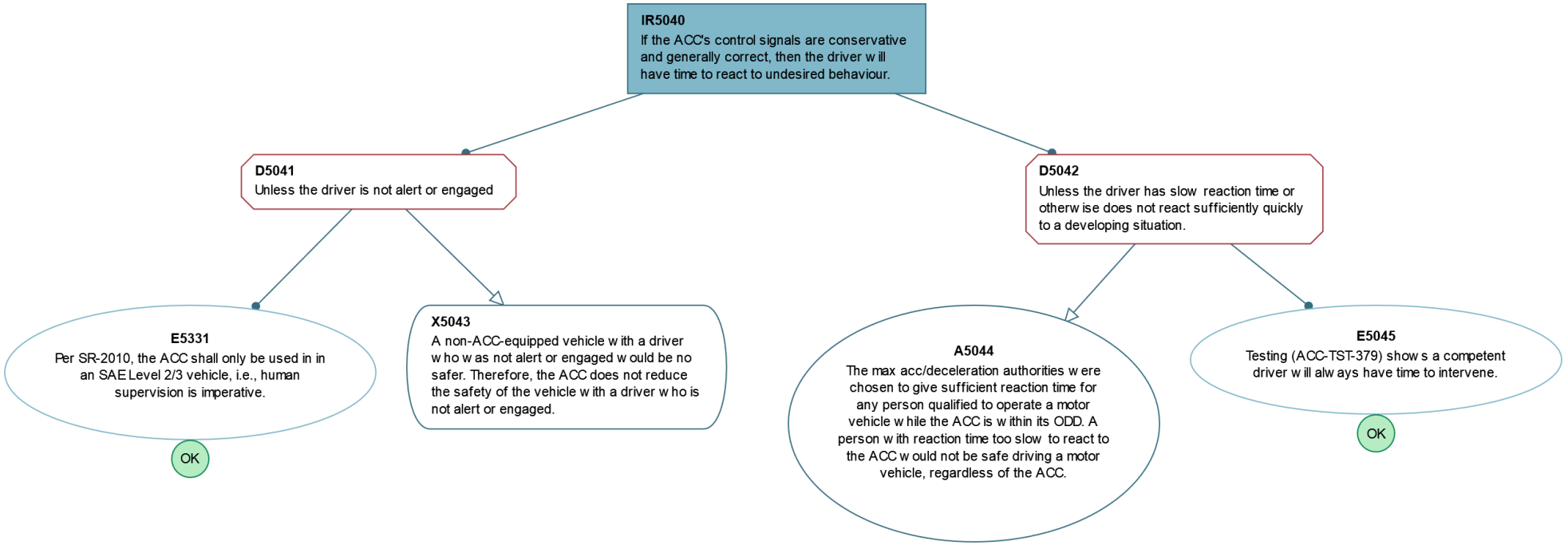
C5000 - The ACC does not reduce the safety of the vehicle while ENGAGED.			
Parent subtree(s)	C1000, C8320	**Descendant subtree(s)**	IR5030, IR5040, C5100, C5200, C5300
Description			
Artifacts	IR5030: Project Description, User Manual	**Glossary Terms**	None



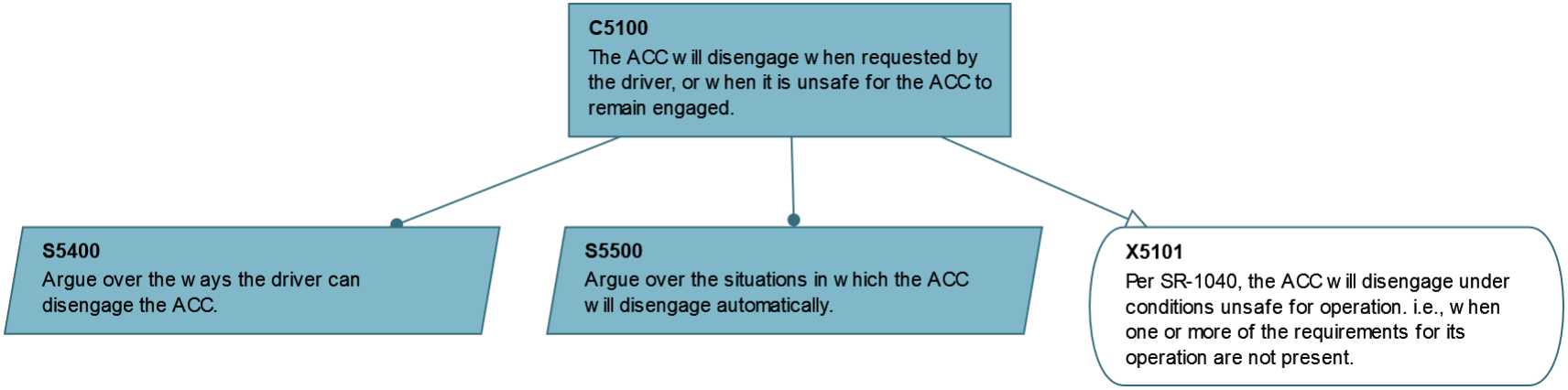
IR5030 - If the ACC controls the vehicle in such a way that the driver has the time and ability to intervene before an unsafe condition develops, the...			
Parent subtree(s)	C5000	**Descendant subtree(s)**	None
Description			
Artifacts	IR5030: Project Description, User Manual	**Glossary Terms**	None



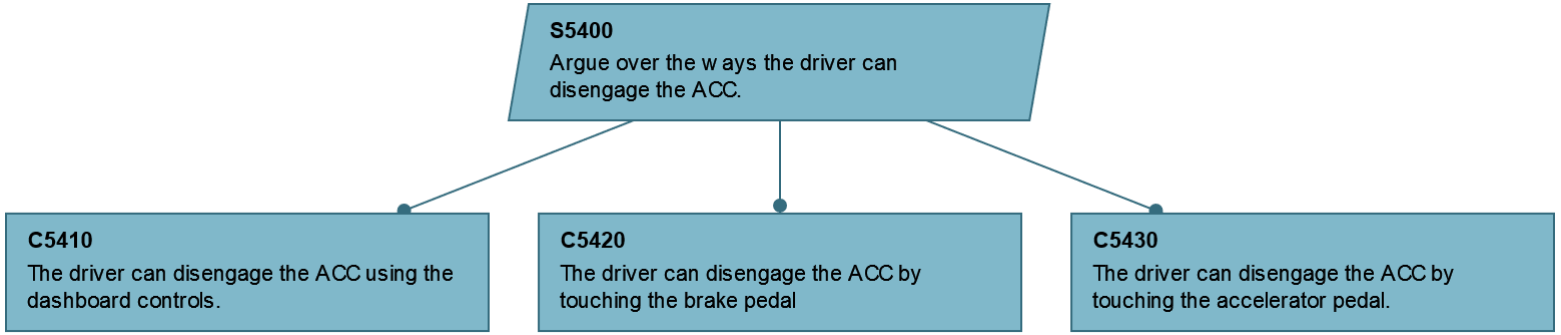
IR5040 - If the ACC's control signals are conservative and generally correct, then the driver will have time to react to undesired behaviour.			
Parent subtree(s)	C5000	**Descendant subtree(s)**	None
Description			
Artifacts	X5043: Project Description; E5331: Safety Manual Requirements	**Glossary Terms**	None



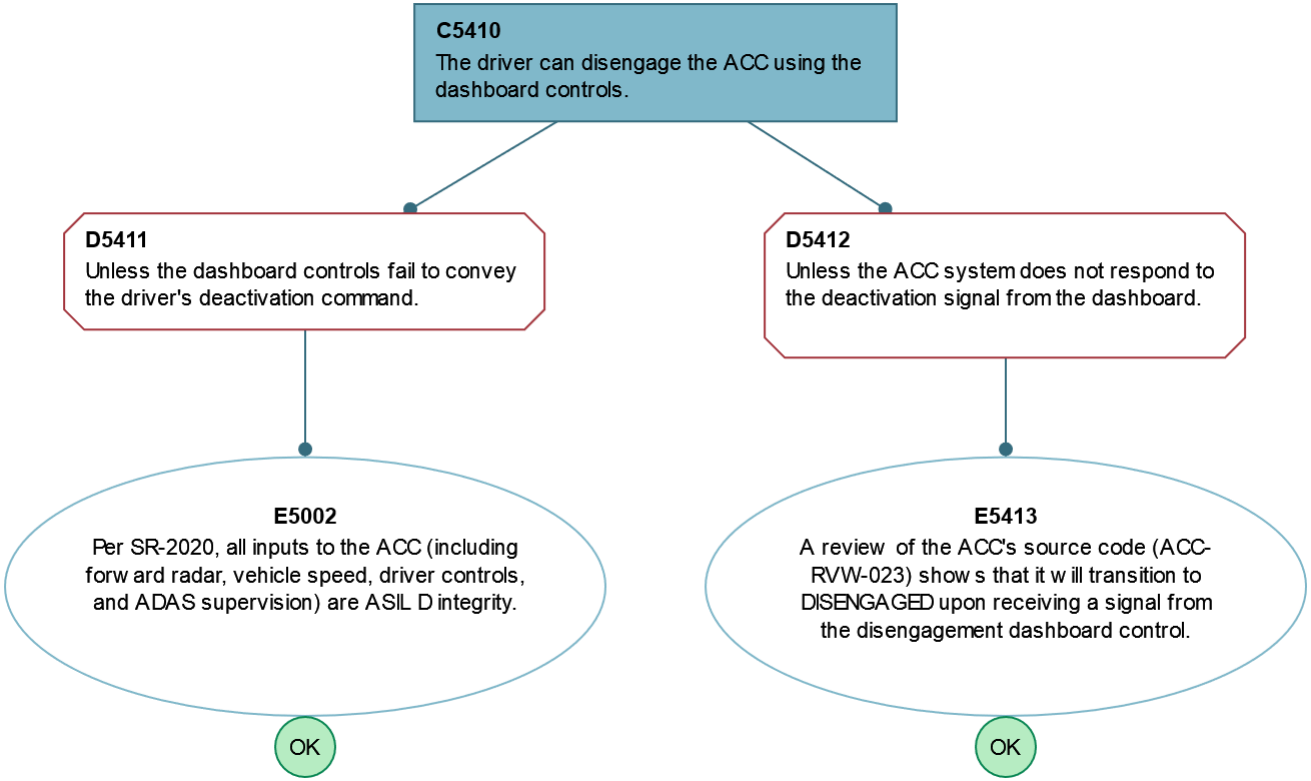
C5100 - The ACC will disengage when requested by the driver, or when it is unsafe for the ACC to remain engaged.			
Parent subtree(s)	C8100, C5000	**Descendant subtree(s)**	S5400, S5500
Description			
Artifacts	None	**Glossary Terms**	None



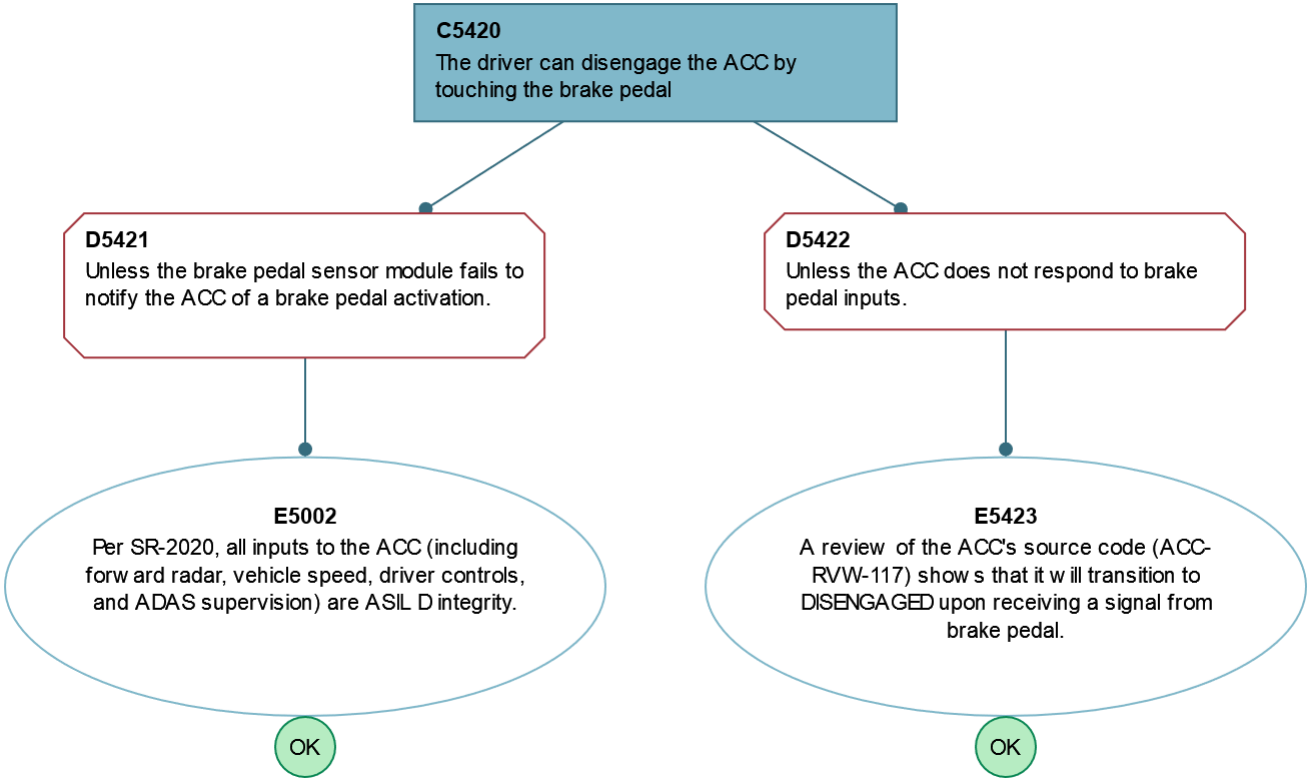
S5400 - Argue over the ways the driver can disengage the ACC.			
Parent subtree(s)	C5100	**Descendant subtree(s)**	C5410, C5420, C5430
Description			
Artifacts	None	**Glossary Terms**	None



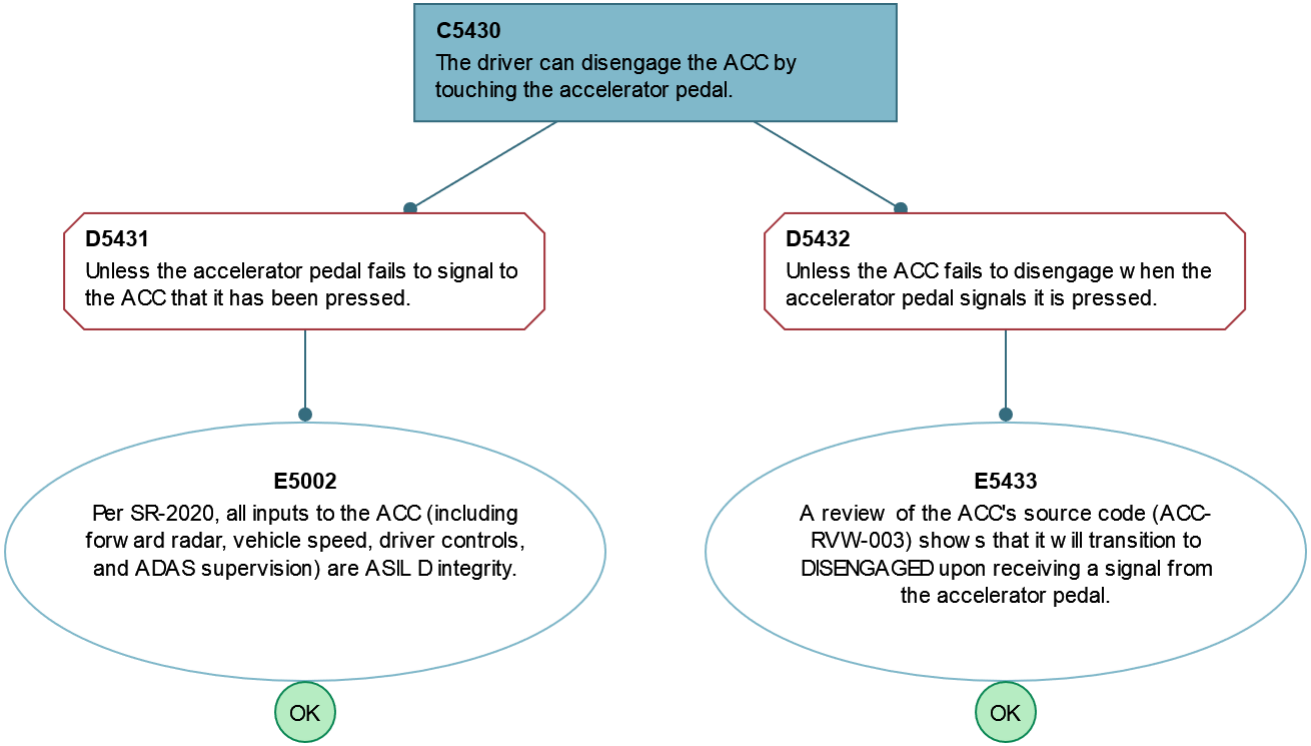
C5410 - The driver can disengage the ACC using the dashboard controls.			
Parent subtree(s)	S5400	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



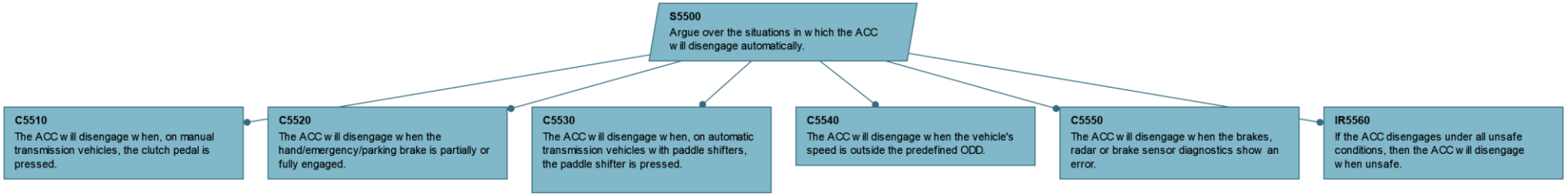
C5420 - The driver can disengage the ACC by touching the brake pedal			
Parent subtree(s)	S5400	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



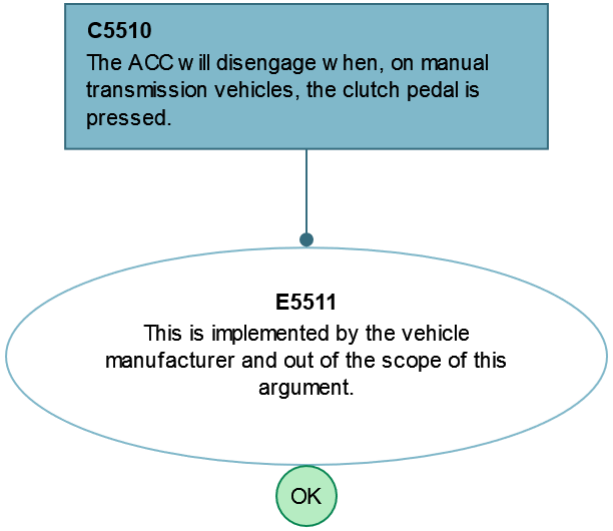
C5430 - The driver can disengage the ACC by touching the accelerator pedal.			
Parent subtree(s)	IR5320, S5400	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



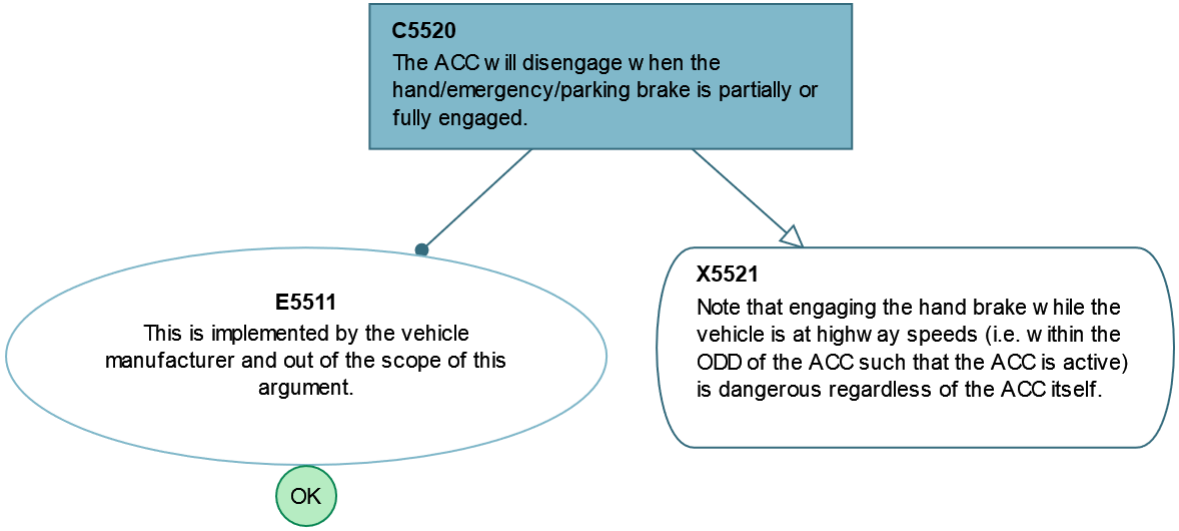
S5500 - Argue over the situations in which the ACC will disengage automatically.			
Parent subtree(s)	C5100	**Descendant subtree(s)**	C5510, C5520, C5530, C5540, C5550, IR5560
Description			
Artifacts	None	**Glossary Terms**	None



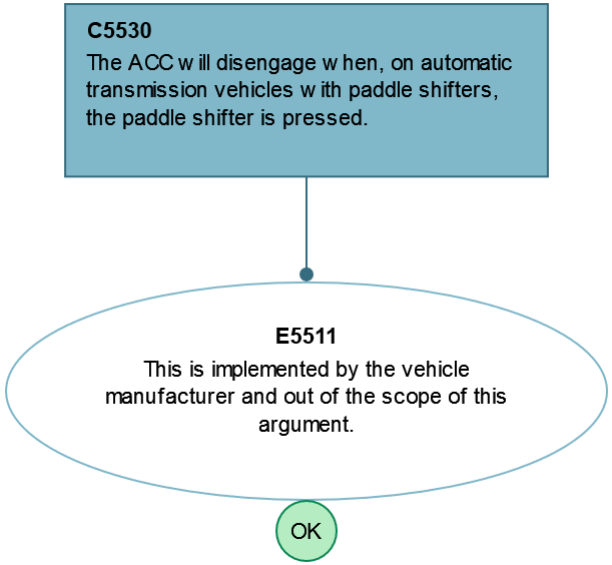
C5510 - The ACC will disengage when, on manual transmission vehicles, the clutch pedal is pressed.			
Parent subtree(s)	S5500	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



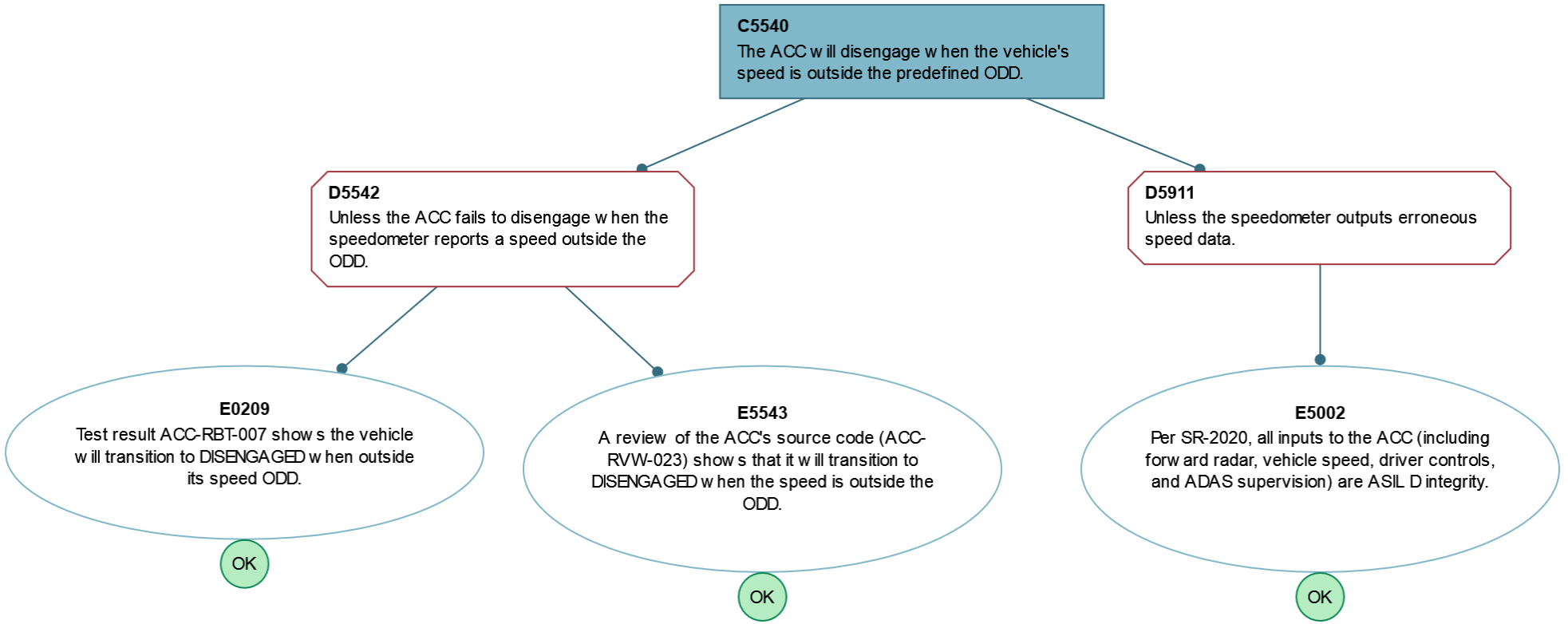
C5520 - The ACC will disengage when the hand/emergency/parking brake is partially or fully engaged.			
Parent subtree(s)	S5500	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



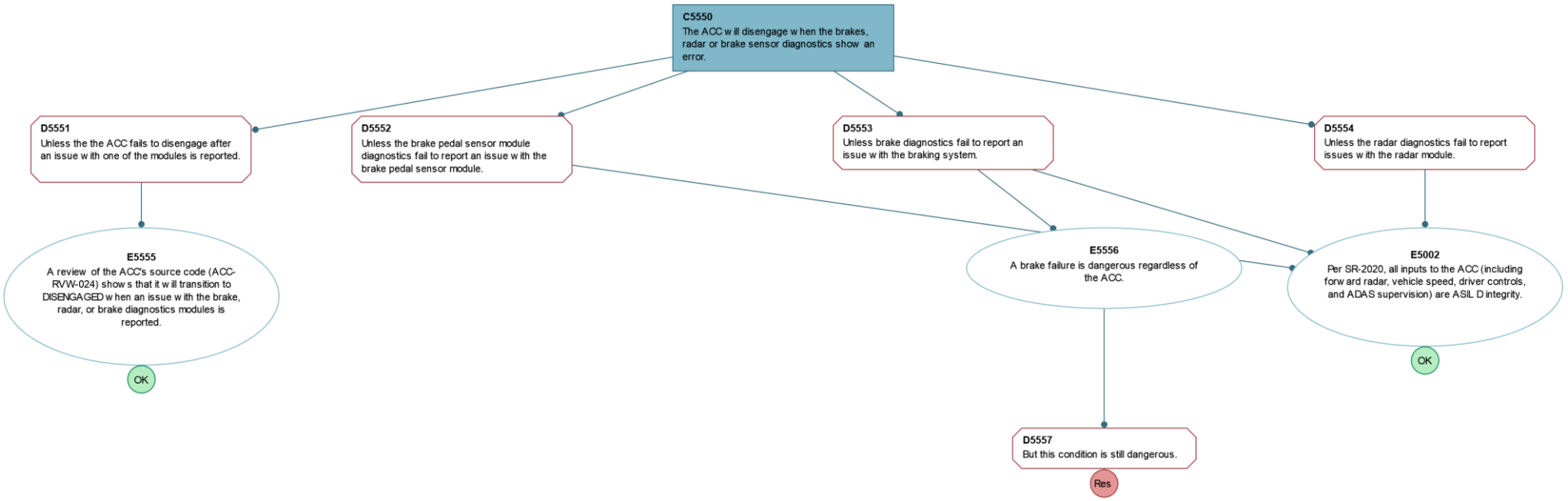
C5530 - The ACC will disengage when, on automatic transmission vehicles with paddle shifters, the paddle shifter is pressed.			
Parent subtree(s)	S5500	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



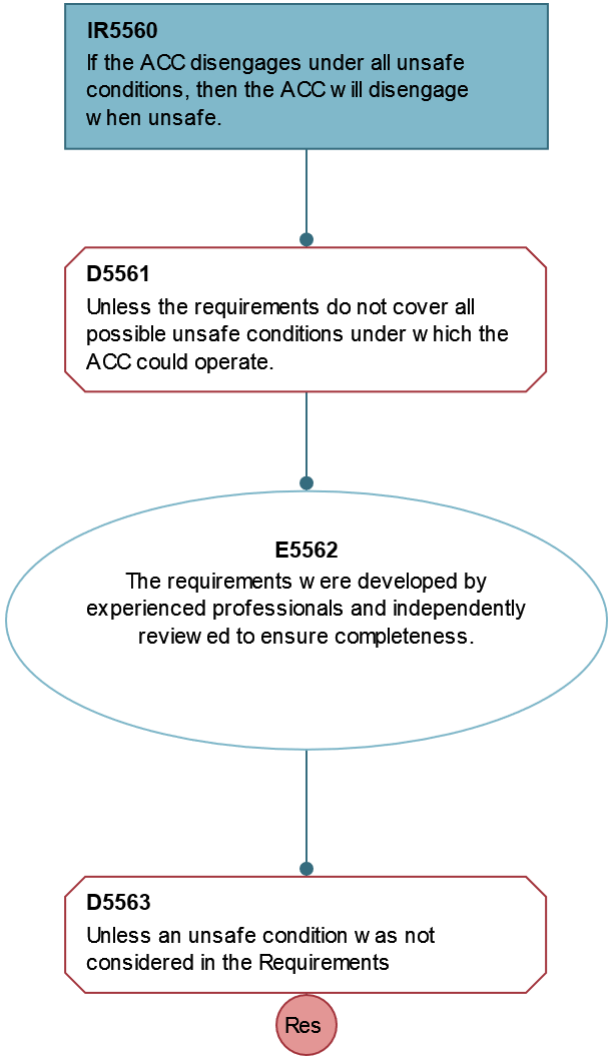
C5540 - The ACC will disengage when the vehicle's speed is outside the predefined ODD.			
Parent subtree(s)	S5500	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



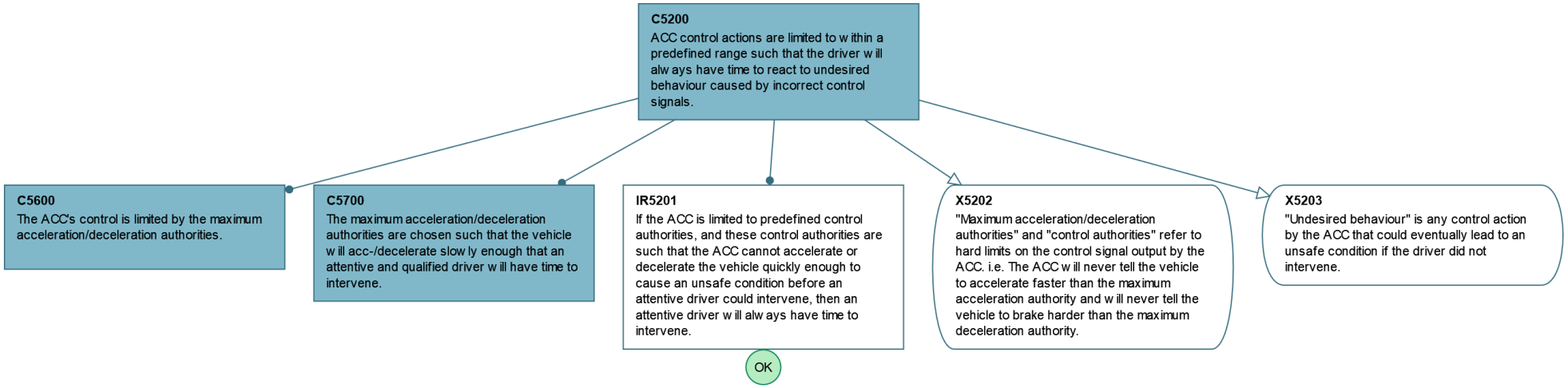
C5550 - The ACC will disengage when the brakes, radar or brake sensor diagnostics show an error.			
Parent subtree(s)	S5500	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



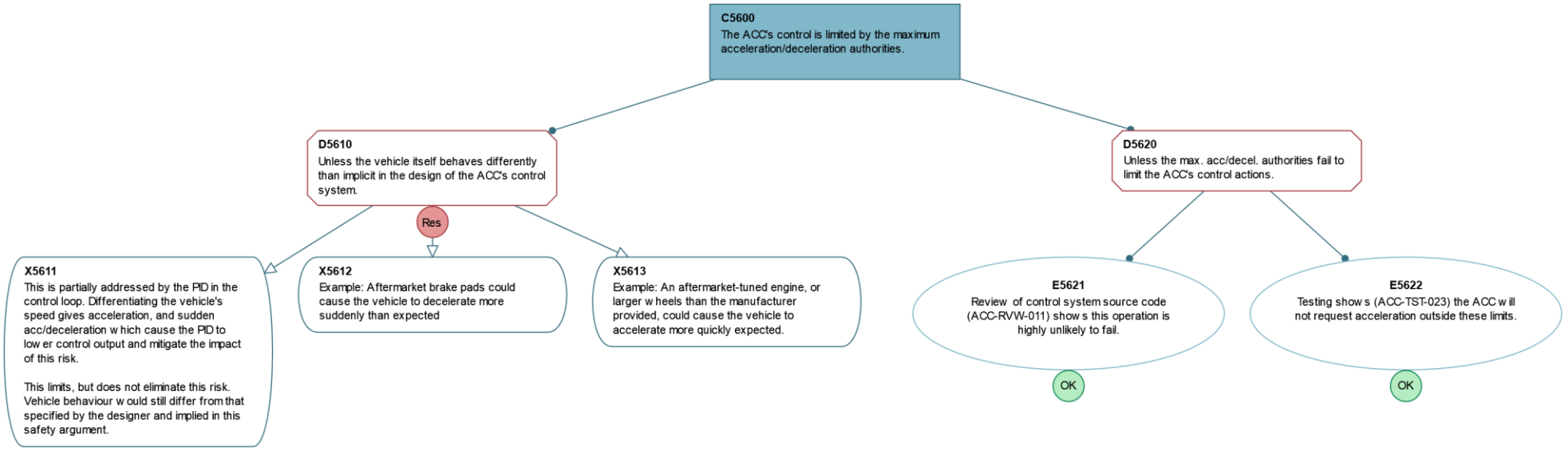
IR5560 - If the ACC disengages under all unsafe conditions, then the ACC will disengage when unsafe.			
Parent subtree(s)	S5500	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



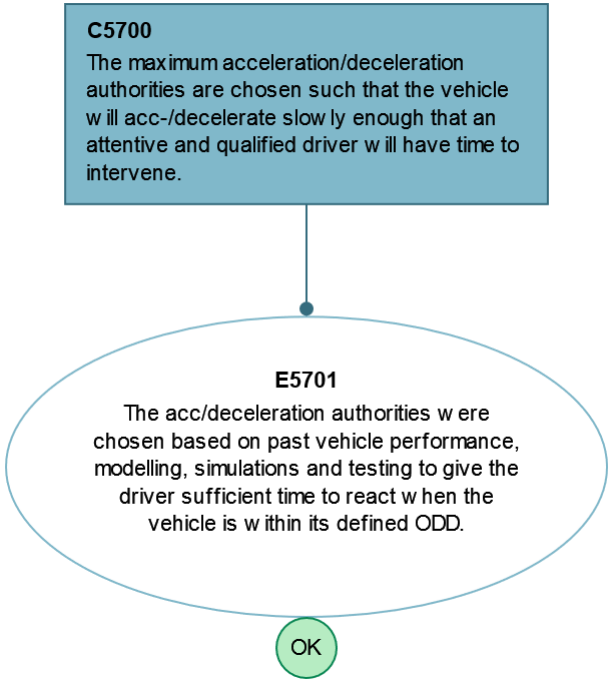
C5200 - ACC control actions are limited to within a predefined range such that the driver will always have time to react to undesired behaviour caus...			
Parent subtree(s)	C5000	**Descendant subtree(s)**	C5600, C5700
Description			
Artifacts	None	**Glossary Terms**	None



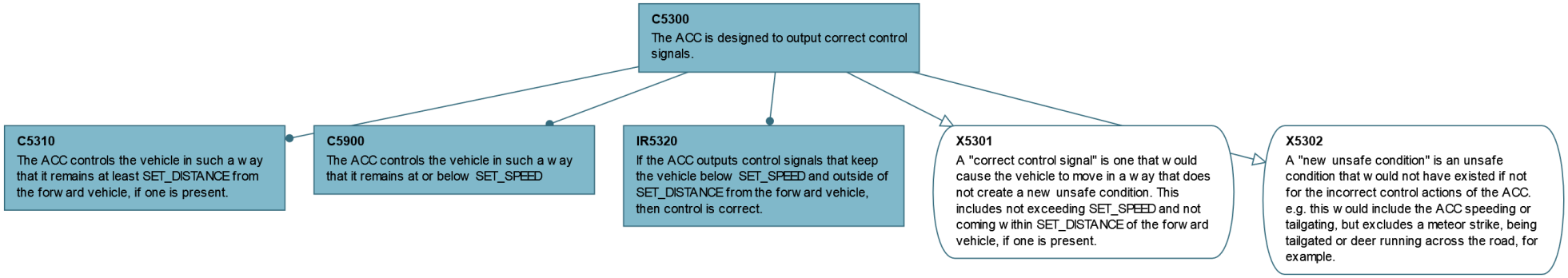
C5600 - The ACC's control is limited by the maximum acceleration/deceleration authorities.			
Parent subtree(s)	C5200	**Descendant subtree(s)**	None
Description			
Artifacts	E5621: Max Acceleration-Deceleration Authority FTA; E5622: Test Results	**Glossary Terms**	None



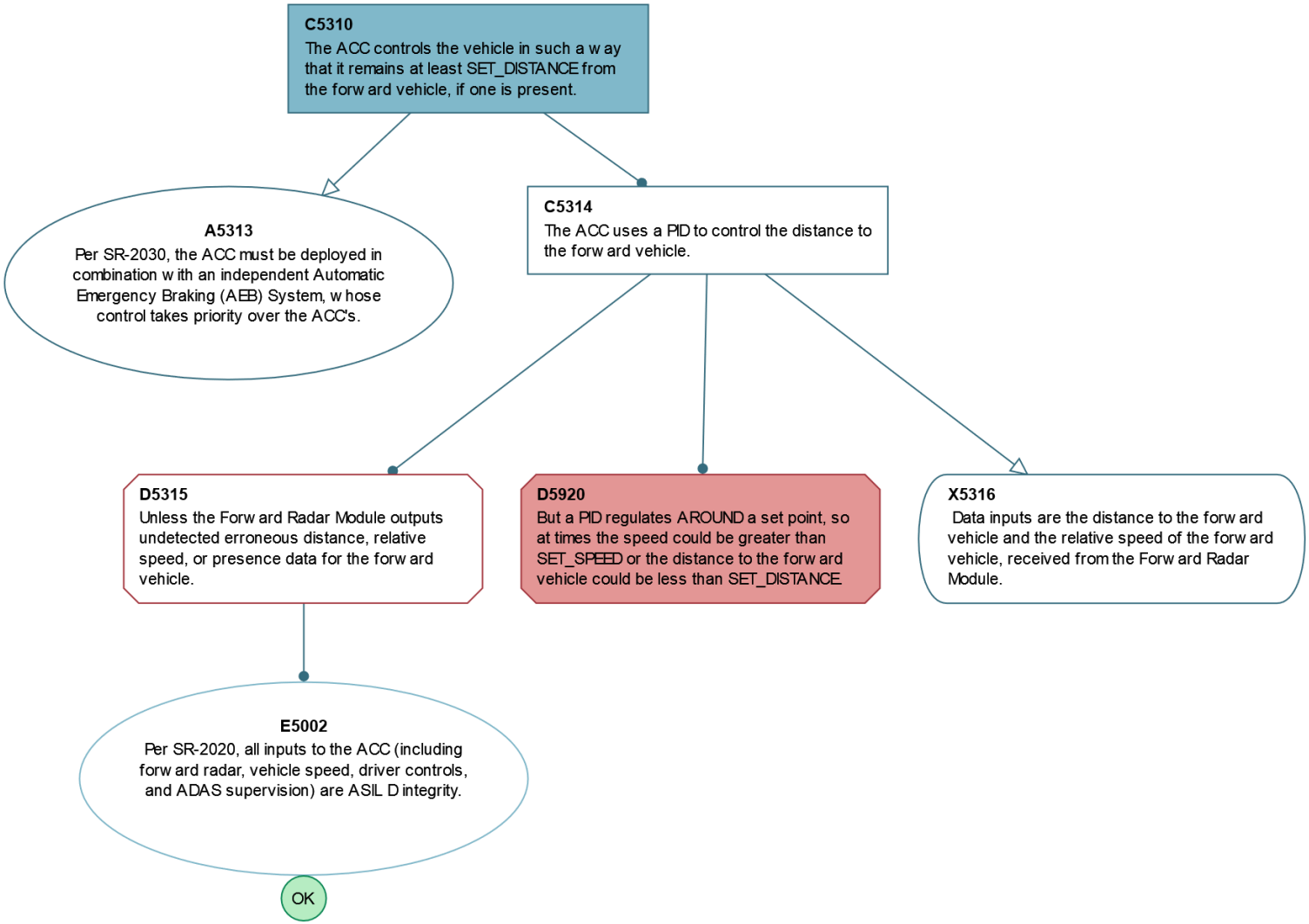
C5700 - The maximum acceleration/deceleration authorities are chosen such that the vehicle will acc-/decelerate slowly enough that an attentive and ...			
Parent subtree(s)	C5200	**Descendant subtree(s)**	None
Description			
Artifacts	E5701: Test Results	**Glossary Terms**	None



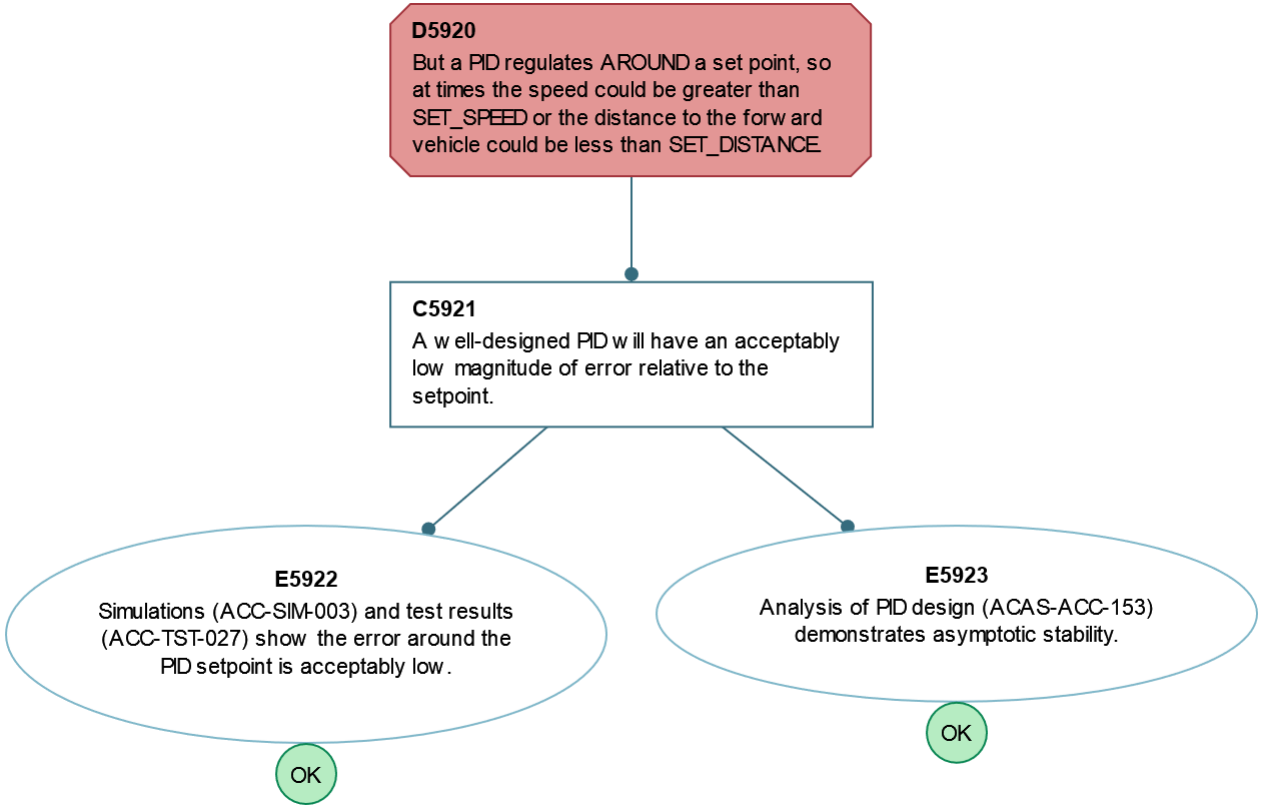
C5300 - The ACC is designed to output correct control signals.			
Parent subtree(s)	C5000	**Descendant subtree(s)**	C5310, IR5320, C5900
Description			
Artifacts	None	**Glossary Terms**	None



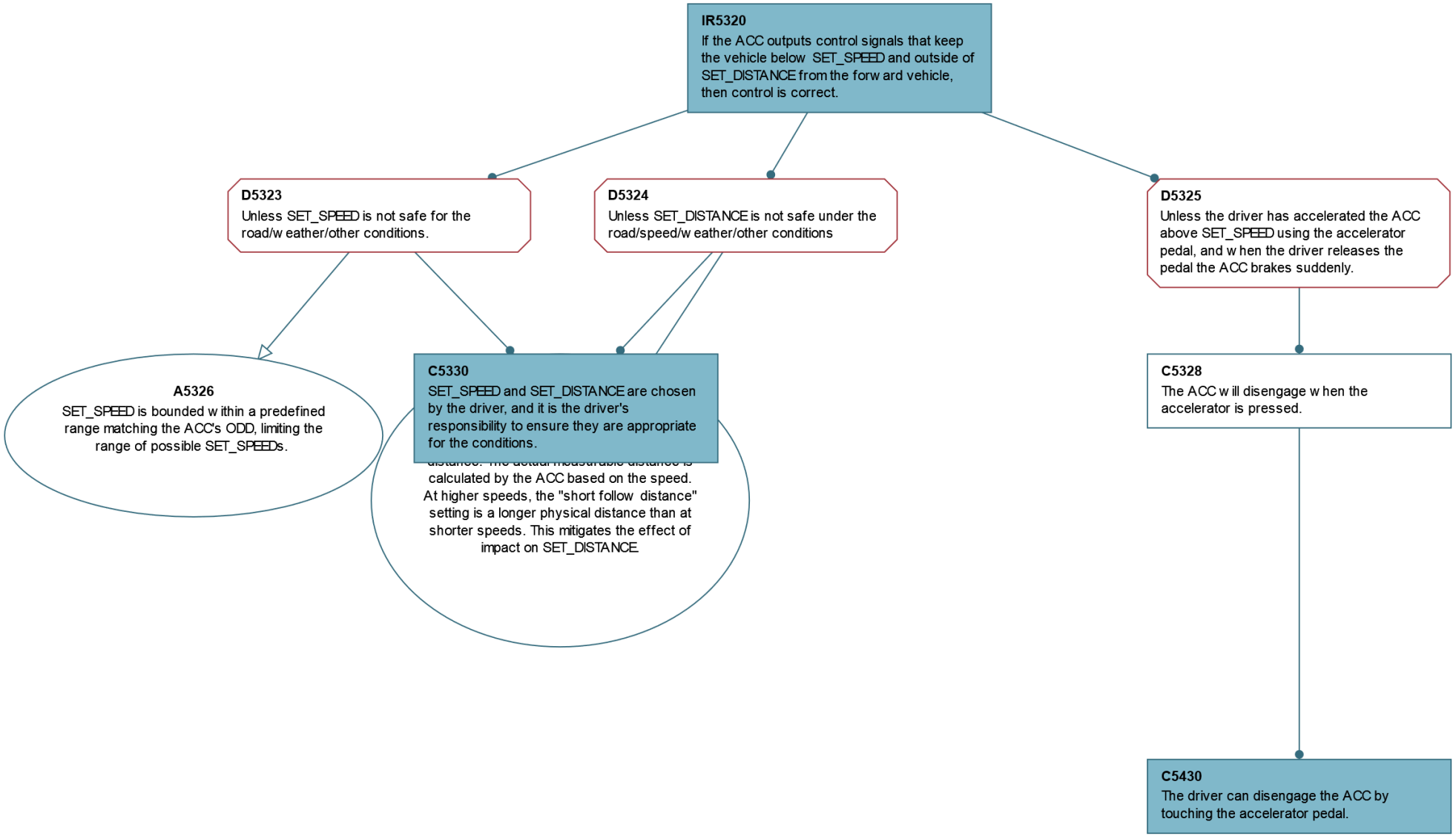
C5310 - The ACC controls the vehicle in such a way that it remains at least SET_DISTANCE from the forward vehicle, if one is present.			
Parent subtree(s)	C5300	**Descendant subtree(s)**	D5920
Description			
Artifacts	None	**Glossary Terms**	None



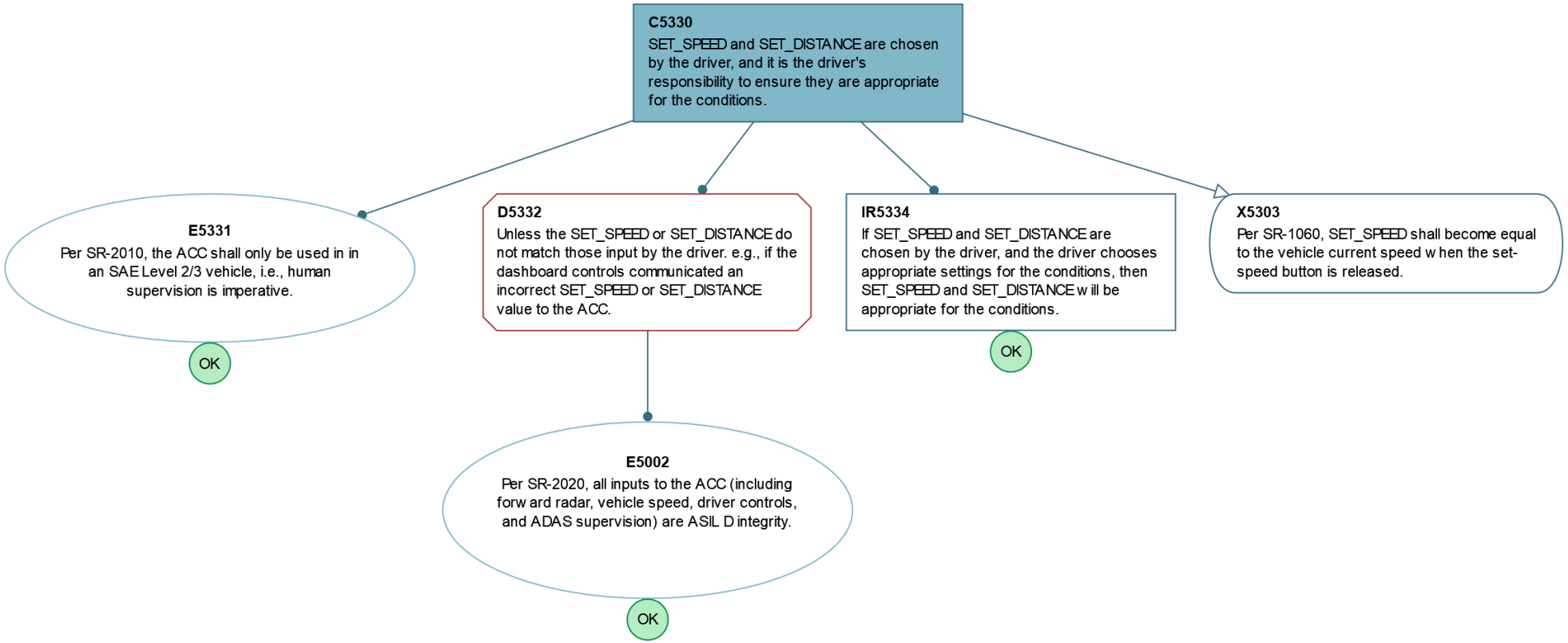
D5920 - But a PID regulates AROUND a set point, so at times the speed could be greater than SET_SPEED or the distance to the forward vehicle could b...			
Parent subtree(s)	C5310, C5900	**Descendant subtree(s)**	None
Description			
Artifacts	E5922: Test Results	**Glossary Terms**	None



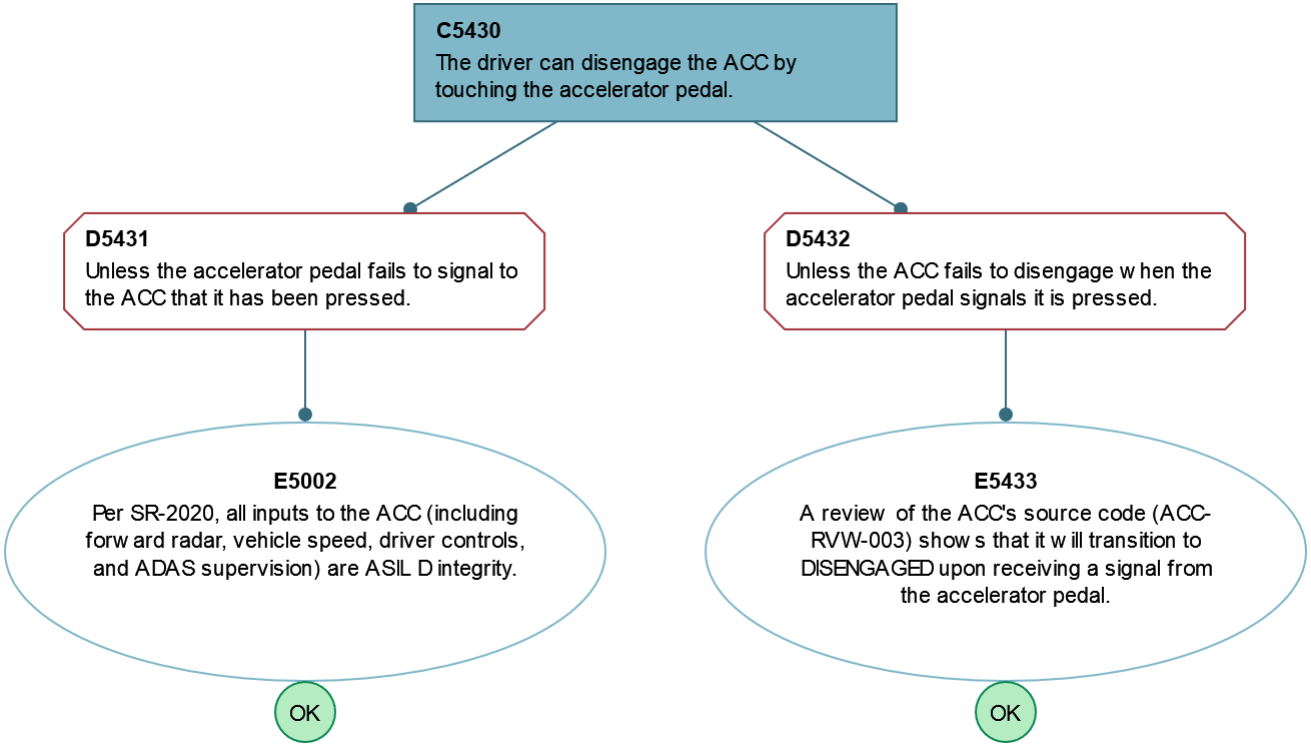
IR5320 - If the ACC outputs control signals that keep the vehicle below SET_SPEED and outside of SET_DISTANCE from the forward vehicle, then control ...			
Parent subtree(s)	C5300	**Descendant subtree(s)**	C5330, C5430
Description			
Artifacts	None	**Glossary Terms**	None



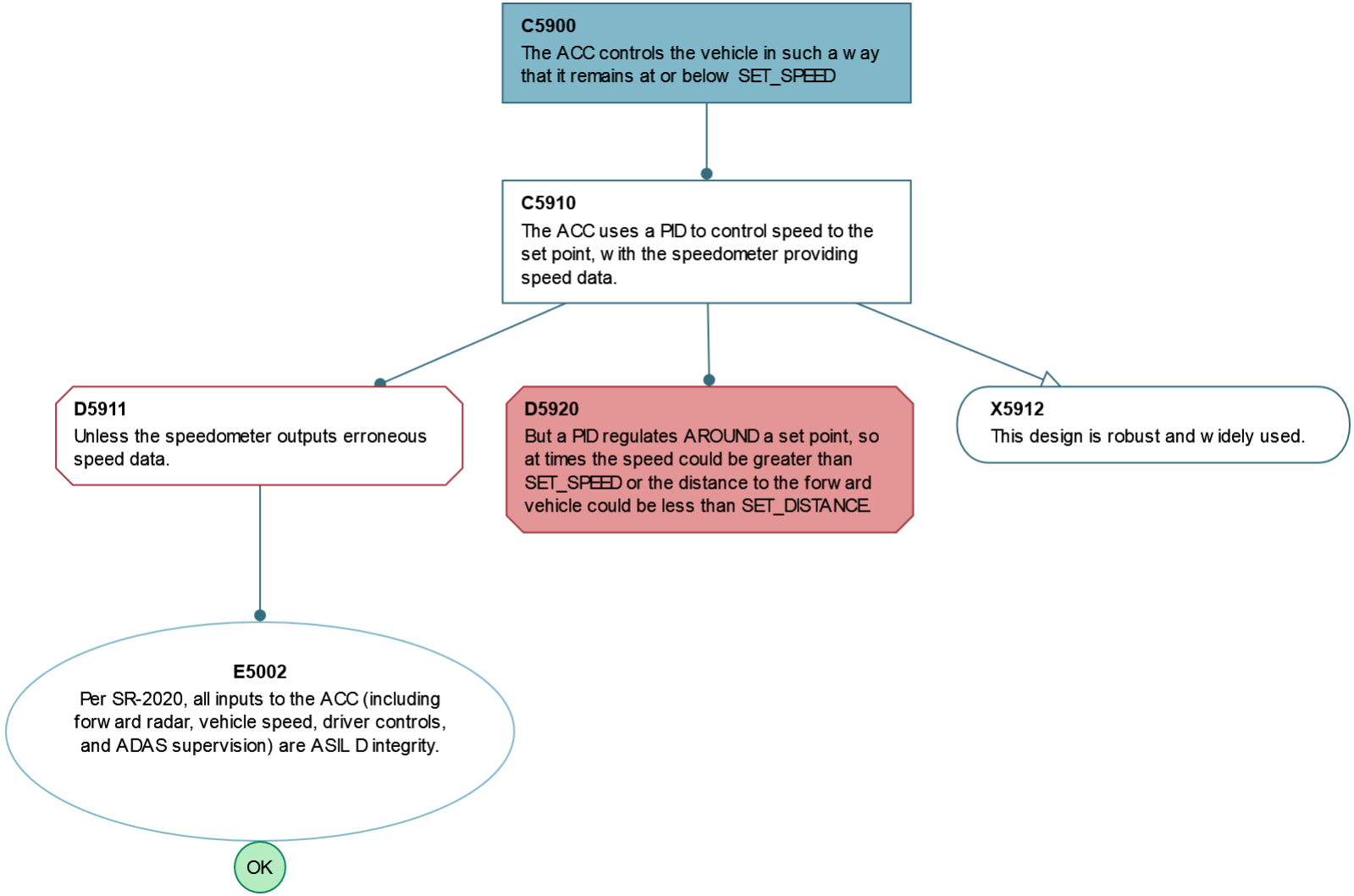
C5330 - SET_SPEED and SET_DISTANCE are chosen by the driver, and it is the driver's responsibility to ensure they are appropriate for the conditions...			
Parent subtree(s)	IR5320	**Descendant subtree(s)**	None
Description			
Artifacts	E5331: Safety Manual Requirements	**Glossary Terms**	None



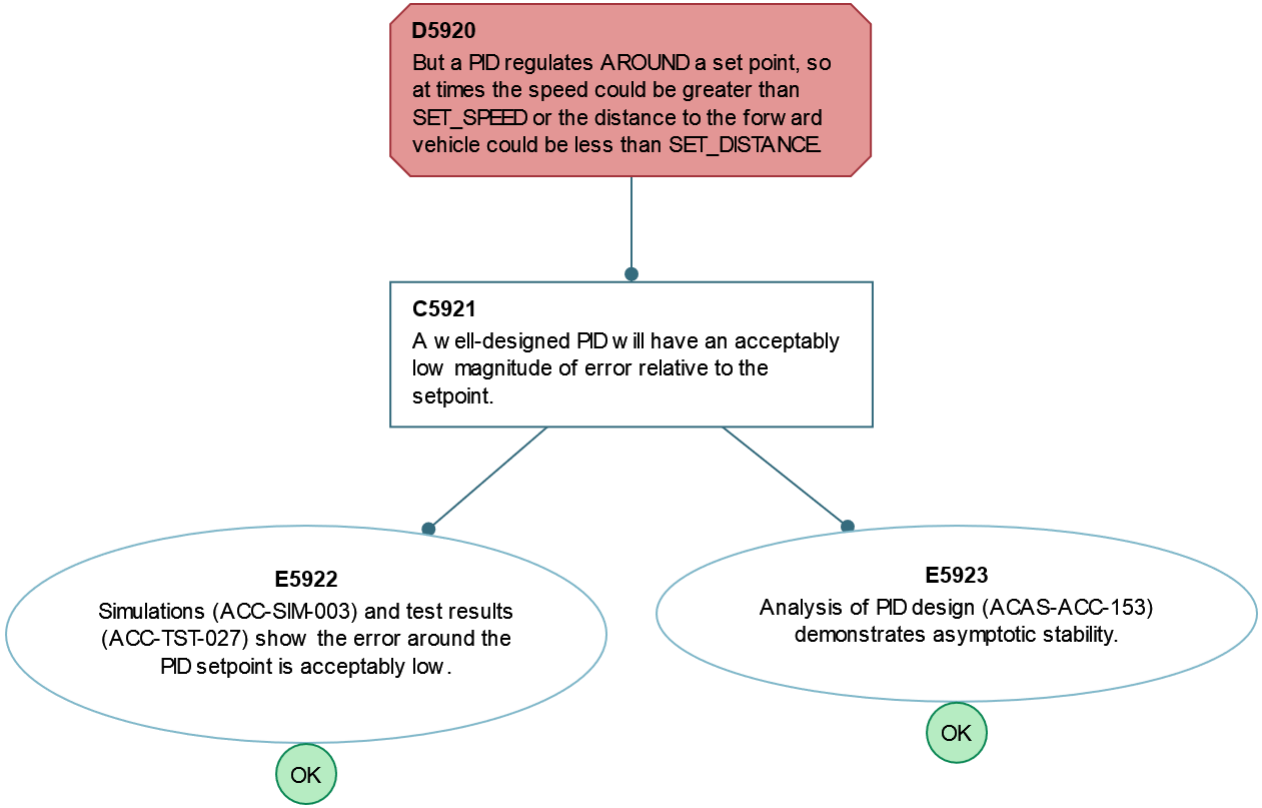
C5430 - The driver can disengage the ACC by touching the accelerator pedal.			
Parent subtree(s)	IR5320, S5400	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



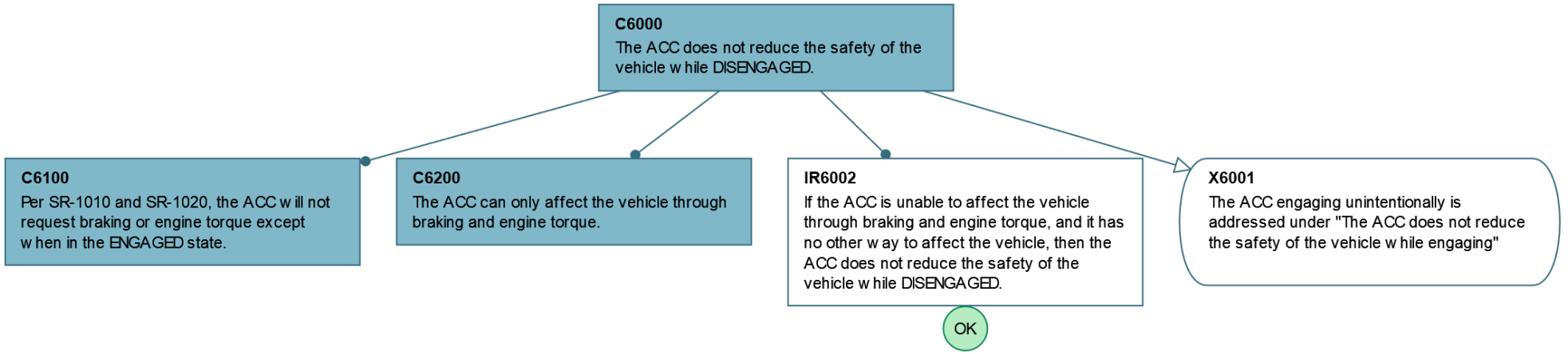
C5900 - The ACC controls the vehicle in such a way that it remains at or below SET_SPEED			
Parent subtree(s)	C5300	**Descendant subtree(s)**	D5920
Description			
Artifacts	None	**Glossary Terms**	None



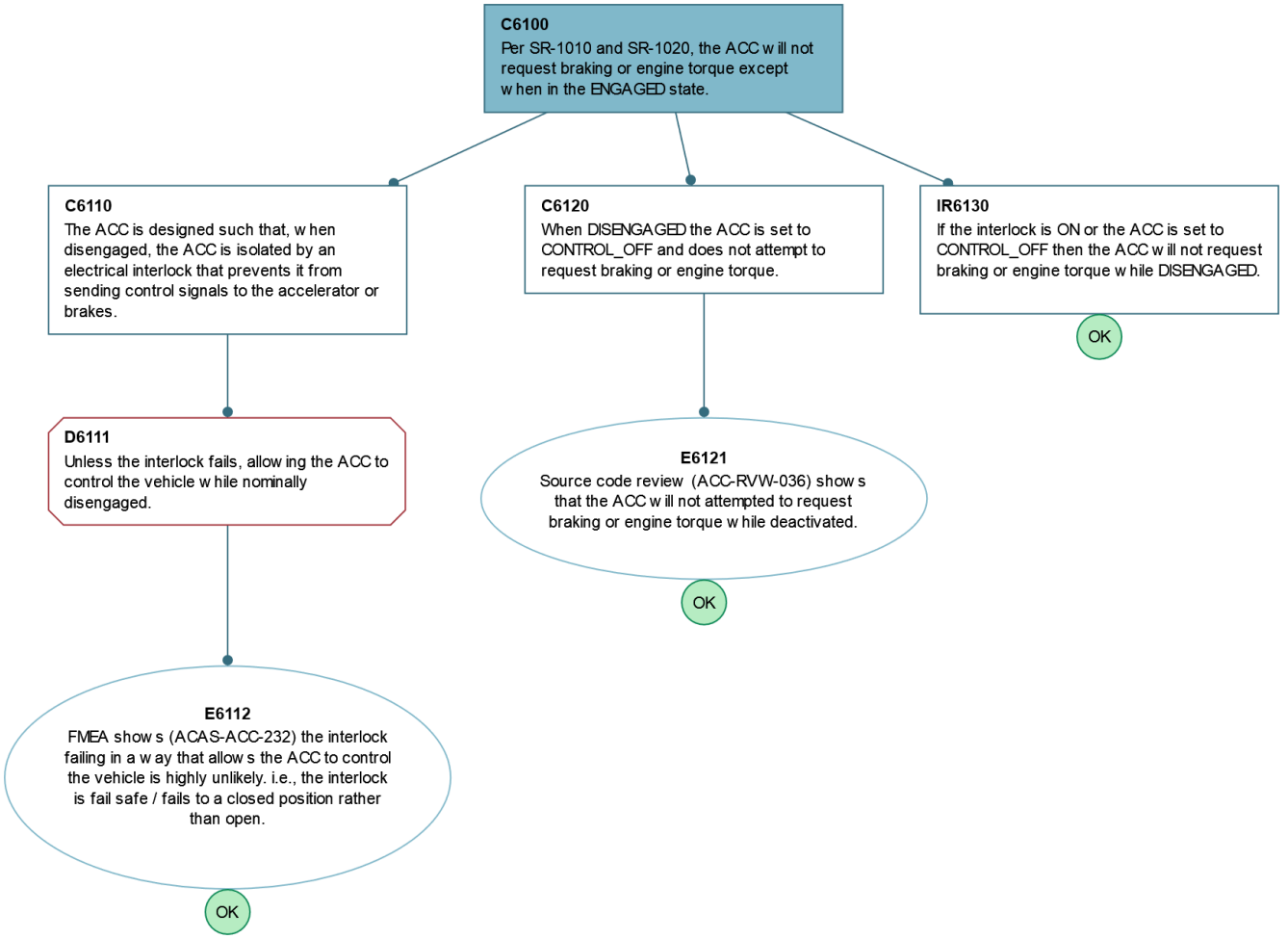
D5920 - But a PID regulates AROUND a set point, so at times the speed could be greater than SET_SPEED or the distance to the forward vehicle could b...			
Parent subtree(s)	C5310, C5900	**Descendant subtree(s)**	None
Description			
Artifacts	E5922: Test Results	**Glossary Terms**	None



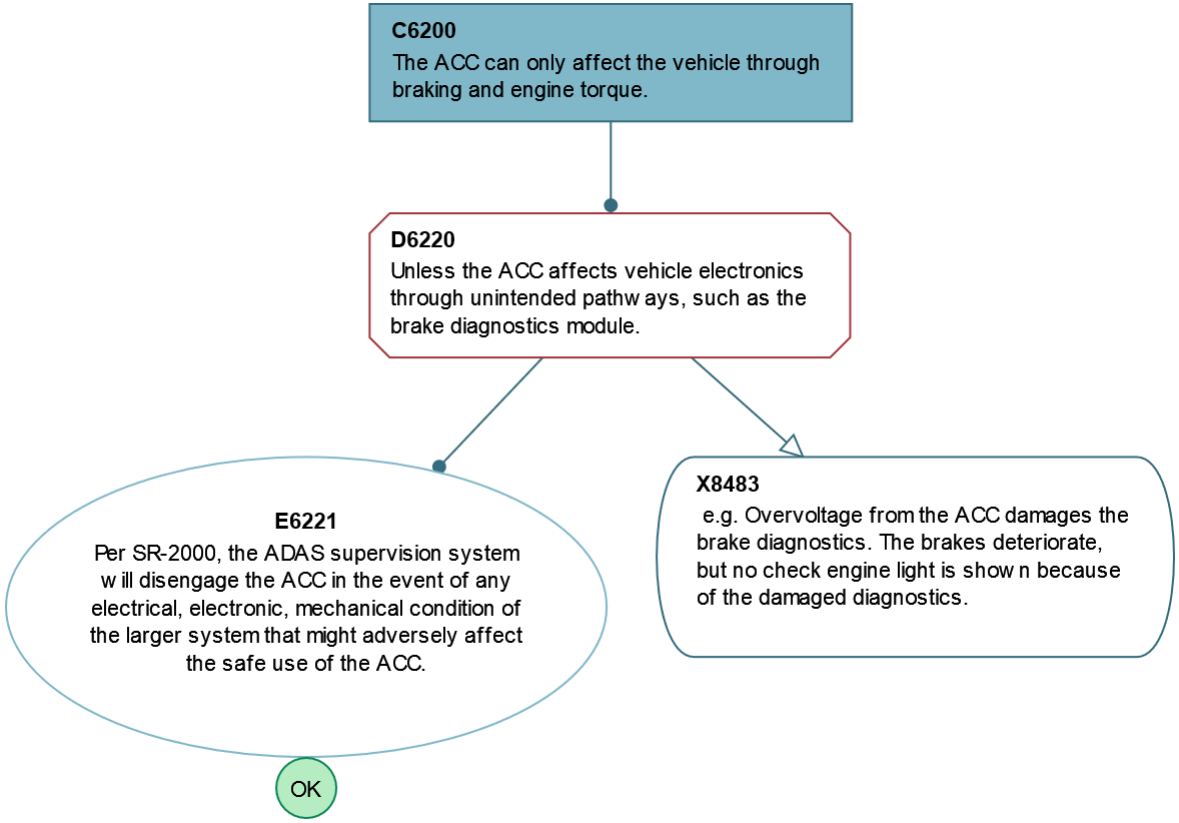
C6000 - The ACC does not reduce the safety of the vehicle while DISENGAGED.			
Parent subtree(s)	C1000, C8330, C7000	**Descendant subtree(s)**	C6100, C6200
Description			
Artifacts	None	**Glossary Terms**	None



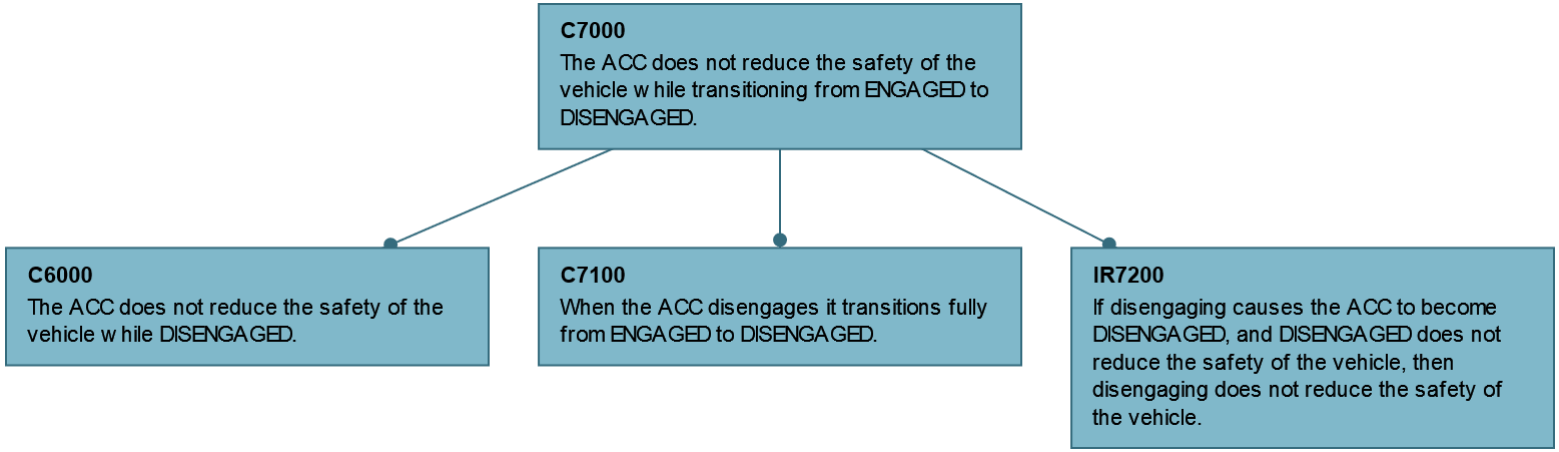
C6100 - Per SR-1010 and SR-1020, the ACC will not request braking or engine torque except when in the ENGAGED state.			
Parent subtree(s)	C6000	**Descendant subtree(s)**	None
Description			
Artifacts	E6112: Interlock FMEA	**Glossary Terms**	None



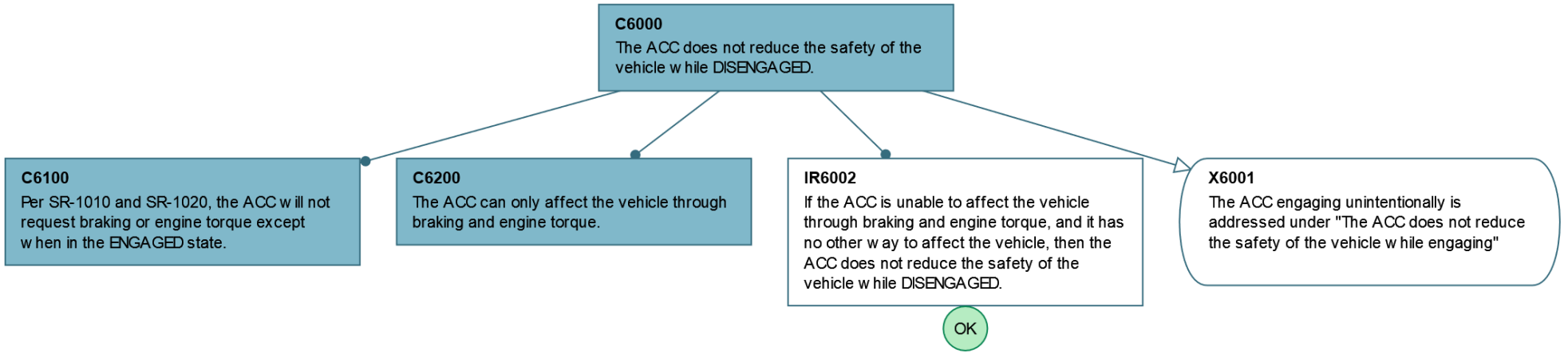
C6200 - The ACC can only affect the vehicle through braking and engine torque.			
Parent subtree(s)	C6000	**Descendant subtree(s)**	None
Description			
Artifacts	E6221: Safety Manual Requirements	**Glossary Terms**	None



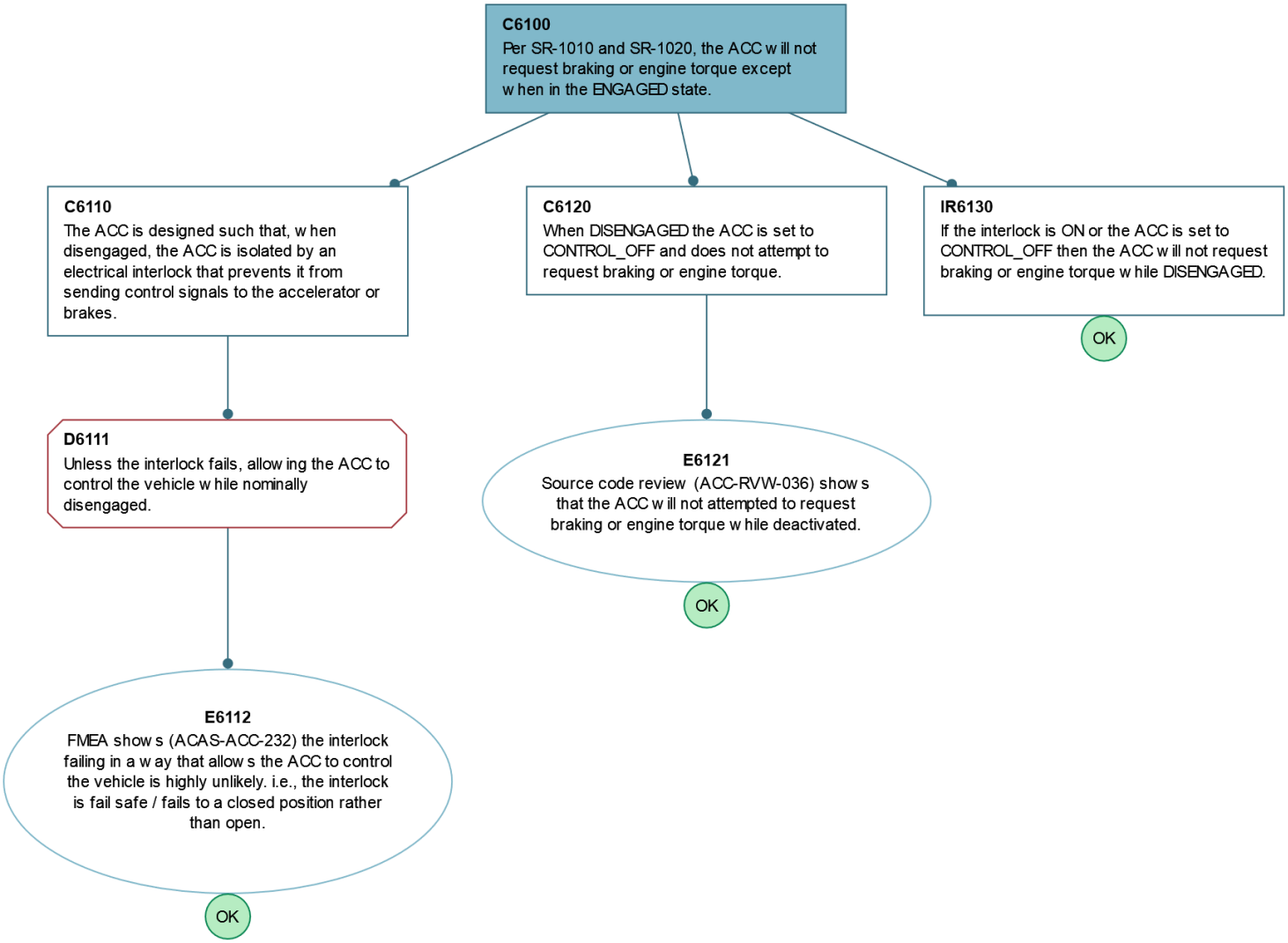
C7000 - The ACC does not reduce the safety of the vehicle while transitioning from ENGAGED to DISENGAGED.			
Parent subtree(s)	C1000	**Descendant subtree(s)**	C6000, C7100, IR7200
Description			
Artifacts	None	**Glossary Terms**	None



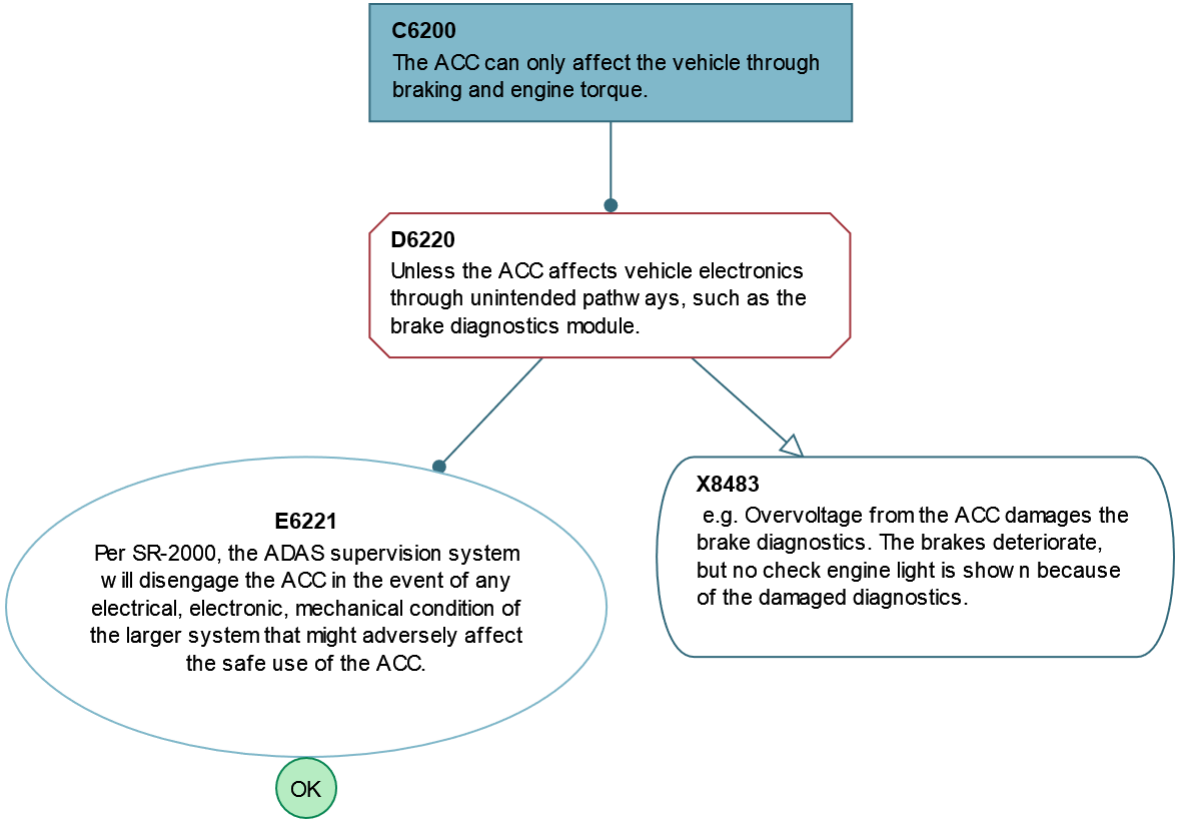
C6000 - The ACC does not reduce the safety of the vehicle while DISENGAGED.			
Parent subtree(s)	C1000, C8330, C7000	**Descendant subtree(s)**	C6100, C6200
Description			
Artifacts	None	**Glossary Terms**	None



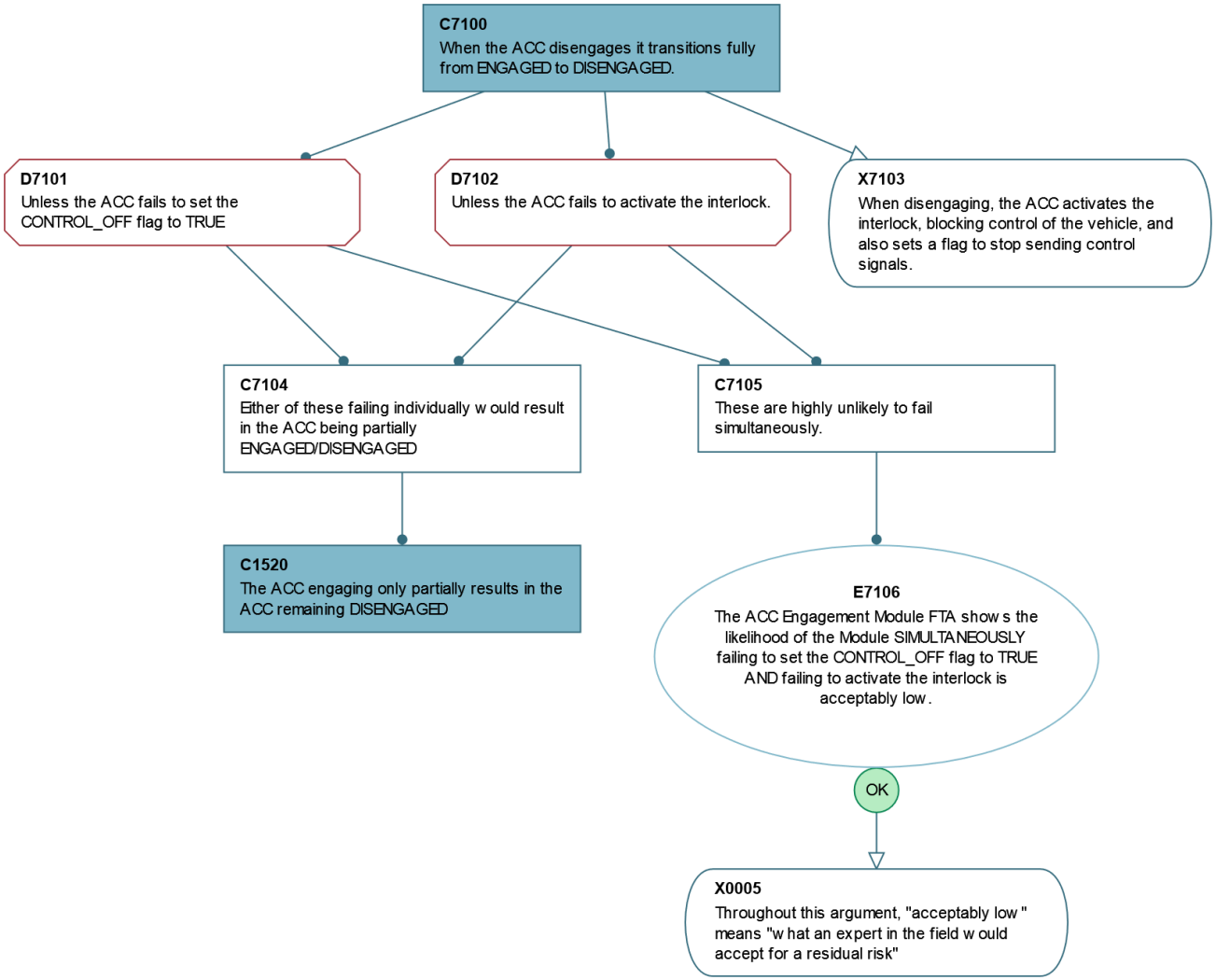
C6100 - Per SR-1010 and SR-1020, the ACC will not request braking or engine torque except when in the ENGAGED state.			
Parent subtree(s)	C6000	**Descendant subtree(s)**	None
Description			
Artifacts	E6112: Interlock FMEA	**Glossary Terms**	None



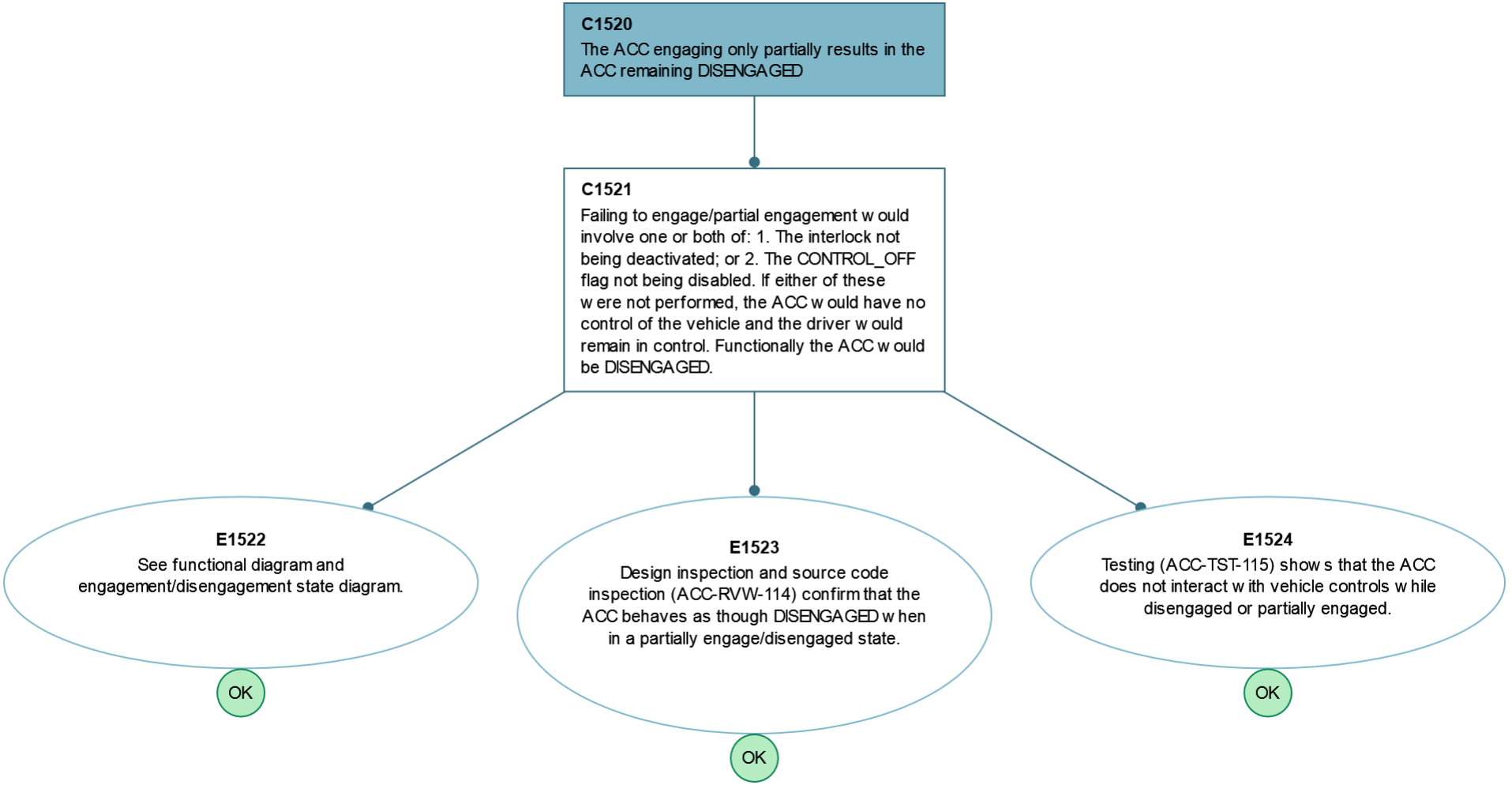
C6200 - The ACC can only affect the vehicle through braking and engine torque.			
Parent subtree(s)	C6000	**Descendant subtree(s)**	None
Description			
Artifacts	E6221: Safety Manual Requirements	**Glossary Terms**	None



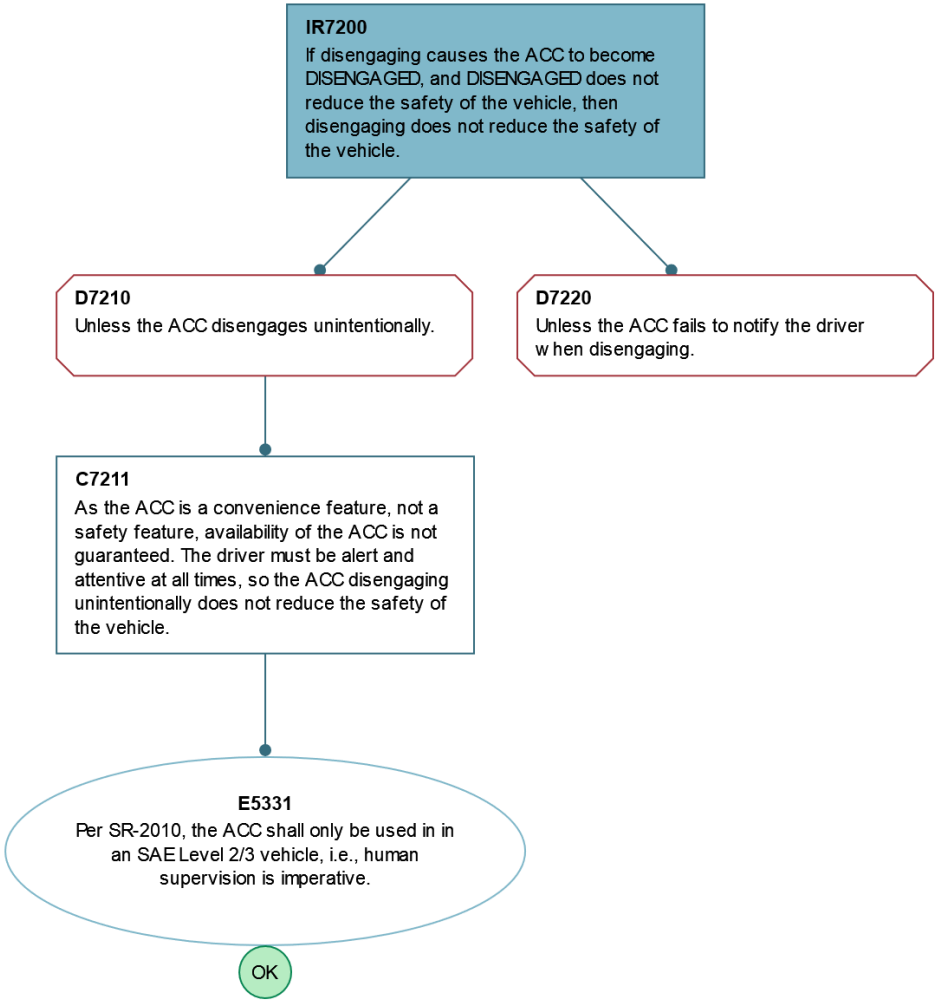
C7100 - When the ACC disengages it transitions fully from ENGAGED to DISENGAGED.			
Parent subtree(s)	C7000	**Descendant subtree(s)**	C1520
Description			
Artifacts	E7106: ACC Engagement Module FTA	**Glossary Terms**	None



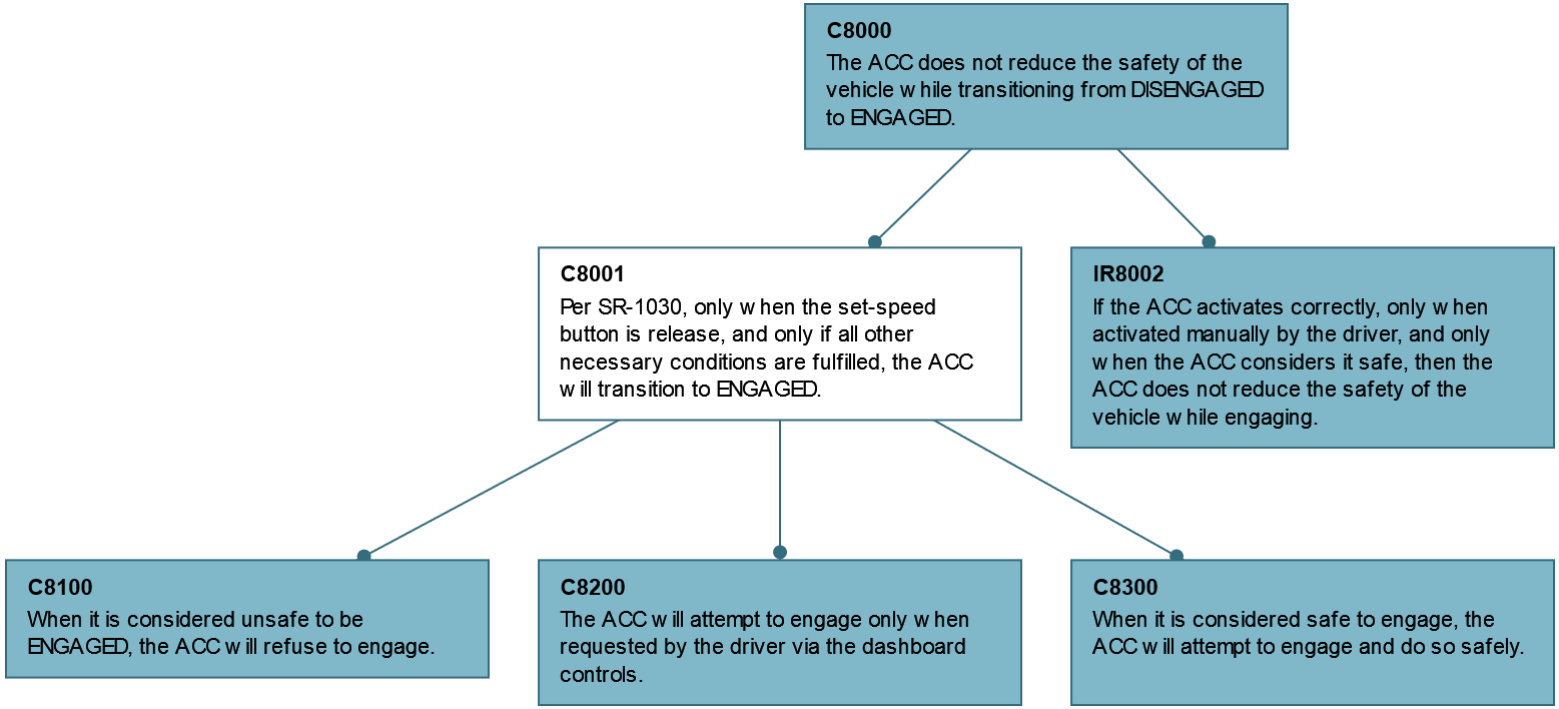
C1520 - The ACC engaging only partially results in the ACC remaining DISENGAGED			
Parent subtree(s)	C7100, IR1500, C8330	**Descendant subtree(s)**	None
Description			
Artifacts	E1524: Test Results	**Glossary Terms**	None



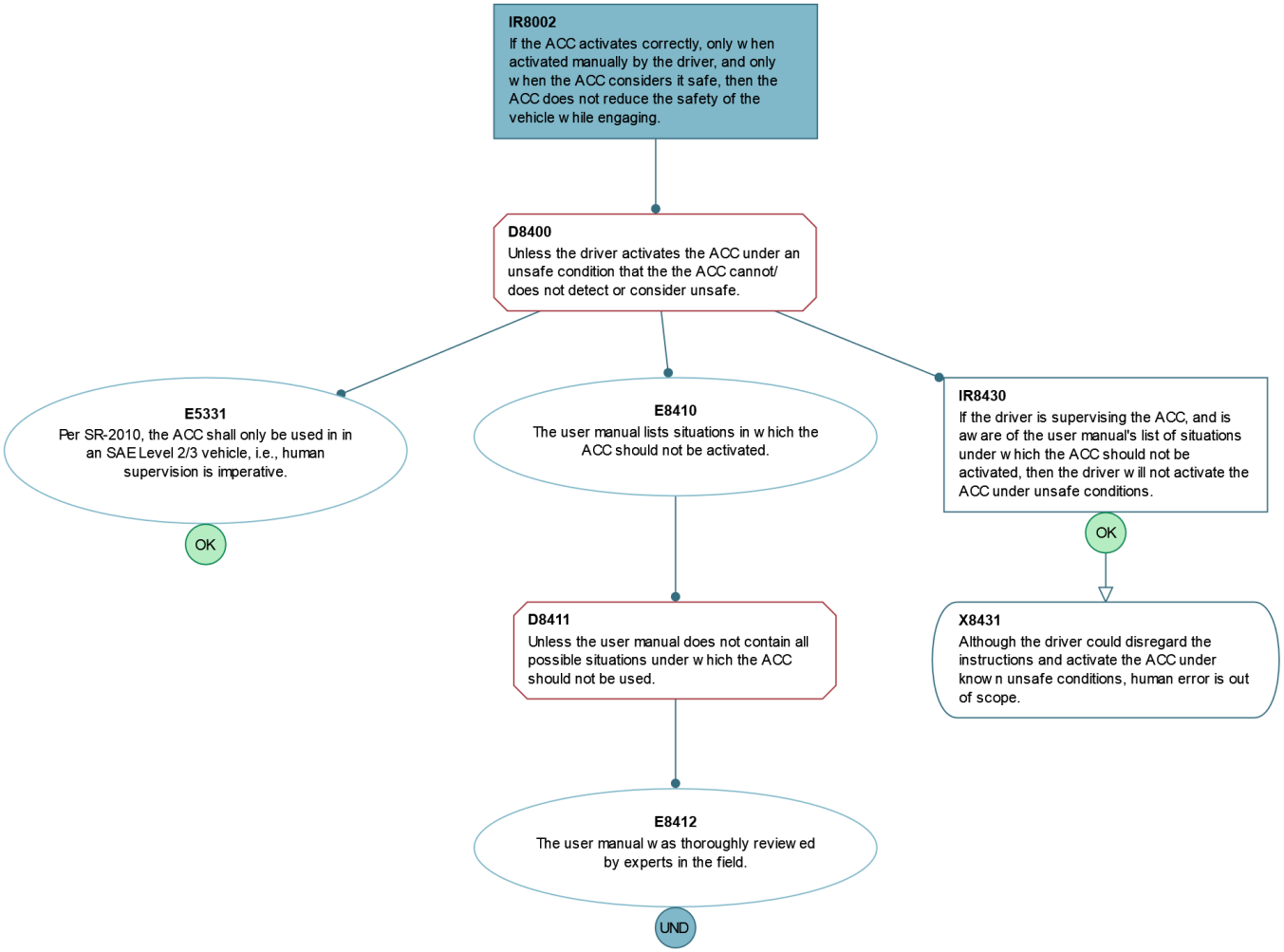
IR7200 - If disengaging causes the ACC to become DISENGAGED, and DISENGAGED does not reduce the safety of the vehicle, then disengaging does not redu...			
Parent subtree(s)	C7000	**Descendant subtree(s)**	None
Description			
Artifacts	E5331: Safety Manual Requirements; C7211: Project Description, User Manual	**Glossary Terms**	None



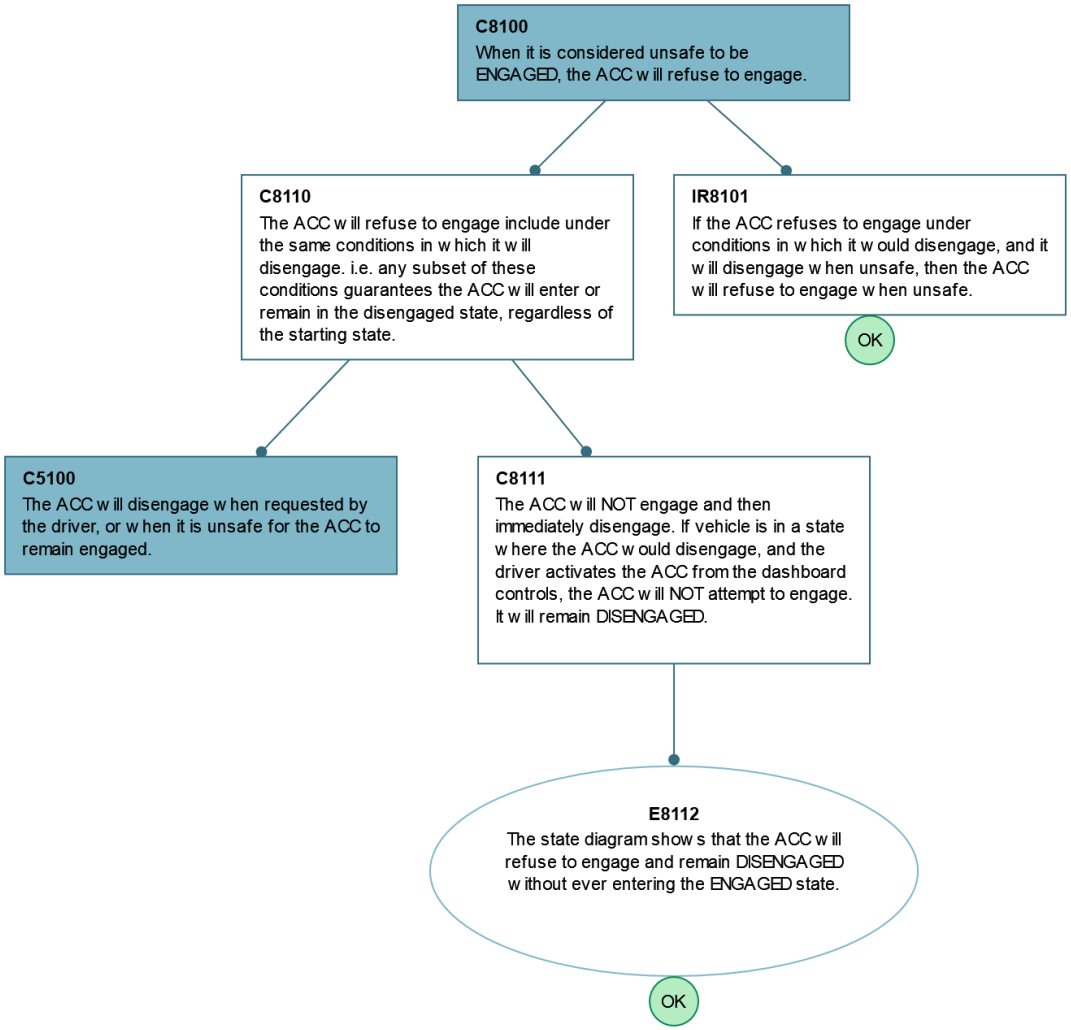
C8000 - The ACC does not reduce the safety of the vehicle while transitioning from DISENGAGED to ENGAGED.			
Parent subtree(s)	C1000	**Descendant subtree(s)**	IR8002, C8100, C8200, C8300
Description			
Artifacts	None	**Glossary Terms**	None



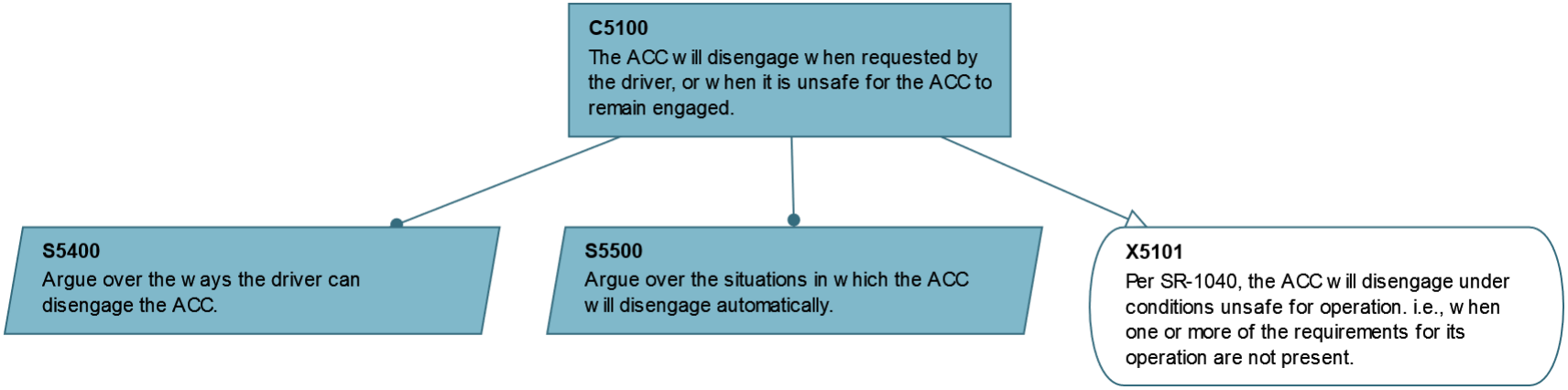
IR8002 - If the ACC activates correctly, only when activated manually by the driver, and only when the ACC considers it safe, then the ACC does not r...			
Parent subtree(s)	C8000	**Descendant subtree(s)**	None
Description			
Artifacts	E5331: Safety Manual Requirements	**Glossary Terms**	None



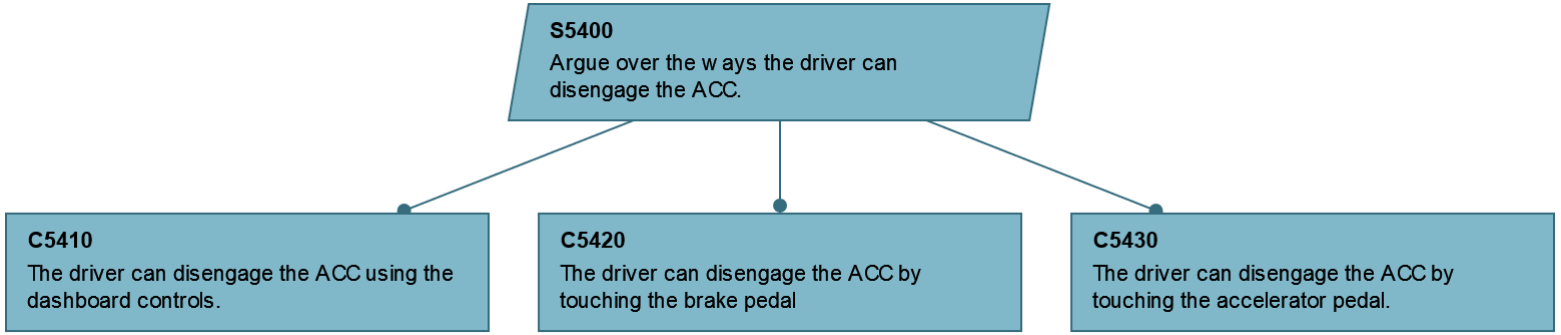
C8100 - When it is considered unsafe to be ENGAGED, the ACC will refuse to engage.			
Parent subtree(s)	C8000	**Descendant subtree(s)**	C5100
Description			
Artifacts	None	**Glossary Terms**	None



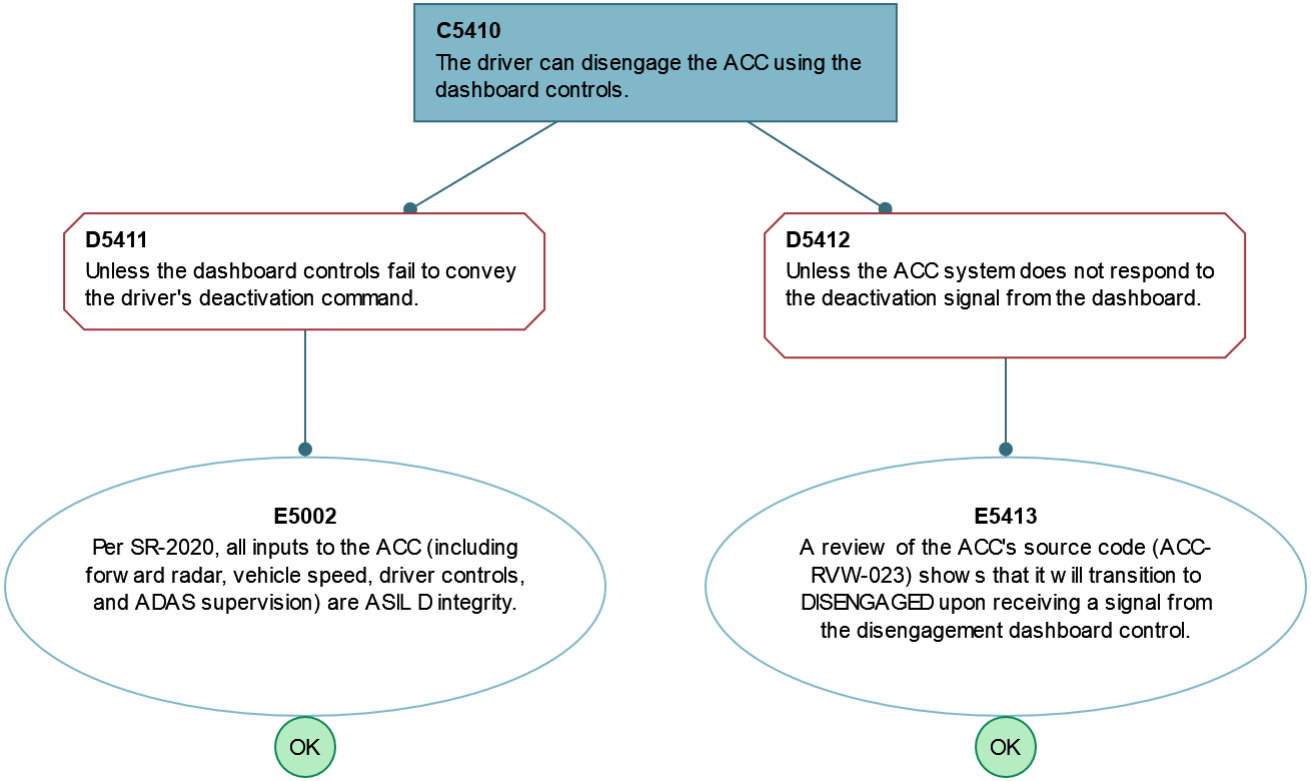
C5100 - The ACC will disengage when requested by the driver, or when it is unsafe for the ACC to remain engaged.			
Parent subtree(s)	C8100, C5000	**Descendant subtree(s)**	S5400, S5500
Description			
Artifacts	None	**Glossary Terms**	None



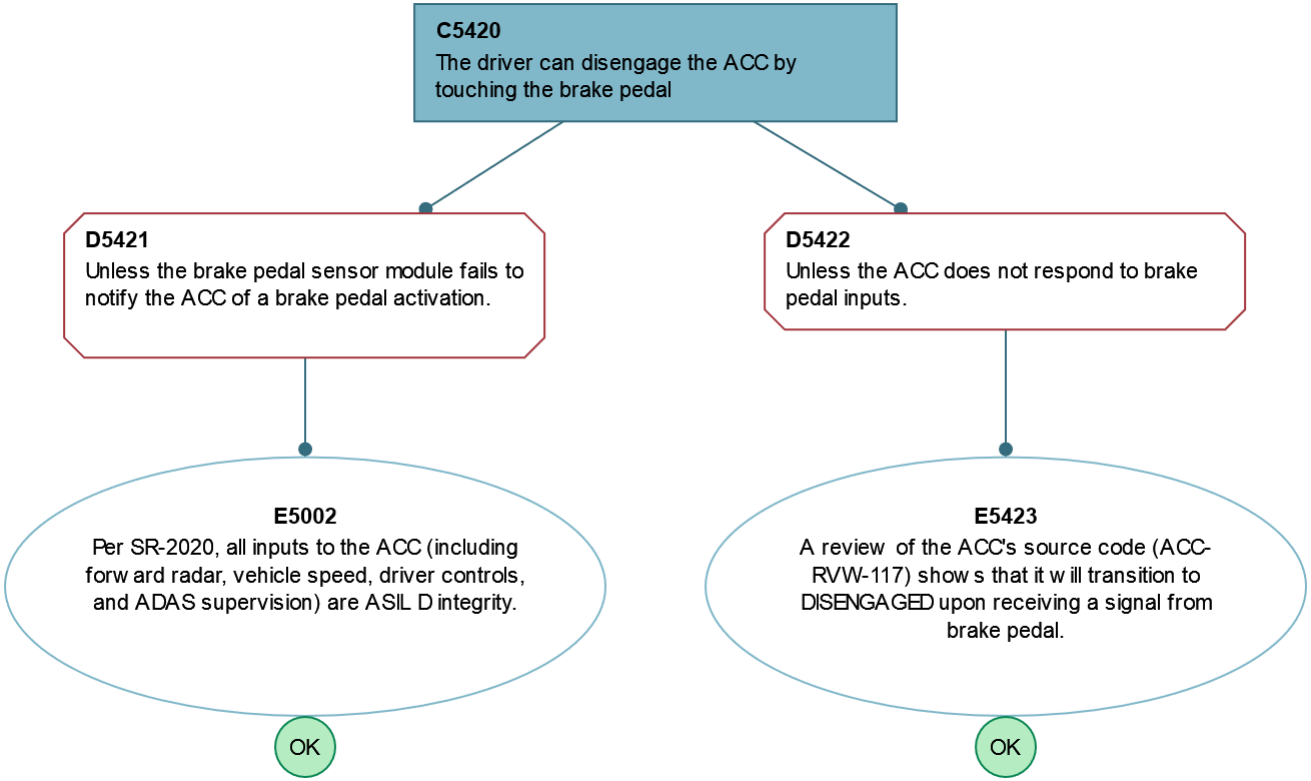
S5400 - Argue over the ways the driver can disengage the ACC.			
Parent subtree(s)	C5100	**Descendant subtree(s)**	C5410, C5420, C5430
Description			
Artifacts	None	**Glossary Terms**	None



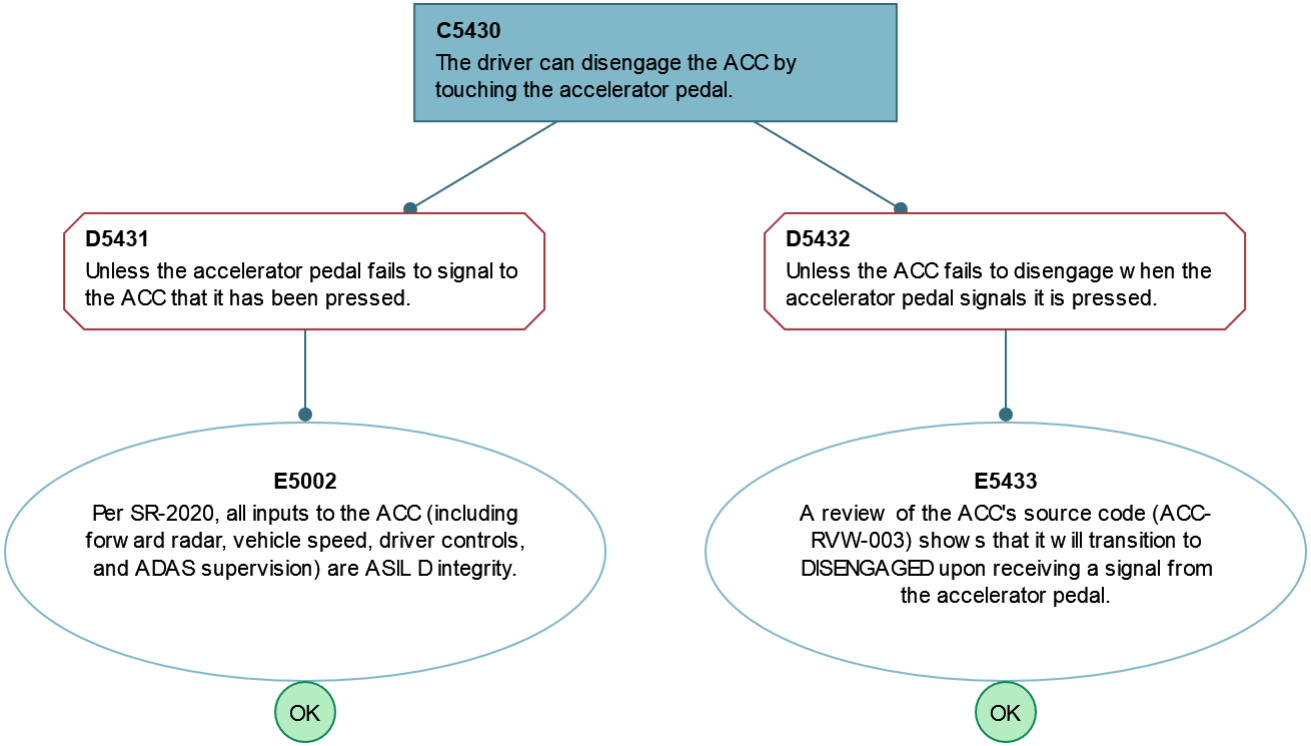
C5410 - The driver can disengage the ACC using the dashboard controls.			
Parent subtree(s)	S5400	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



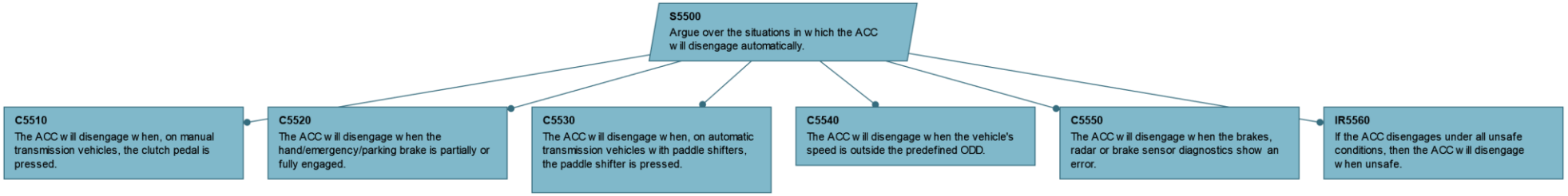
C5420 - The driver can disengage the ACC by touching the brake pedal			
Parent subtree(s)	S5400	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



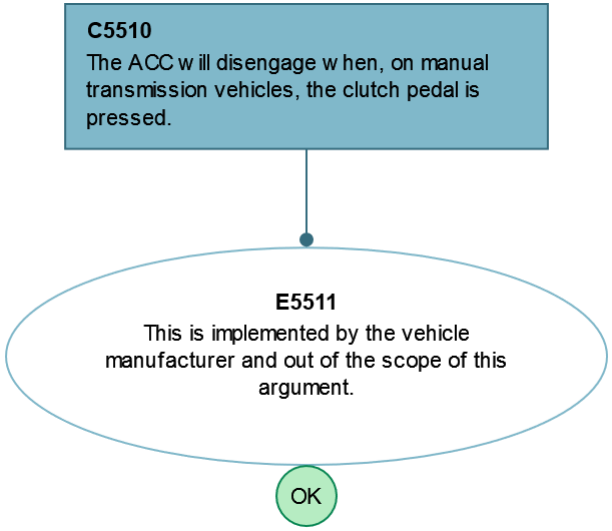
C5430 - The driver can disengage the ACC by touching the accelerator pedal.			
Parent subtree(s)	IR5320, S5400	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



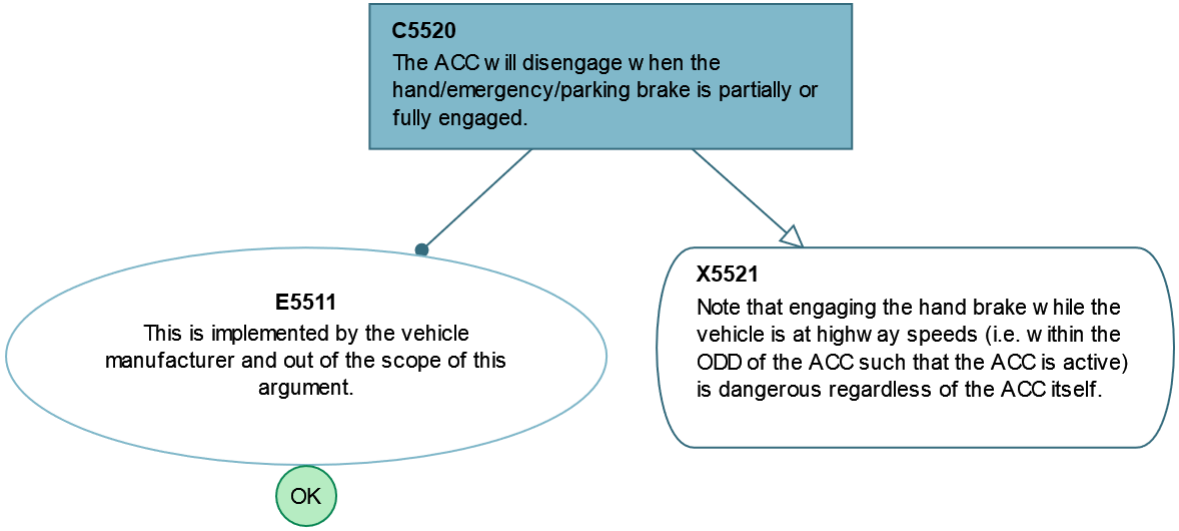
S5500 - Argue over the situations in which the ACC will disengage automatically.			
Parent subtree(s)	C5100	**Descendant subtree(s)**	C5510, C5520, C5530, C5540, C5550, IR5560
Description			
Artifacts	None	**Glossary Terms**	None



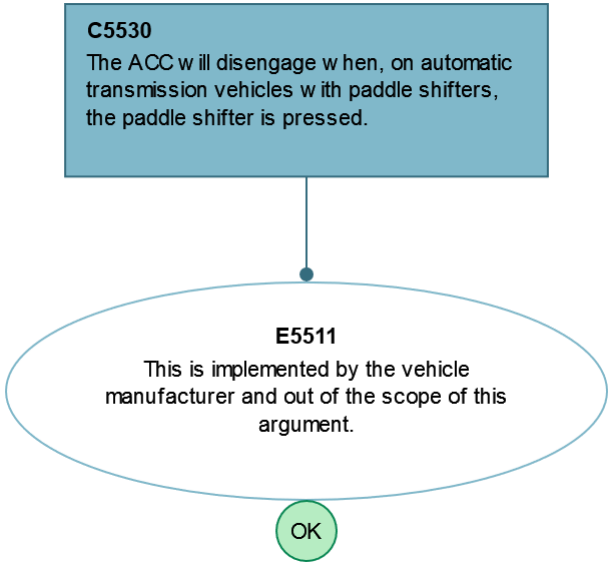
C5510 - The ACC will disengage when, on manual transmission vehicles, the clutch pedal is pressed.			
Parent subtree(s)	S5500	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



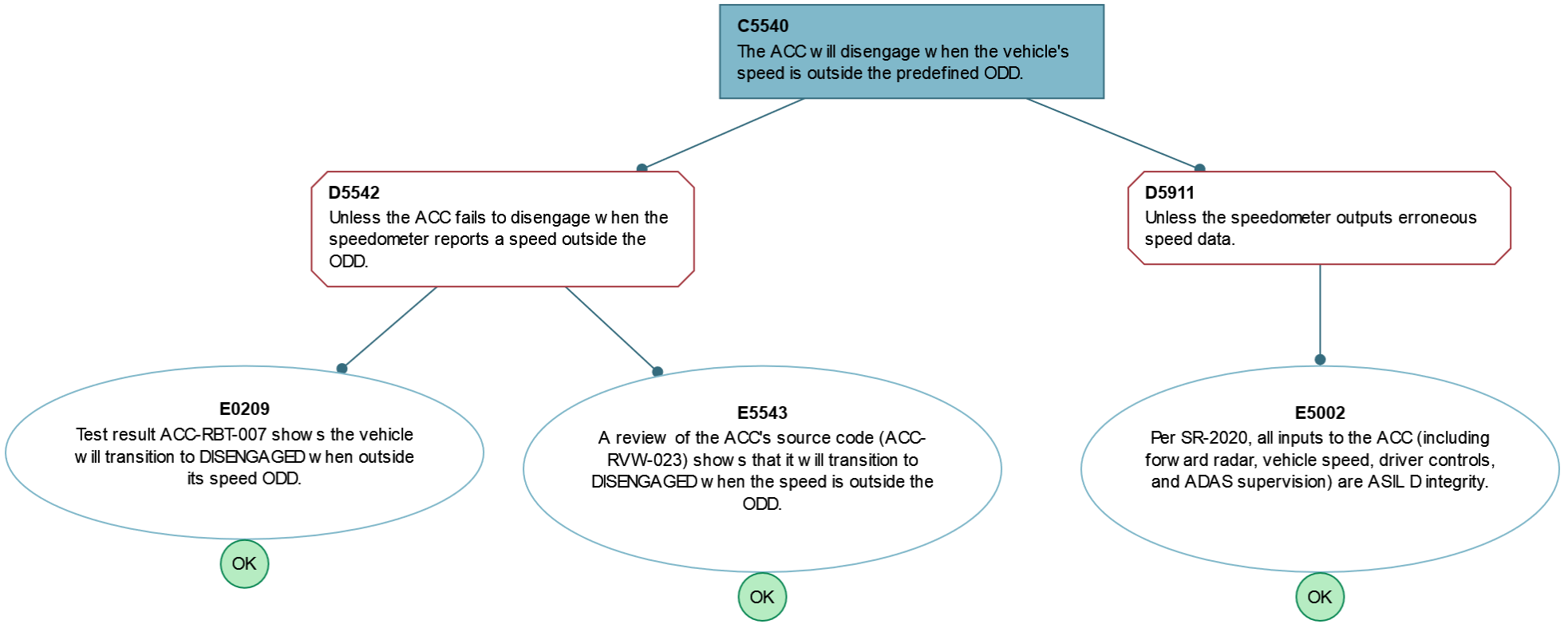
C5520 - The ACC will disengage when the hand/emergency/parking brake is partially or fully engaged.			
Parent subtree(s)	S5500	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



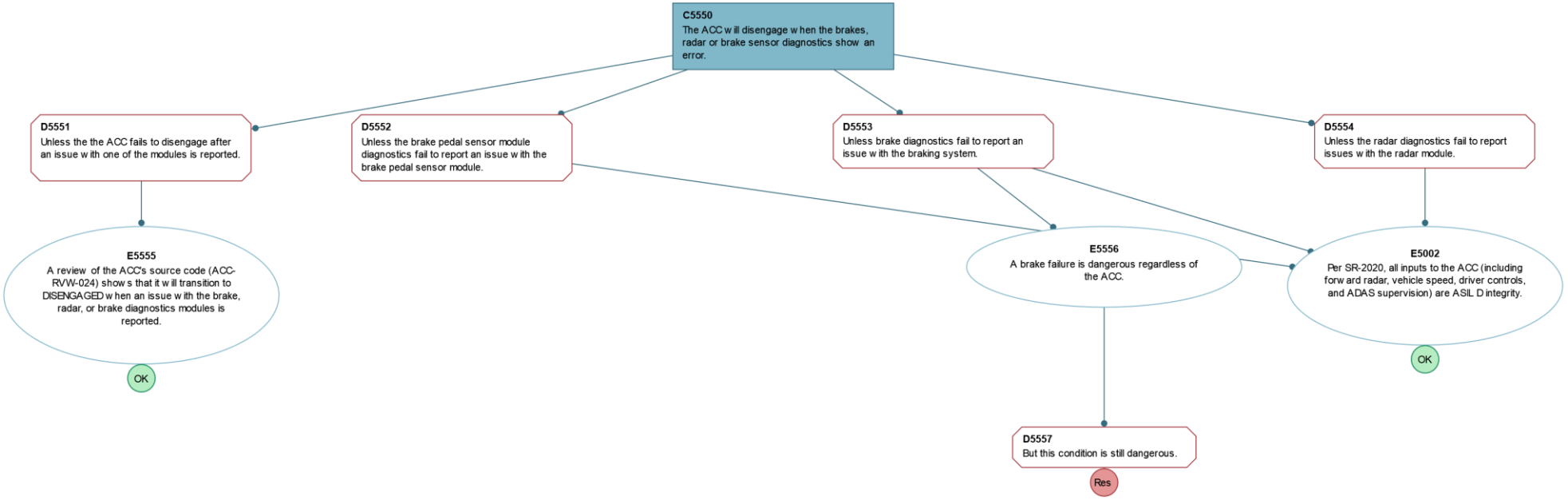
C5530 - The ACC will disengage when, on automatic transmission vehicles with paddle shifters, the paddle shifter is pressed.			
Parent subtree(s)	S5500	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



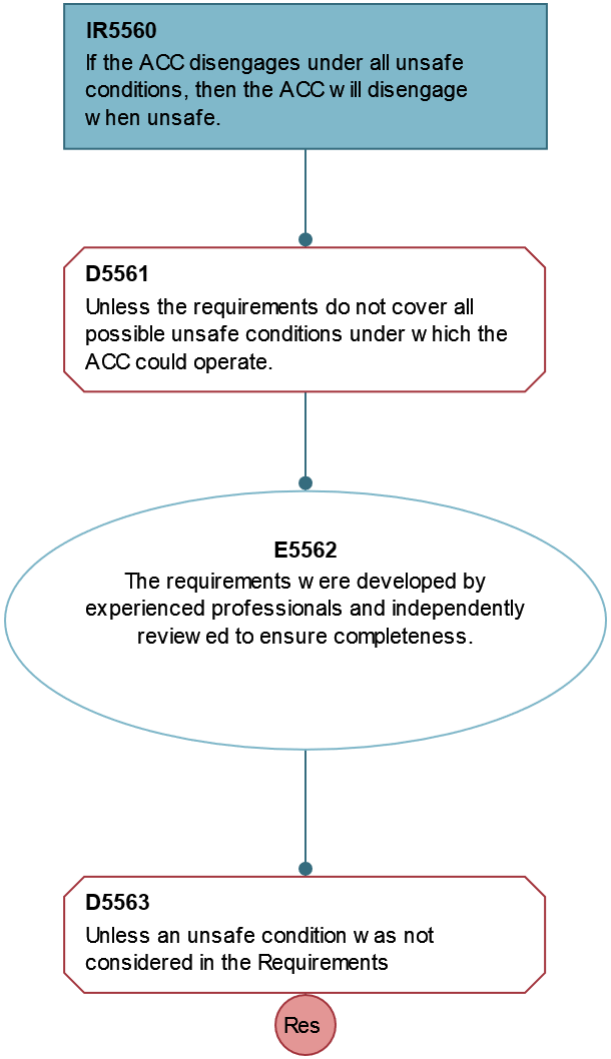
C5540 - The ACC will disengage when the vehicle's speed is outside the predefined ODD.			
Parent subtree(s)	S5500	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



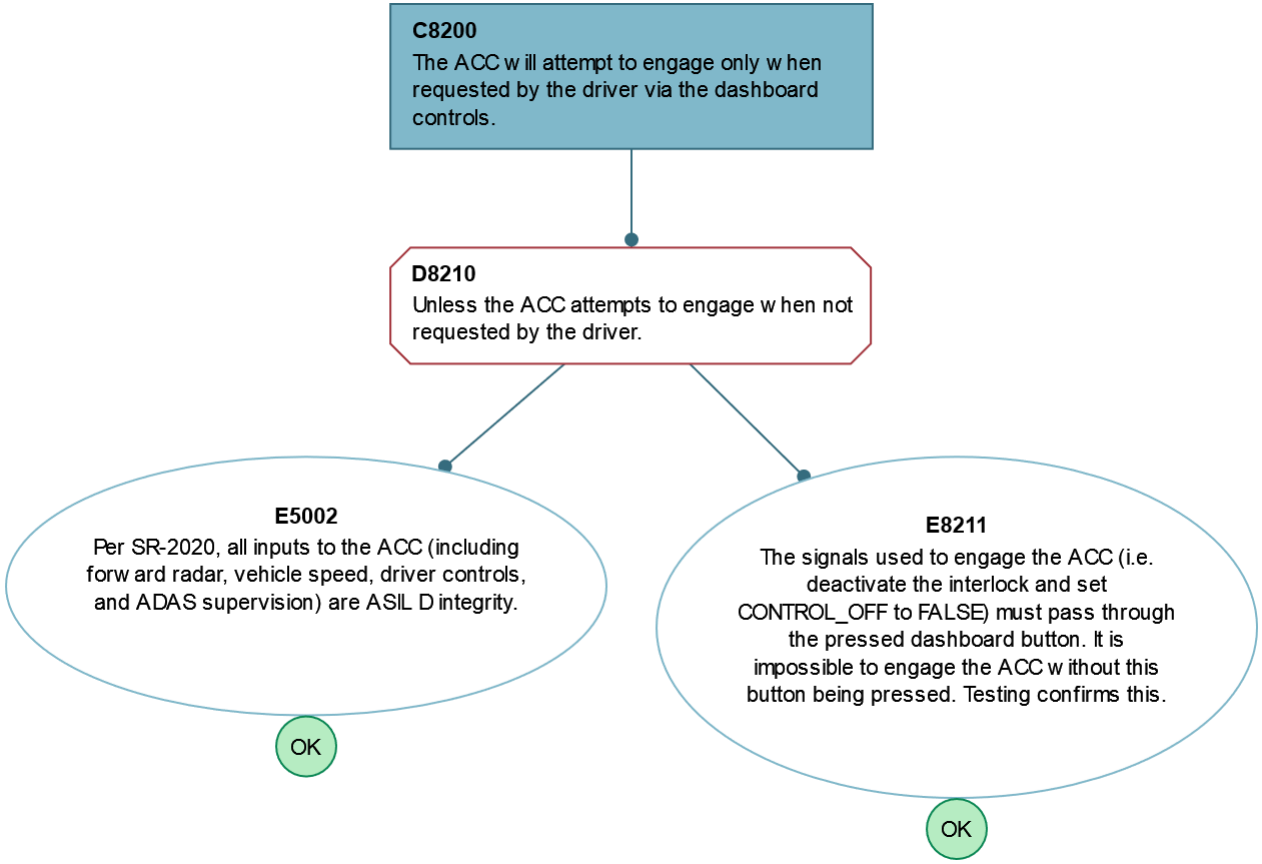
C5550 - The ACC will disengage when the brakes, radar or brake sensor diagnostics show an error.			
Parent subtree(s)	S5500	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



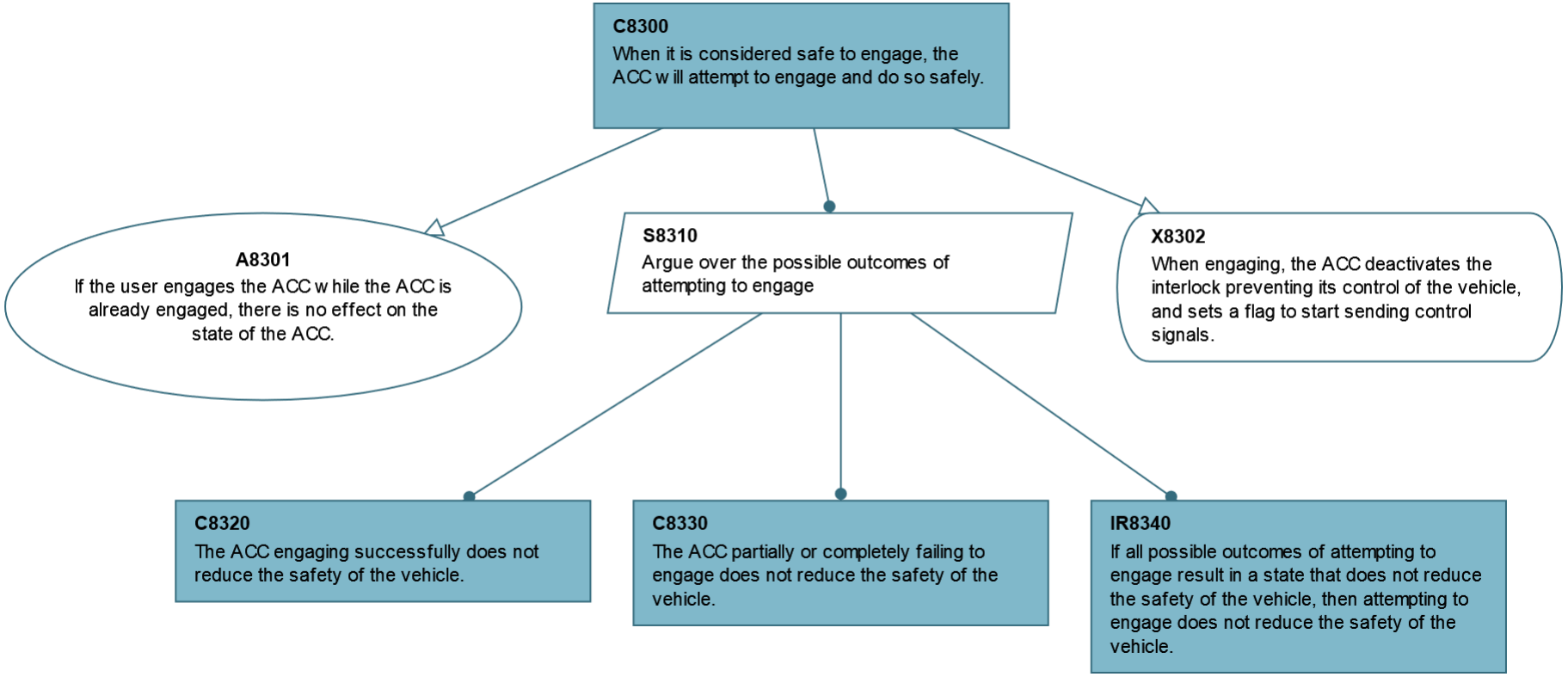
IR5560 - If the ACC disengages under all unsafe conditions, then the ACC will disengage when unsafe.			
Parent subtree(s)	S5500	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



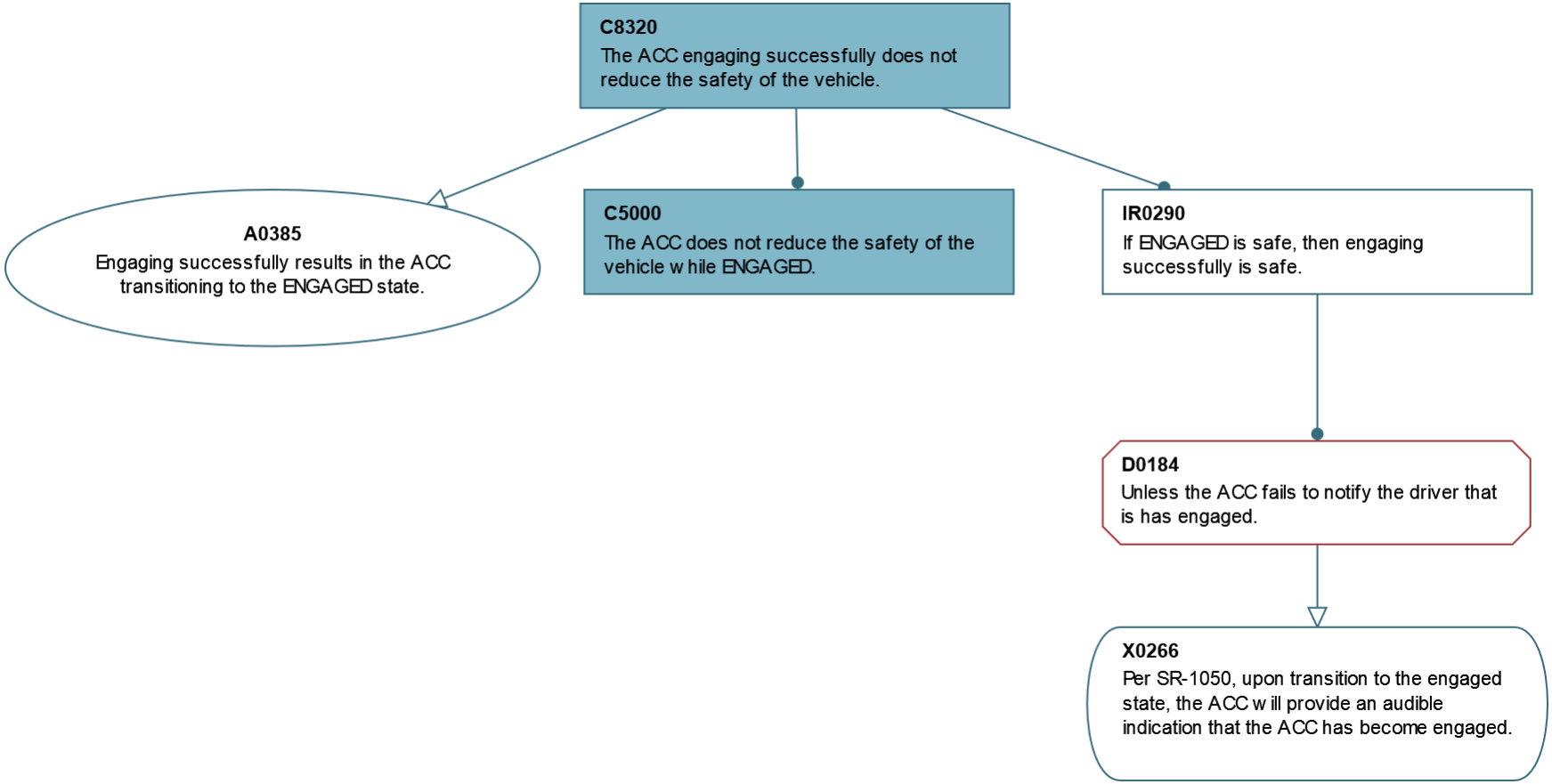
C8200 - The ACC will attempt to engage only when requested by the driver via the dashboard controls.			
Parent subtree(s)	C8000	**Descendant subtree(s)**	None
Description			
Artifacts	E8211: Test Results	**Glossary Terms**	None



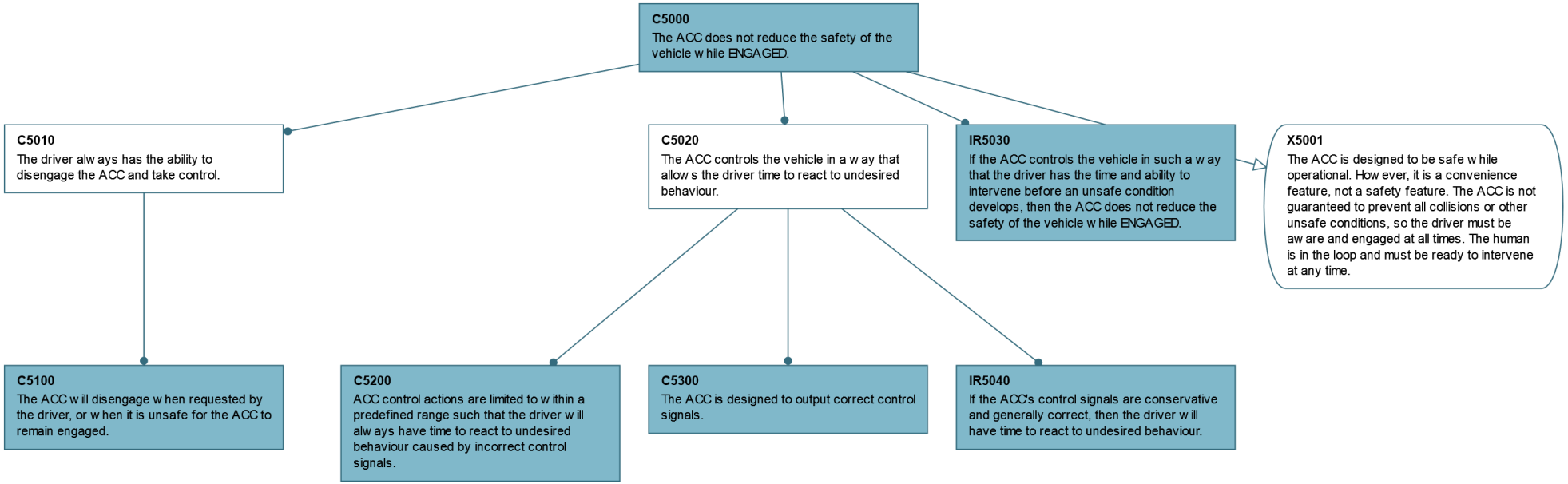
C8300 - When it is considered safe to engage, the ACC will attempt to engage and do so safely.			
Parent subtree(s)	C8000	**Descendant subtree(s)**	C8320, C8330, IR8340
Description			
Artifacts	None	**Glossary Terms**	None



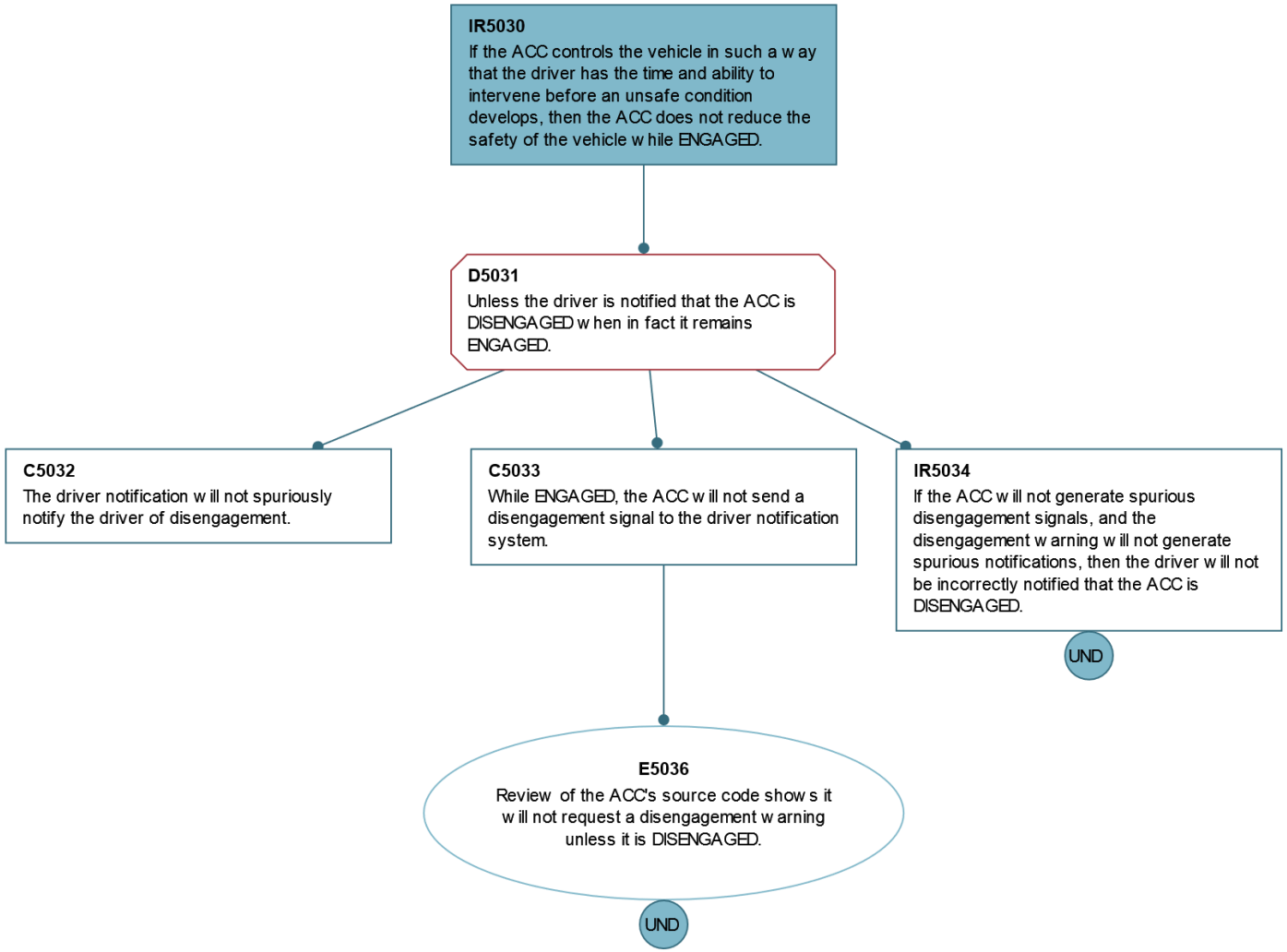
C8320 - The ACC engaging successfully does not reduce the safety of the vehicle.			
Parent subtree(s)	C8300	**Descendant subtree(s)**	C5000
Description			
Artifacts	None	**Glossary Terms**	None



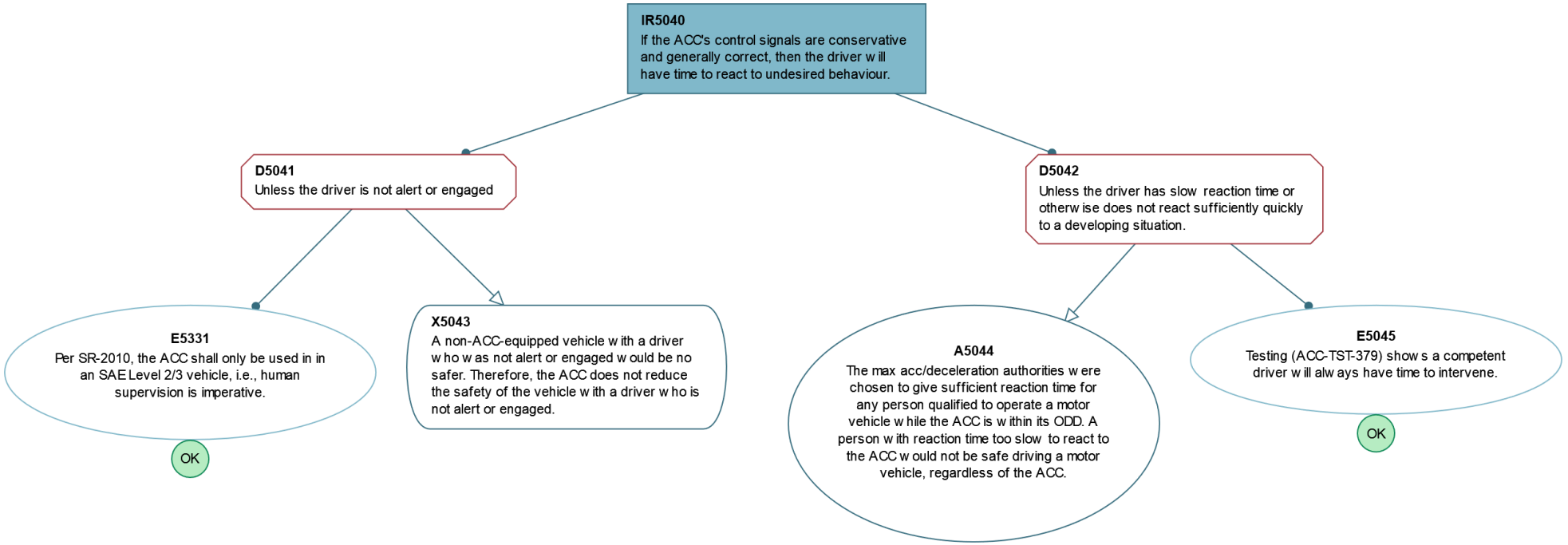
C5000 - The ACC does not reduce the safety of the vehicle while ENGAGED.			
Parent subtree(s)	C1000, C8320	**Descendant subtree(s)**	IR5030, IR5040, C5100, C5200, C5300
Description			
Artifacts	IR5030: Project Description, User Manual	**Glossary Terms**	None



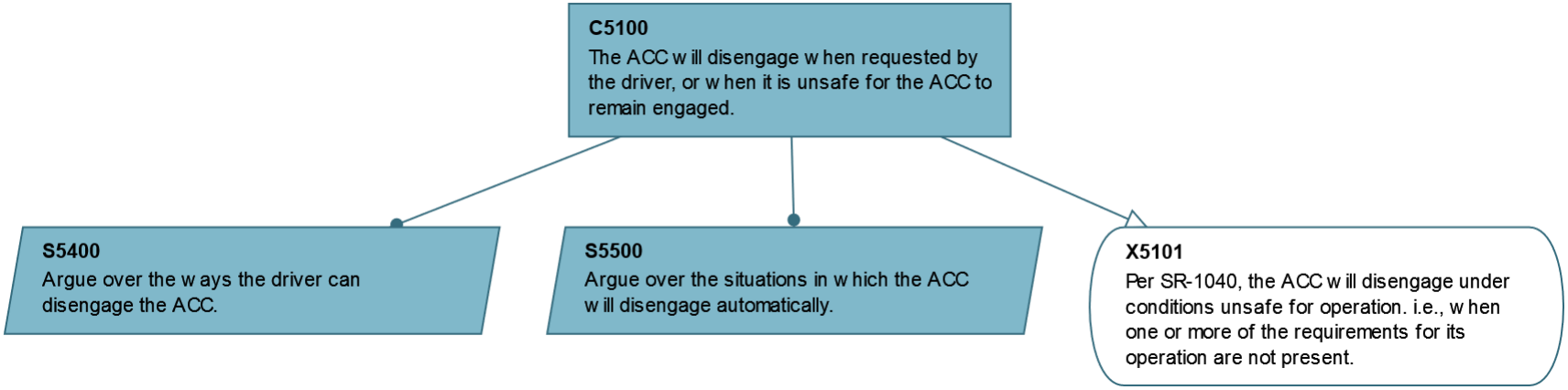
IR5030 - If the ACC controls the vehicle in such a way that the driver has the time and ability to intervene before an unsafe condition develops, the...			
Parent subtree(s)	C5000	**Descendant subtree(s)**	None
Description			
Artifacts	IR5030: Project Description, User Manual	**Glossary Terms**	None



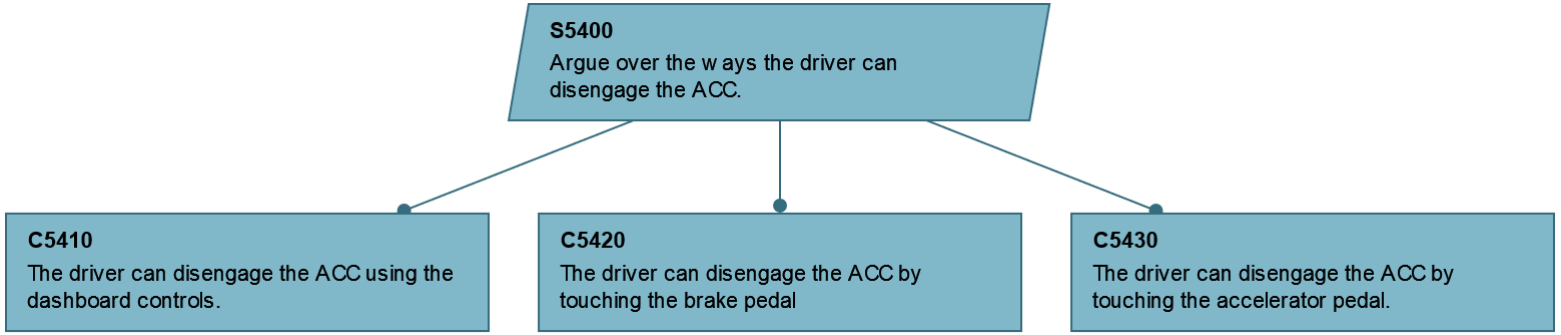
IR5040 - If the ACC's control signals are conservative and generally correct, then the driver will have time to react to undesired behaviour.			
Parent subtree(s)	C5000	**Descendant subtree(s)**	None
Description			
Artifacts	X5043: Project Description; E5331: Safety Manual Requirements	**Glossary Terms**	None



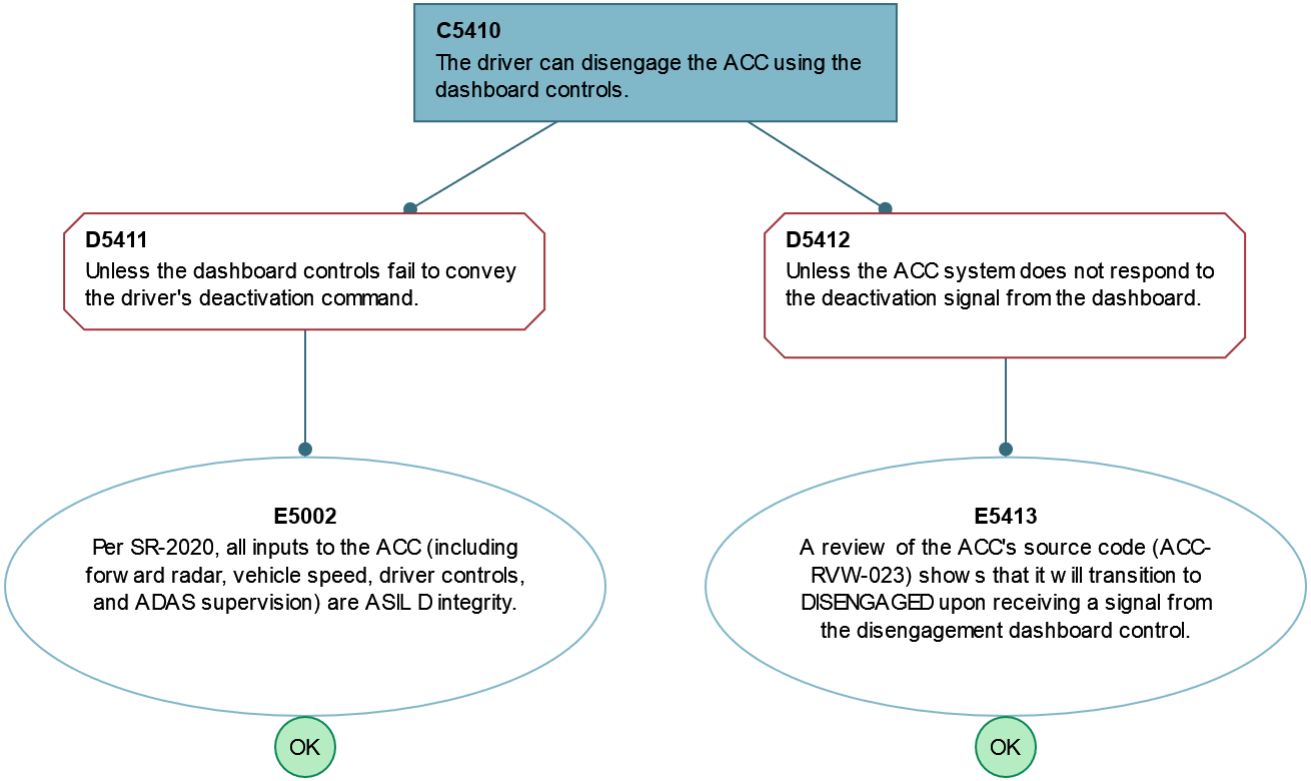
C5100 - The ACC will disengage when requested by the driver, or when it is unsafe for the ACC to remain engaged.			
Parent subtree(s)	C8100, C5000	**Descendant subtree(s)**	S5400, S5500
Description			
Artifacts	None	**Glossary Terms**	None



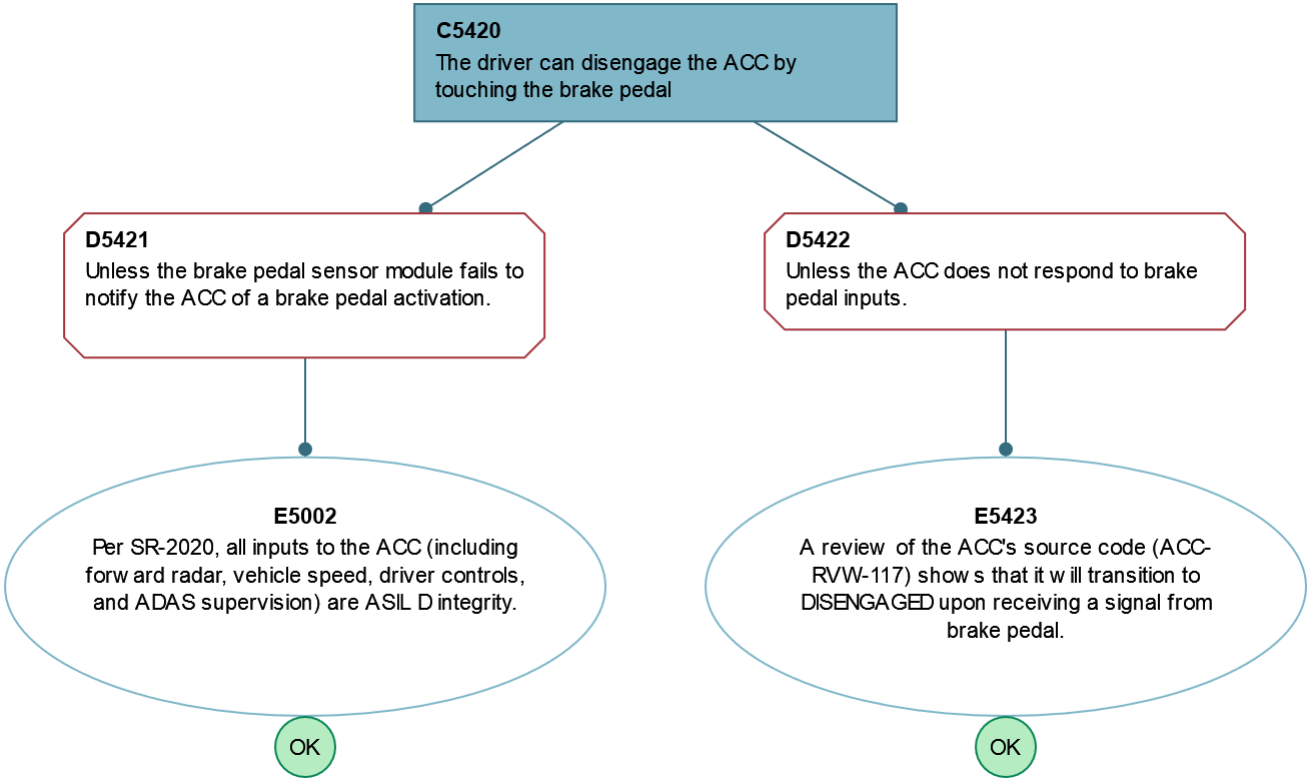
S5400 - Argue over the ways the driver can disengage the ACC.			
Parent subtree(s)	C5100	**Descendant subtree(s)**	C5410, C5420, C5430
Description			
Artifacts	None	**Glossary Terms**	None



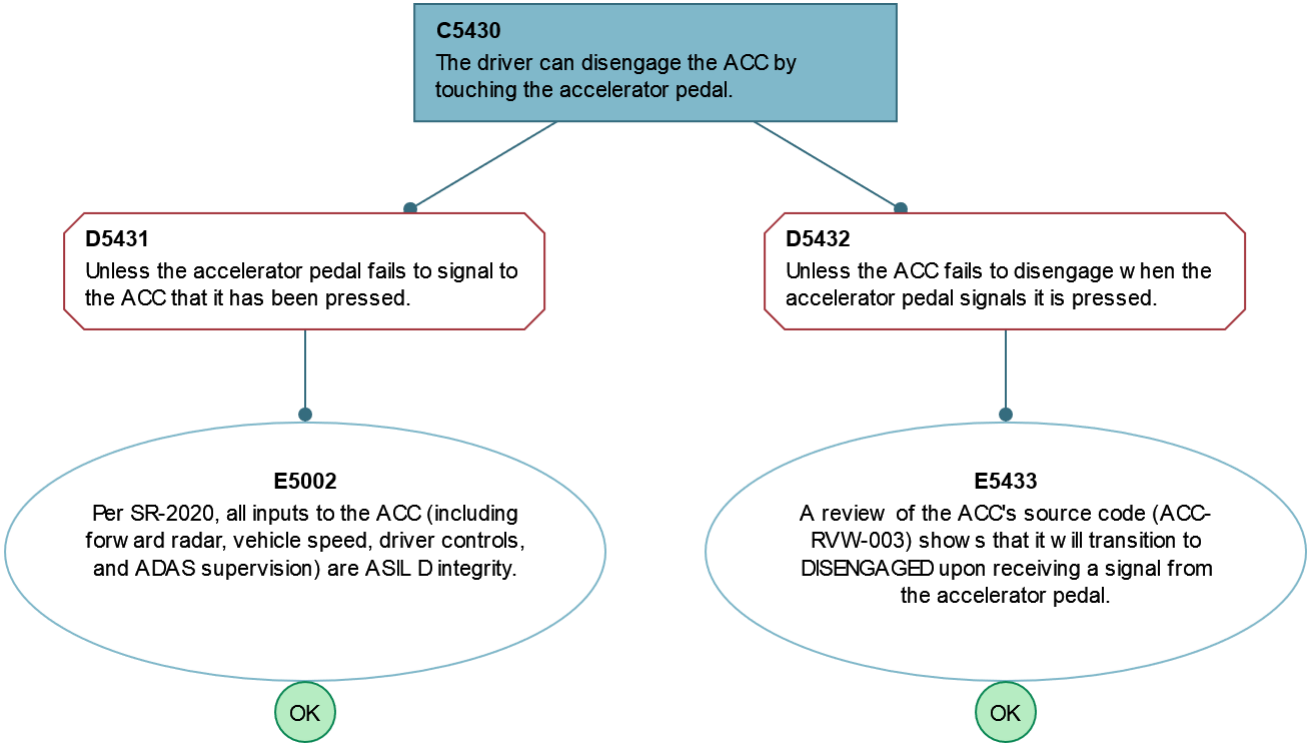
C5410 - The driver can disengage the ACC using the dashboard controls.			
Parent subtree(s)	S5400	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



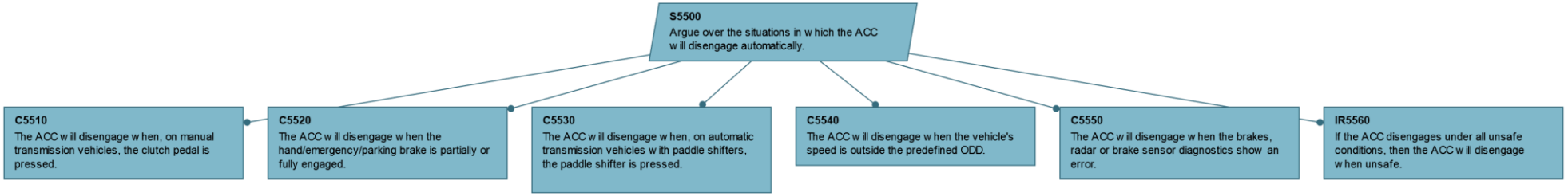
C5420 - The driver can disengage the ACC by touching the brake pedal			
Parent subtree(s)	S5400	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



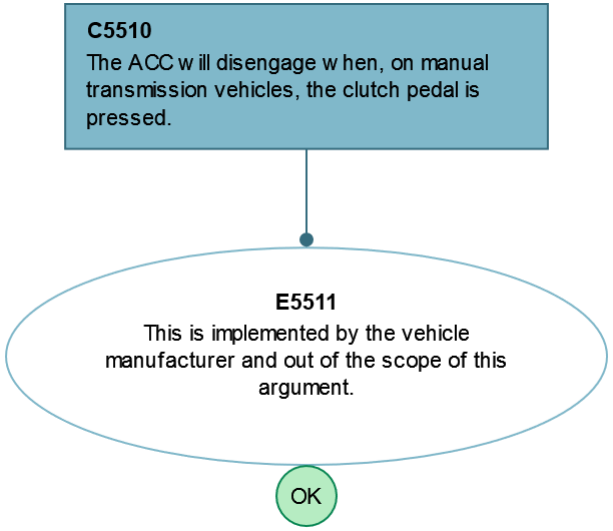
C5430 - The driver can disengage the ACC by touching the accelerator pedal.			
Parent subtree(s)	IR5320, S5400	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



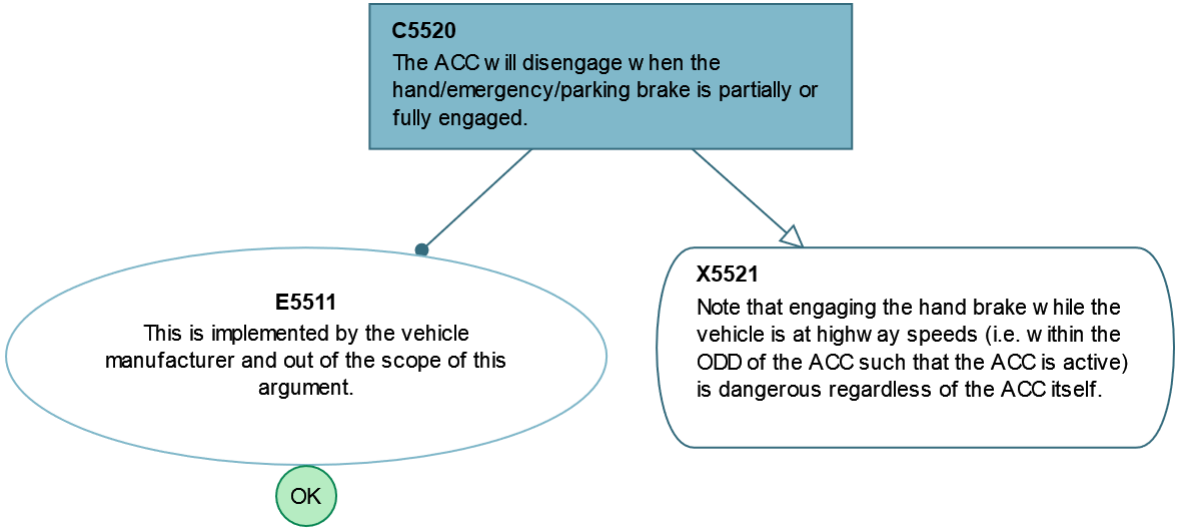
S5500 - Argue over the situations in which the ACC will disengage automatically.			
Parent subtree(s)	C5100	**Descendant subtree(s)**	C5510, C5520, C5530, C5540, C5550, IR5560
Description			
Artifacts	None	**Glossary Terms**	None



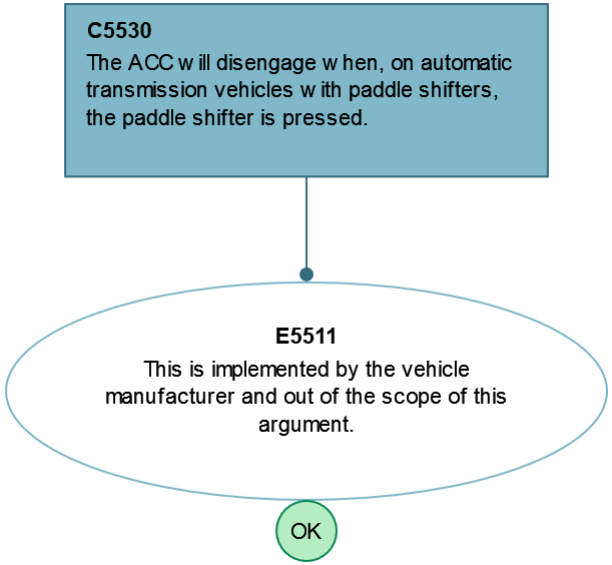
C5510 - The ACC will disengage when, on manual transmission vehicles, the clutch pedal is pressed.			
Parent subtree(s)	S5500	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



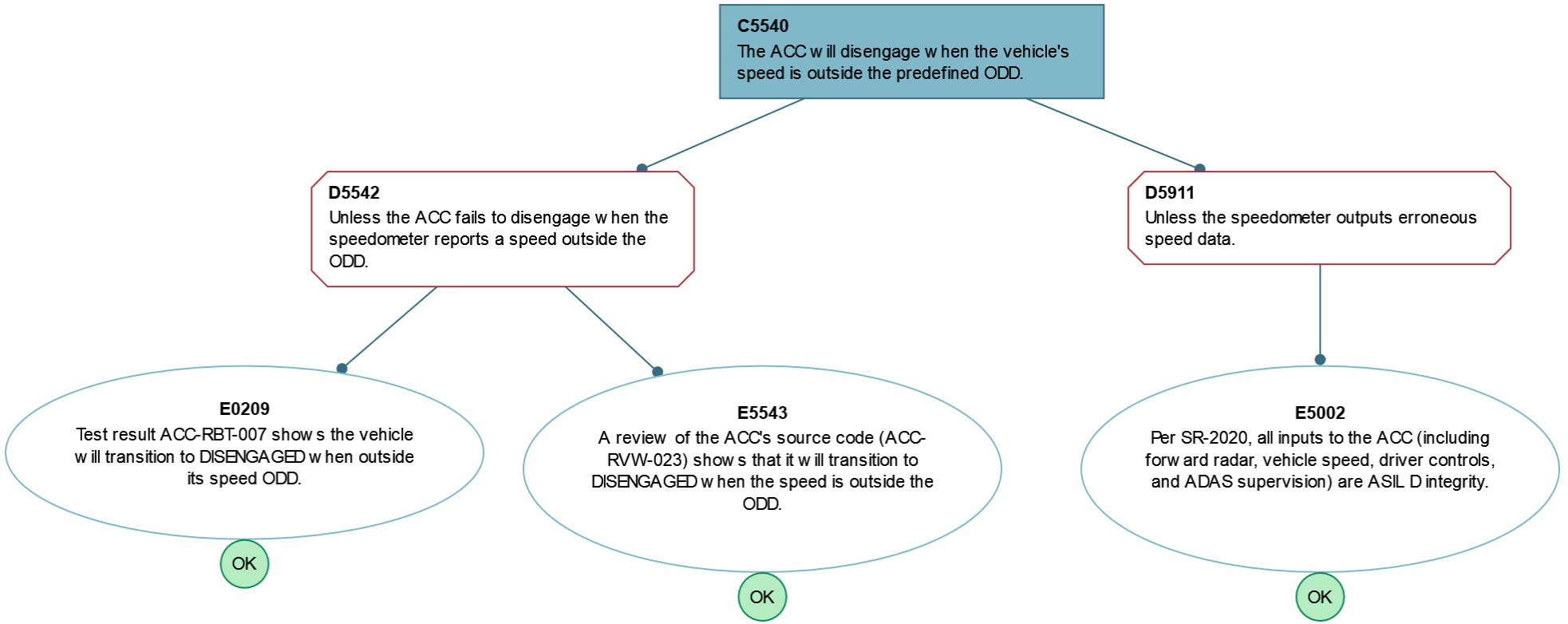
C5520 - The ACC will disengage when the hand/emergency/parking brake is partially or fully engaged.			
Parent subtree(s)	S5500	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



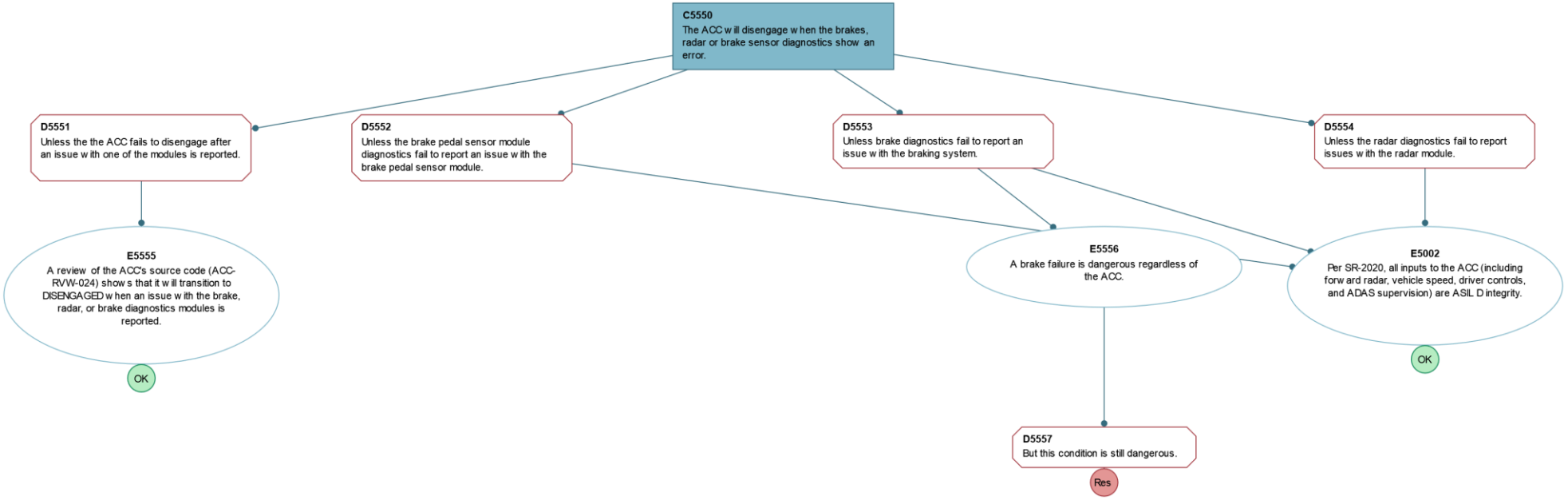
C5530 - The ACC will disengage when, on automatic transmission vehicles with paddle shifters, the paddle shifter is pressed.			
Parent subtree(s)	S5500	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



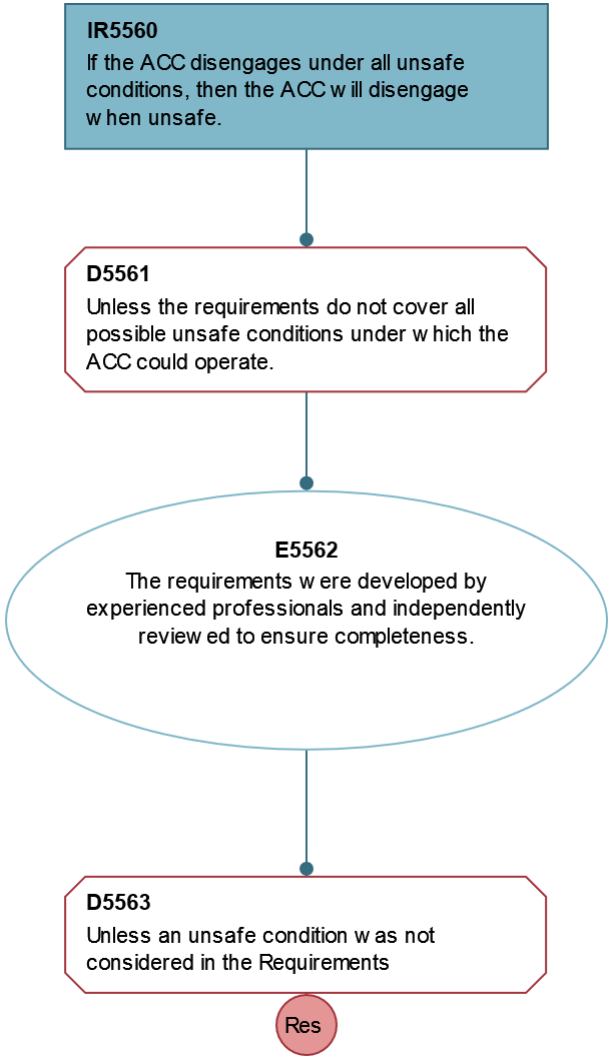
C5540 - The ACC will disengage when the vehicle's speed is outside the predefined ODD.			
Parent subtree(s)	S5500	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



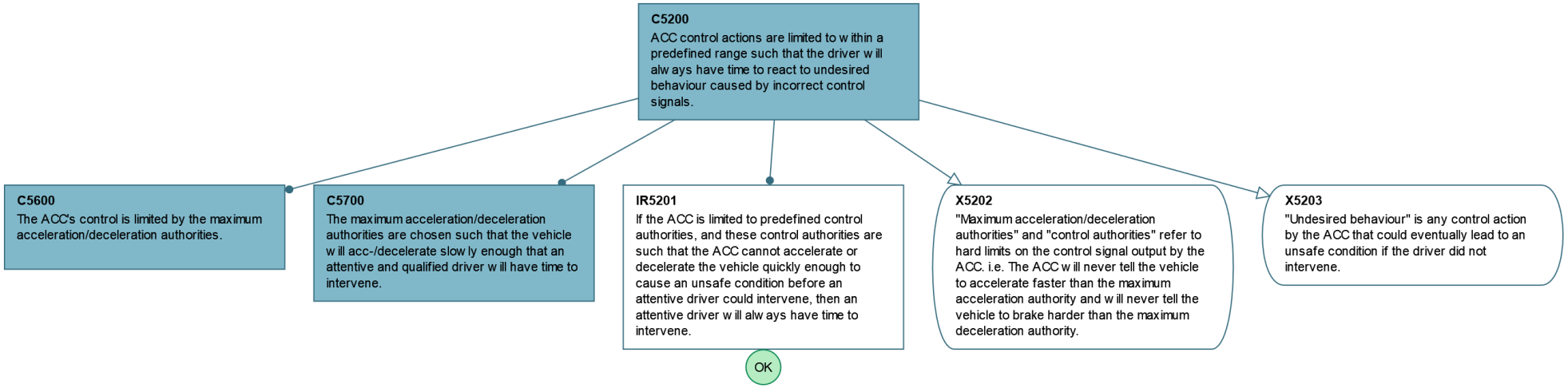
C5550 - The ACC will disengage when the brakes, radar or brake sensor diagnostics show an error.			
Parent subtree(s)	S5500	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



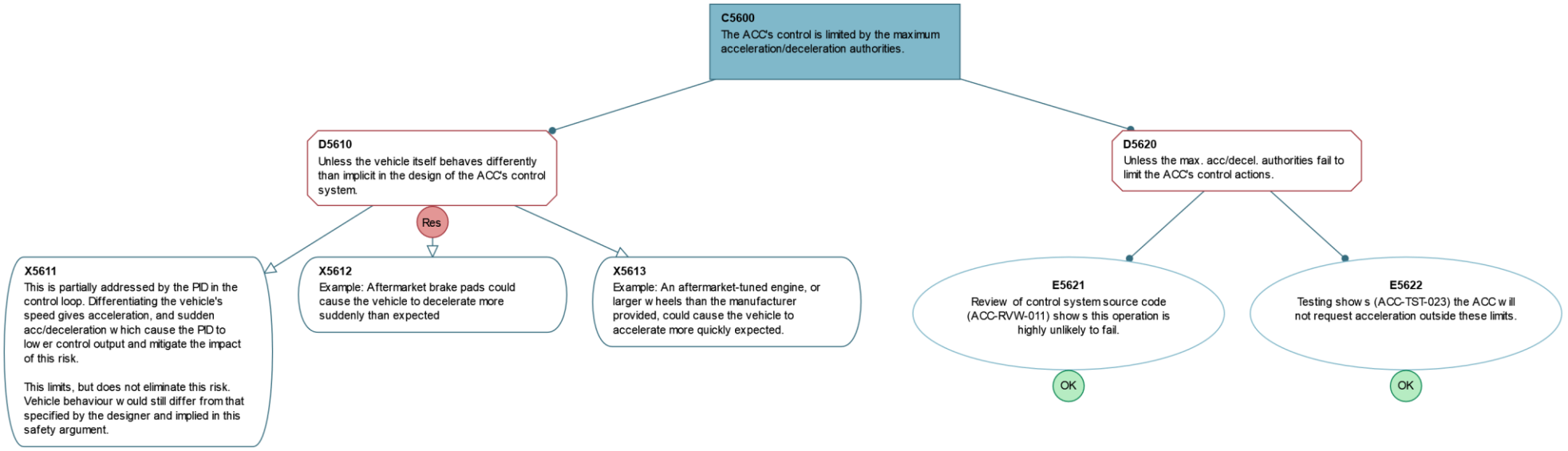
IR5560 - If the ACC disengages under all unsafe conditions, then the ACC will disengage when unsafe.			
Parent subtree(s)	S5500	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



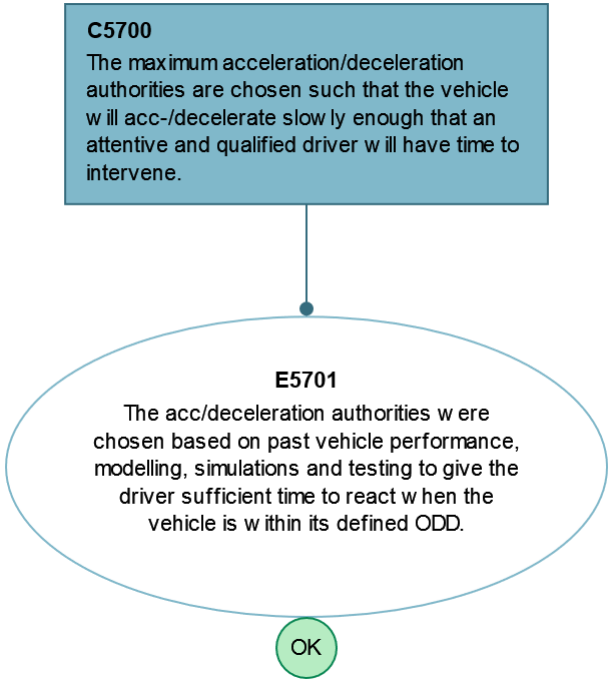
C5200 - ACC control actions are limited to within a predefined range such that the driver will always have time to react to undesired behaviour caus...			
Parent subtree(s)	C5000	**Descendant subtree(s)**	C5600, C5700
Description			
Artifacts	None	**Glossary Terms**	None



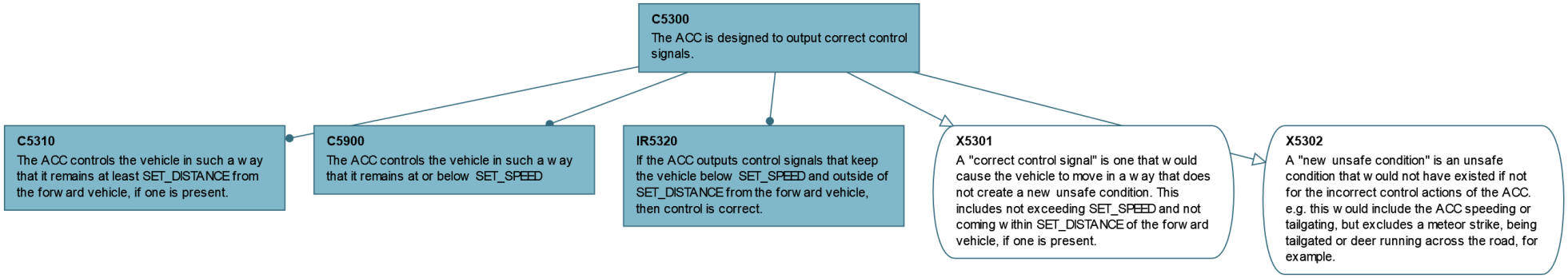
C5600 - The ACC's control is limited by the maximum acceleration/deceleration authorities.			
Parent subtree(s)	C5200	**Descendant subtree(s)**	None
Description			
Artifacts	E5621: Max Acceleration-Deceleration Authority FTA; E5622: Test Results	**Glossary Terms**	None



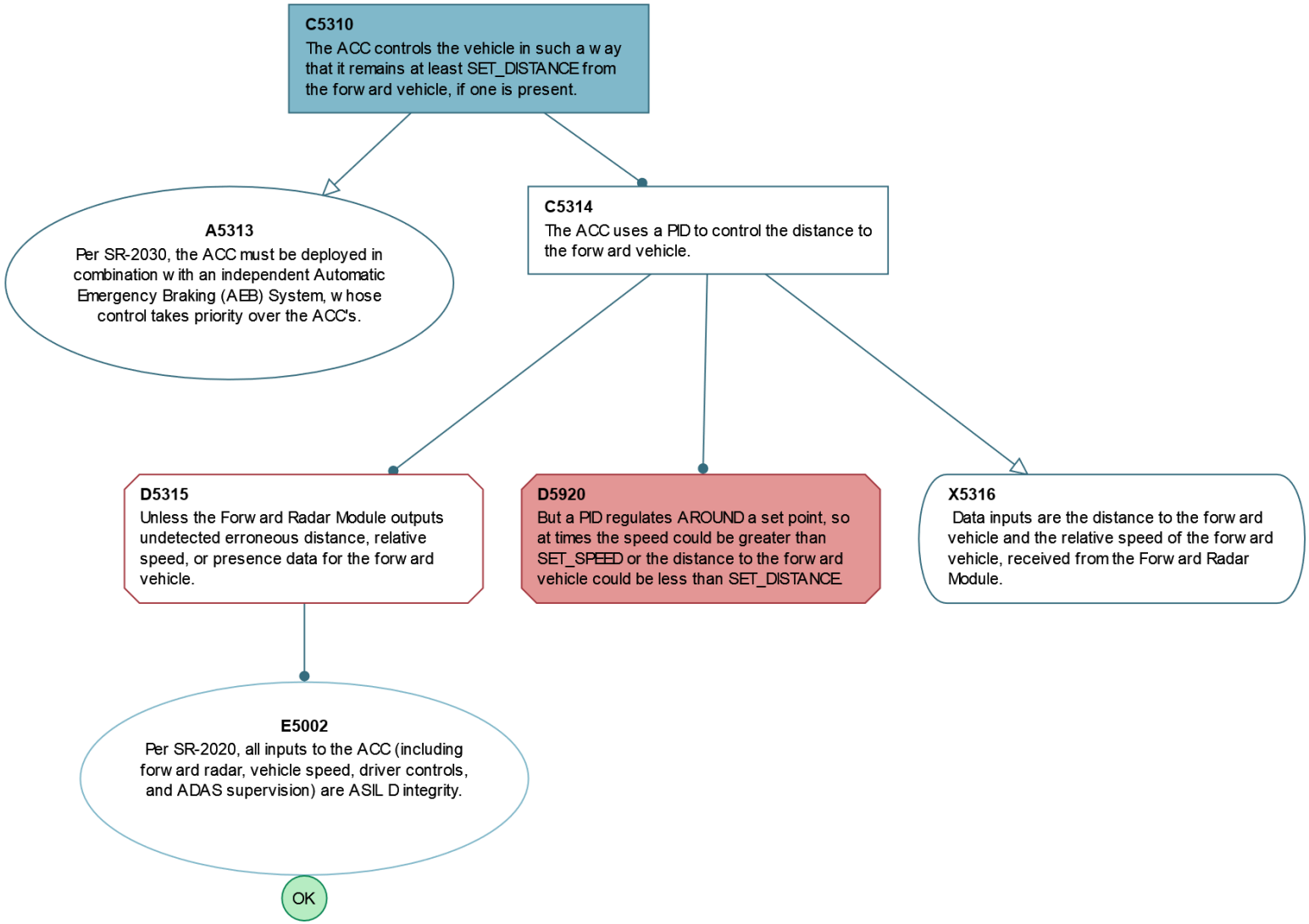
C5700 - The maximum acceleration/deceleration authorities are chosen such that the vehicle will acc-/decelerate slowly enough that an attentive and ...			
Parent subtree(s)	C5200	**Descendant subtree(s)**	None
Description			
Artifacts	E5701: Test Results	**Glossary Terms**	None



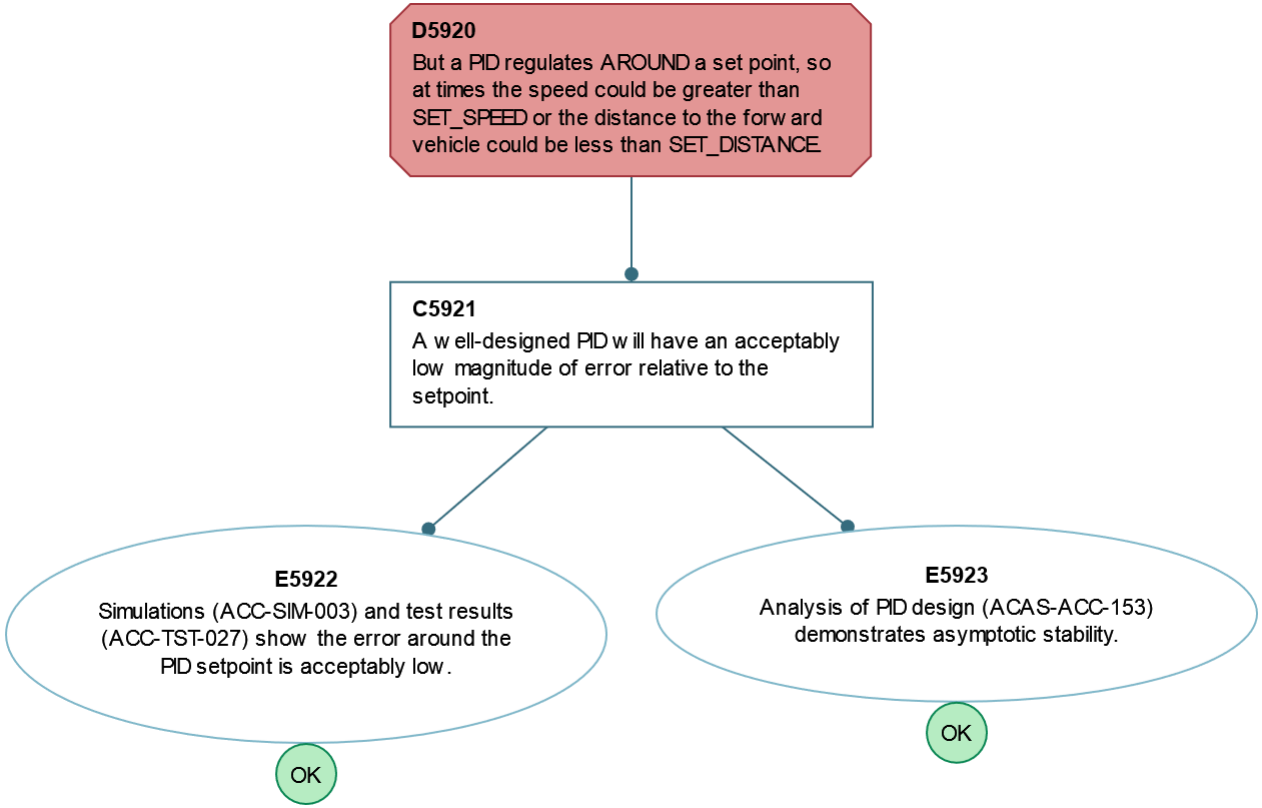
C5300 - The ACC is designed to output correct control signals.			
Parent subtree(s)	C5000	**Descendant subtree(s)**	C5310, IR5320, C5900
Description			
Artifacts	None	**Glossary Terms**	None



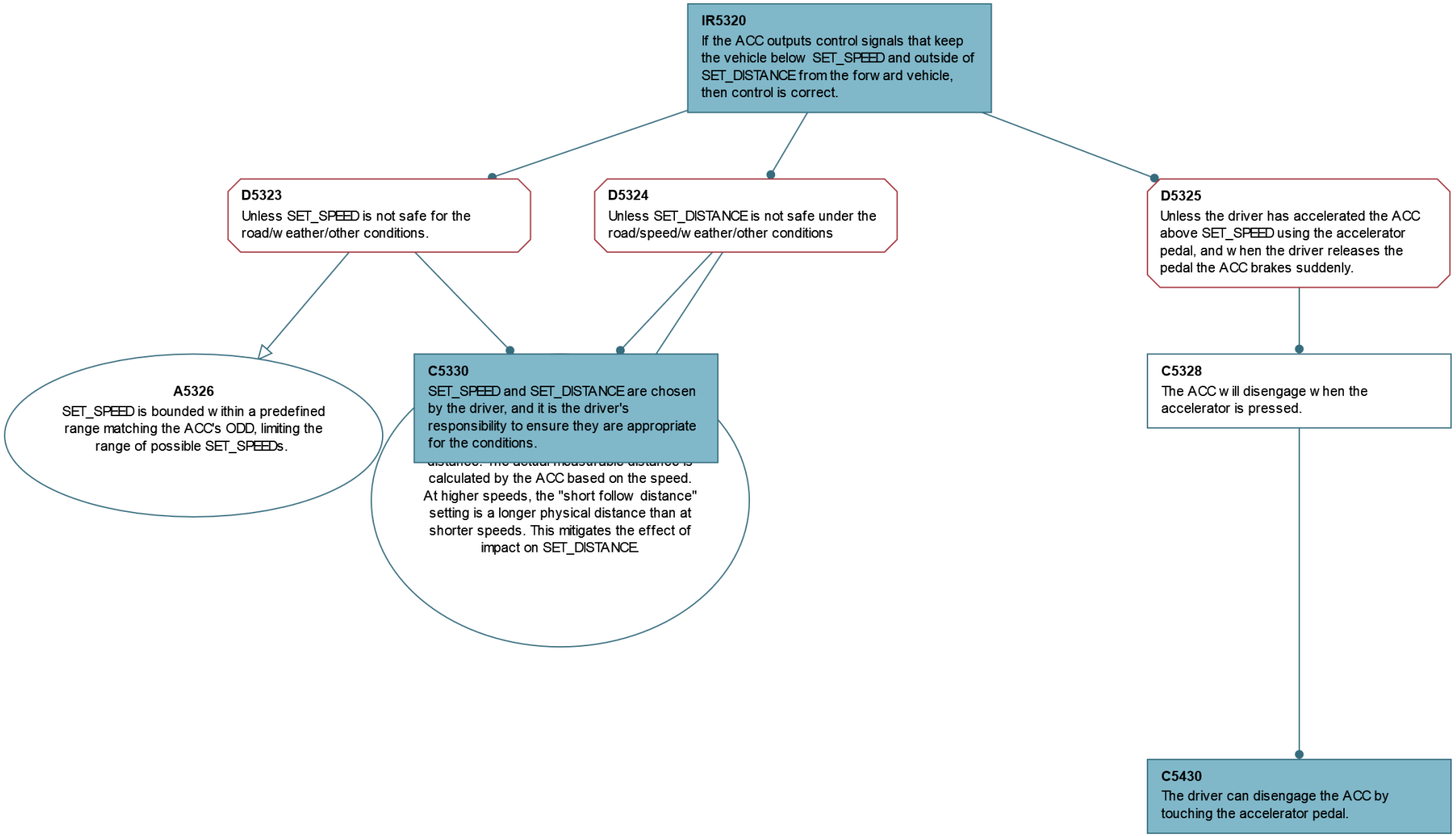
C5310 - The ACC controls the vehicle in such a way that it remains at least SET_DISTANCE from the forward vehicle, if one is present.			
Parent subtree(s)	C5300	**Descendant subtree(s)**	D5920
Description			
Artifacts	None	**Glossary Terms**	None



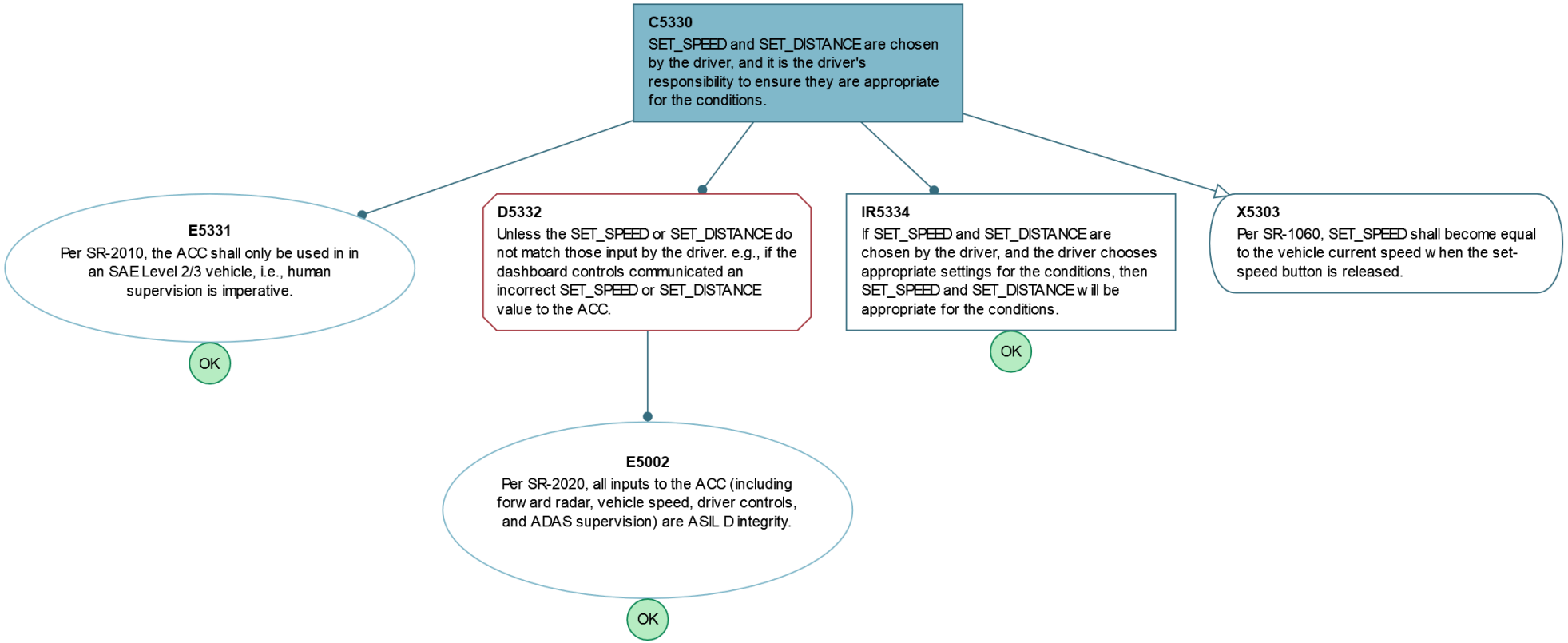
D5920 - But a PID regulates AROUND a set point, so at times the speed could be greater than SET_SPEED or the distance to the forward vehicle could b...			
Parent subtree(s)	C5310, C5900	**Descendant subtree(s)**	None
Description			
Artifacts	E5922: Test Results	**Glossary Terms**	None



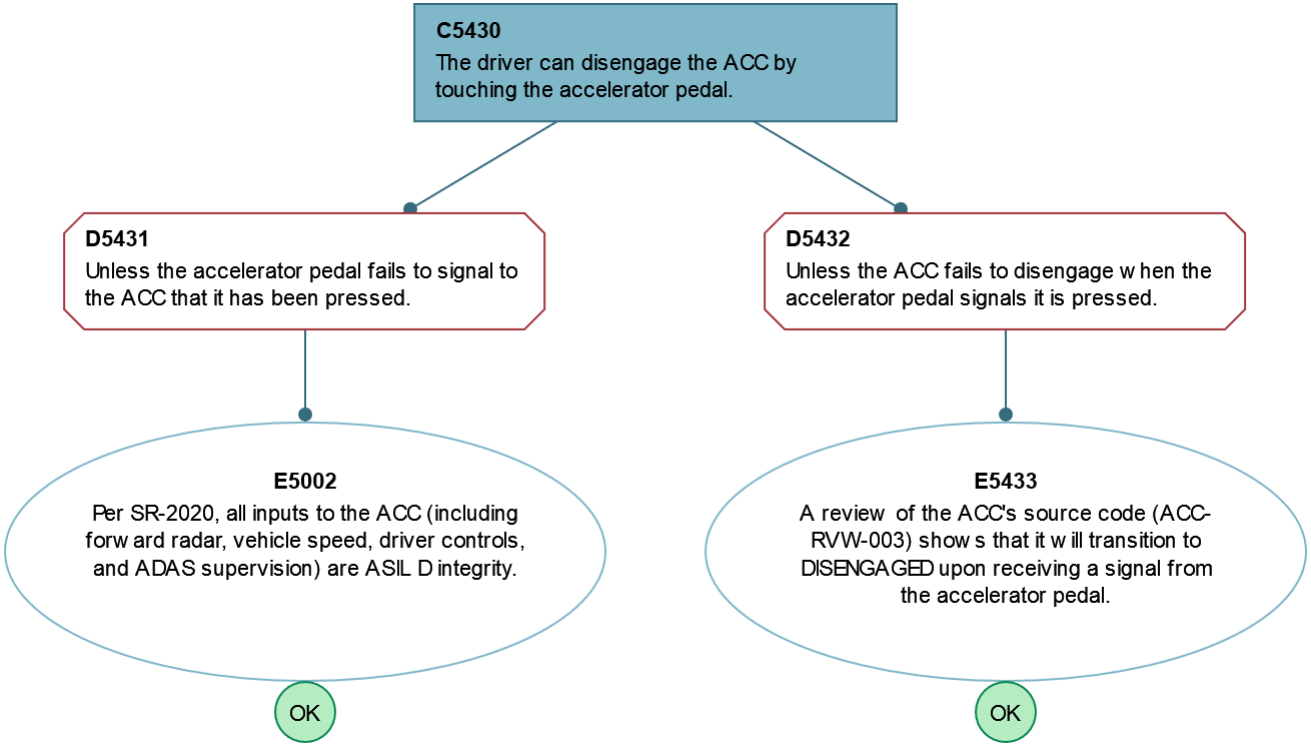
IR5320 - If the ACC outputs control signals that keep the vehicle below SET_SPEED and outside of SET_DISTANCE from the forward vehicle, then control ...			
Parent subtree(s)	C5300	**Descendant subtree(s)**	C5330, C5430
Description			
Artifacts	None	**Glossary Terms**	None



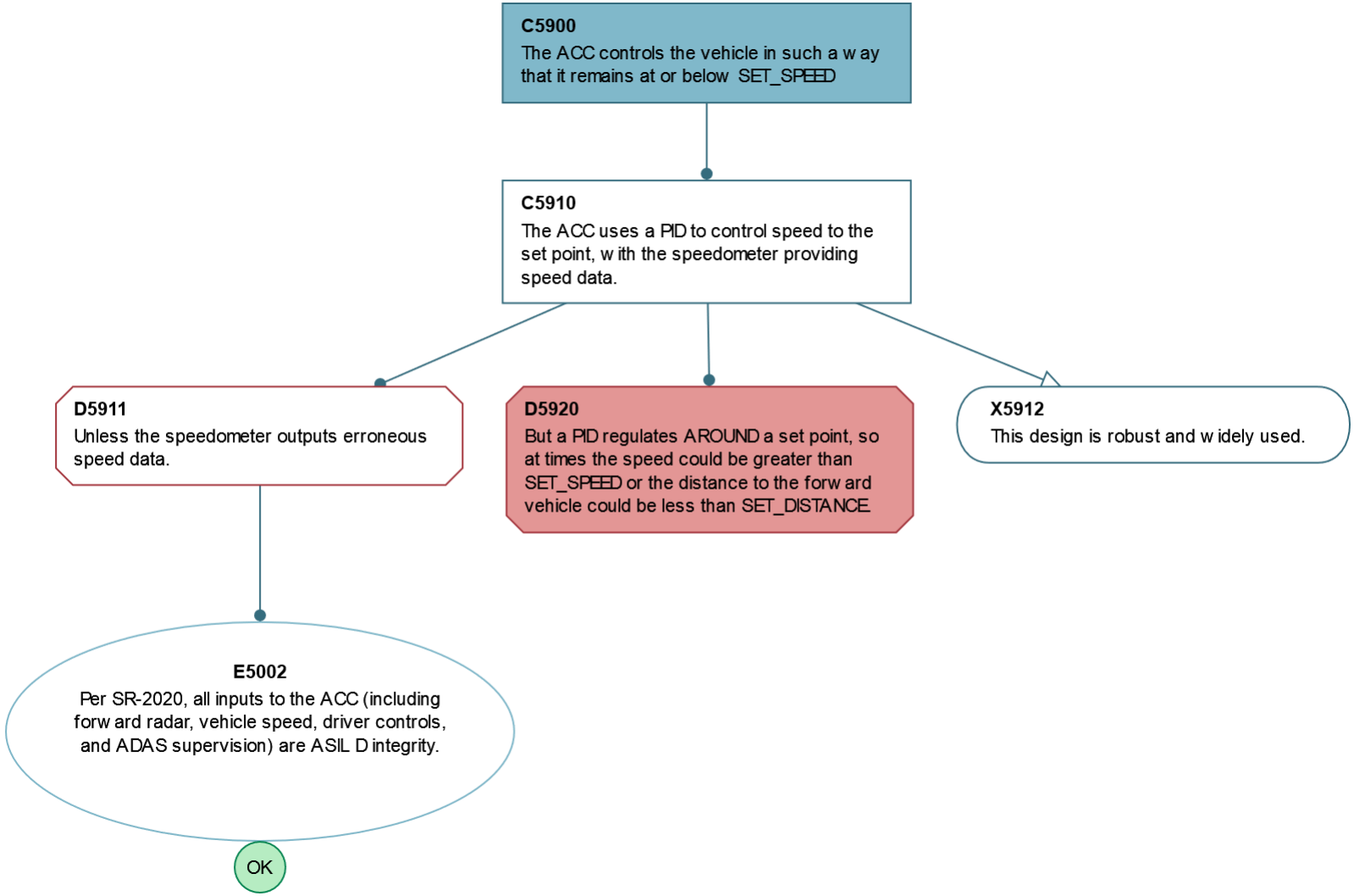
C5330 - SET_SPEED and SET_DISTANCE are chosen by the driver, and it is the driver's responsibility to ensure they are appropriate for the conditions...			
Parent subtree(s)	IR5320	**Descendant subtree(s)**	None
Description			
Artifacts	E5331: Safety Manual Requirements	**Glossary Terms**	None



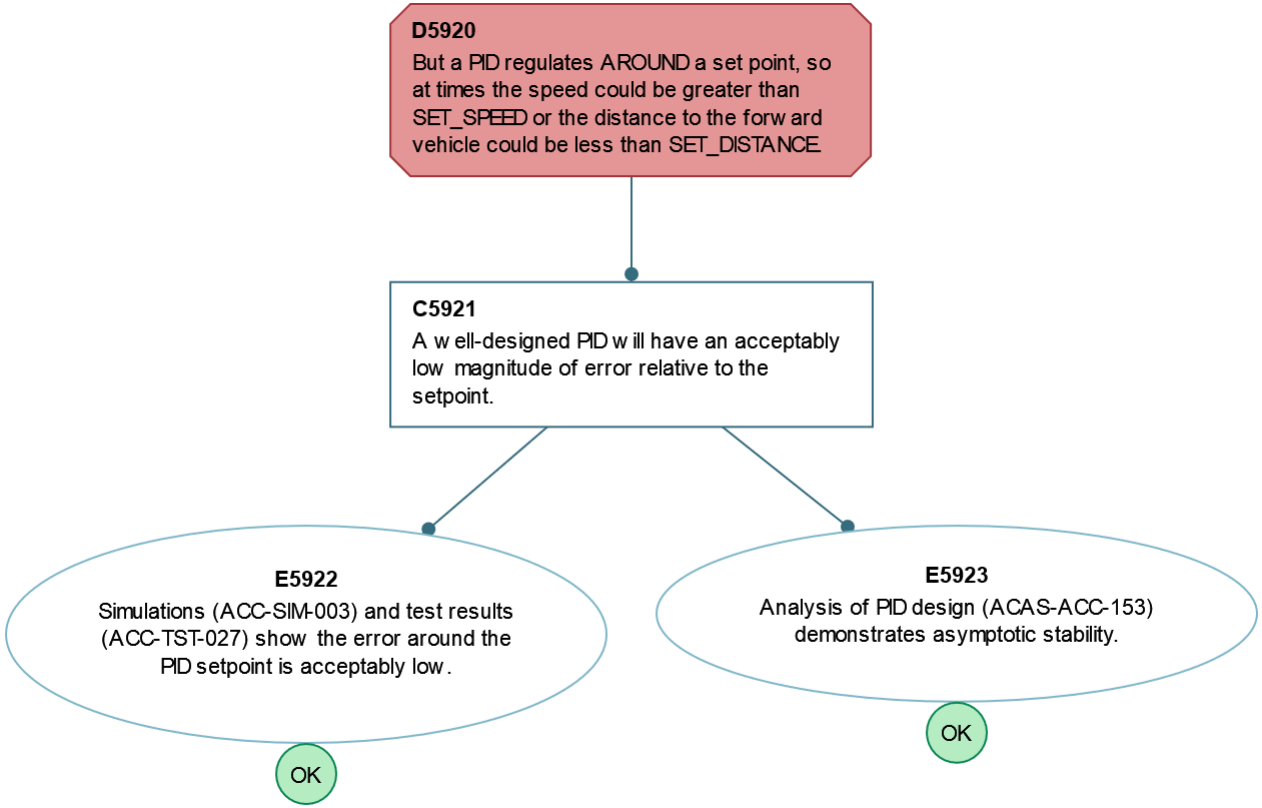
C5430 - The driver can disengage the ACC by touching the accelerator pedal.			
Parent subtree(s)	IR5320, S5400	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



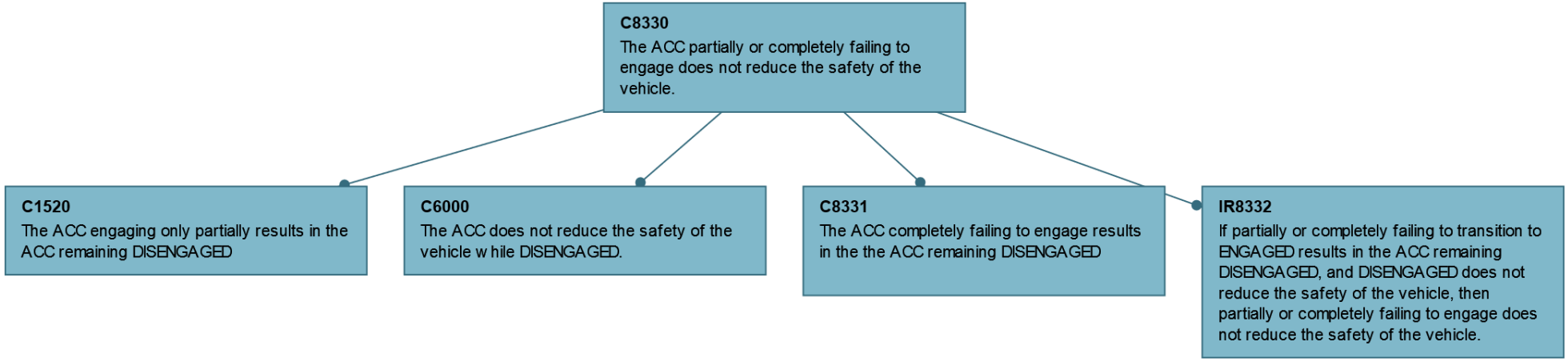
C5900 - The ACC controls the vehicle in such a way that it remains at or below SET_SPEED			
Parent subtree(s)	C5300	**Descendant subtree(s)**	D5920
Description			
Artifacts	None	**Glossary Terms**	None



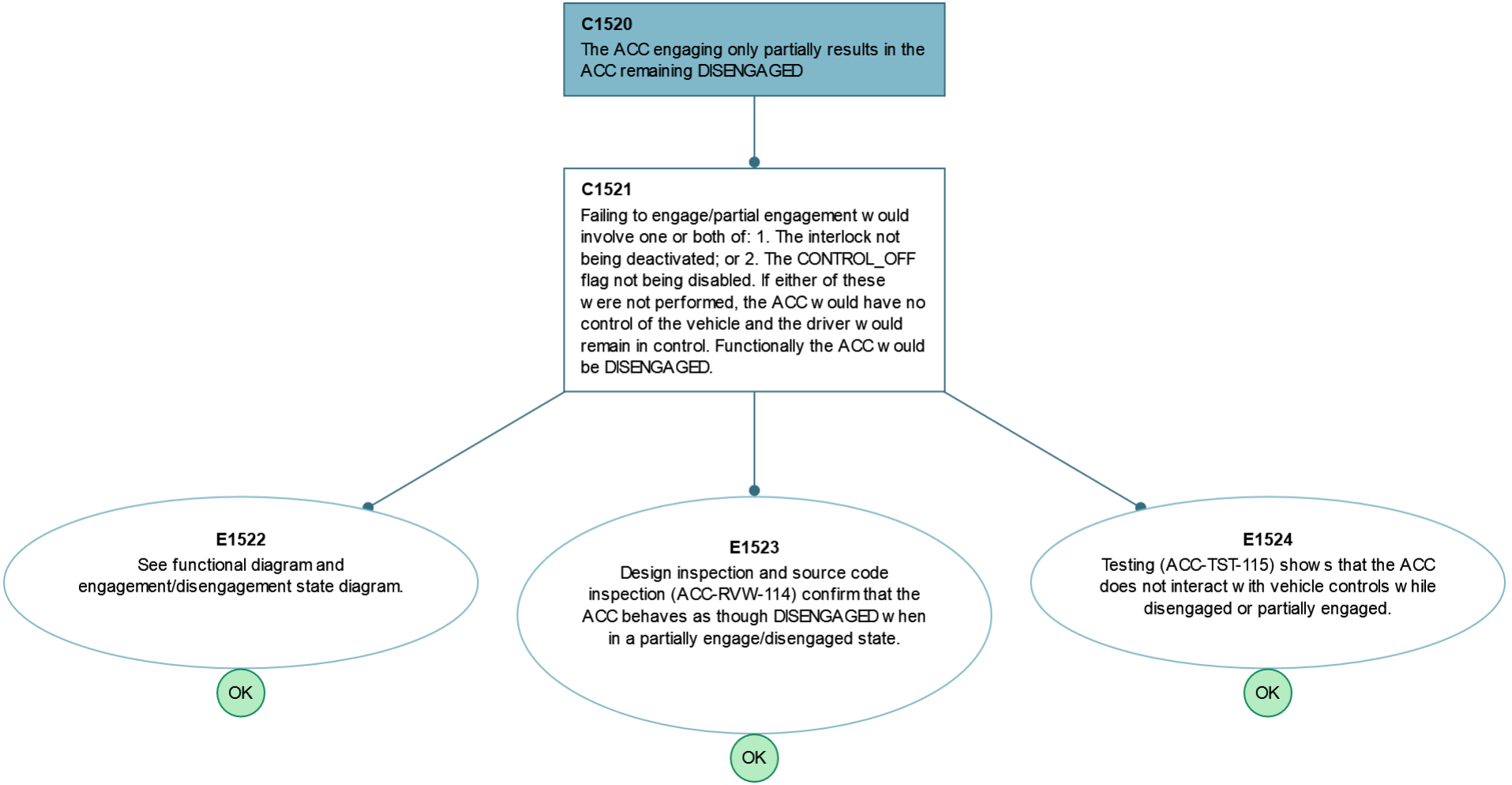
D5920 - But a PID regulates AROUND a set point, so at times the speed could be greater than SET_SPEED or the distance to the forward vehicle could b...			
Parent subtree(s)	C5310, C5900	**Descendant subtree(s)**	None
Description			
Artifacts	E5922: Test Results	**Glossary Terms**	None



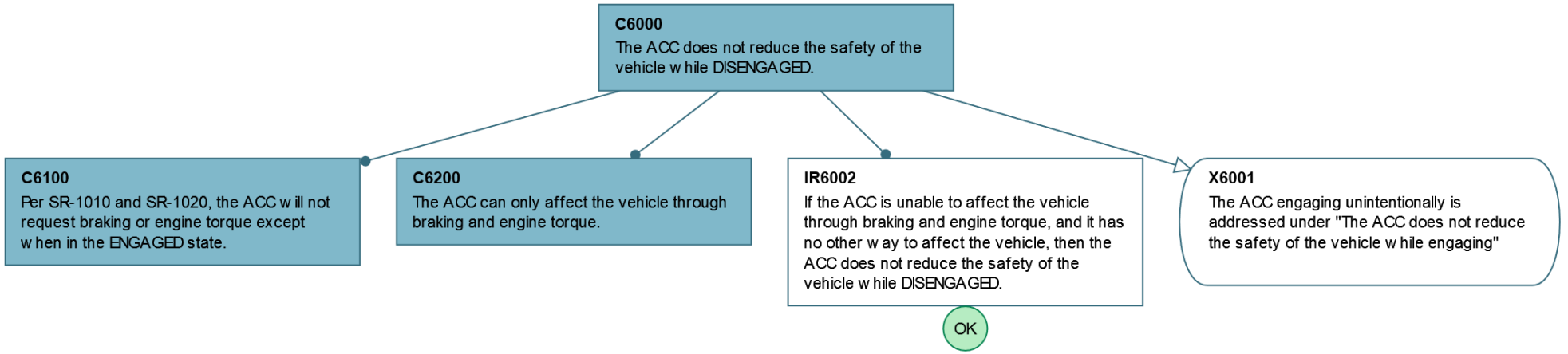
C8330 - The ACC partially or completely failing to engage does not reduce the safety of the vehicle.			
Parent subtree(s)	C8300	**Descendant subtree(s)**	C1520, C6000, C8331, IR8332
Description			
Artifacts	None	**Glossary Terms**	None



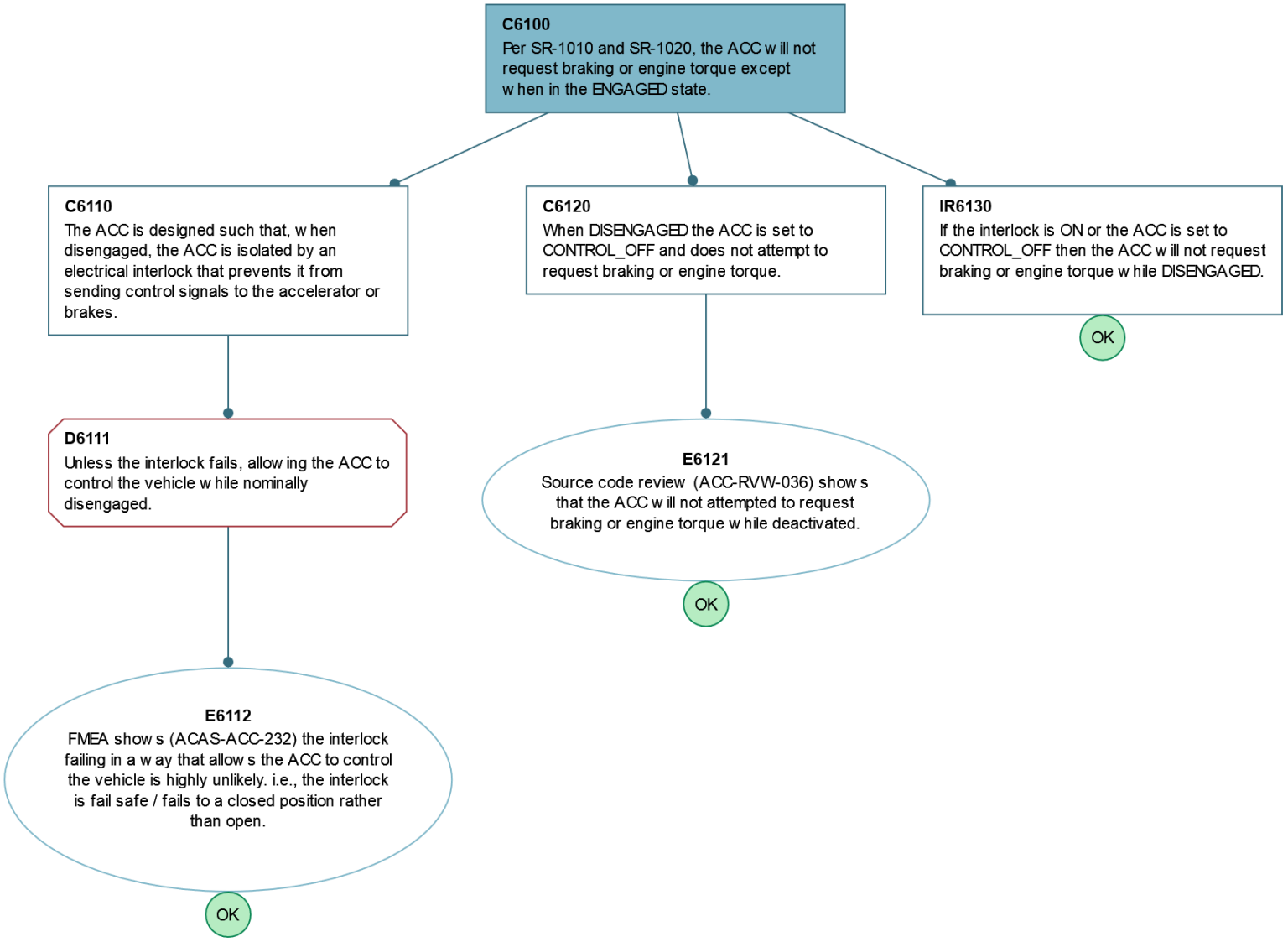
C1520 - The ACC engaging only partially results in the ACC remaining DISENGAGED			
Parent subtree(s)	C7100, IR1500, C8330	**Descendant subtree(s)**	None
Description			
Artifacts	E1524: Test Results	**Glossary Terms**	None



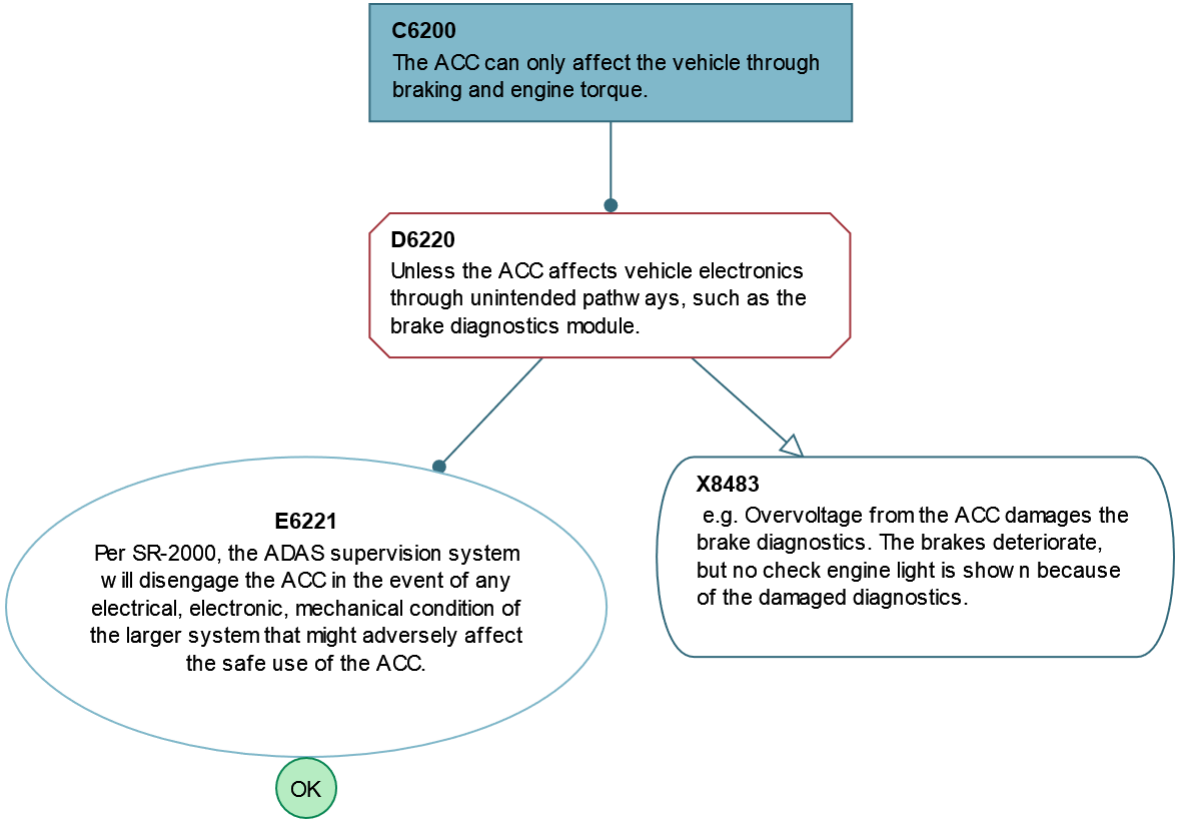
C6000 - The ACC does not reduce the safety of the vehicle while DISENGAGED.			
Parent subtree(s)	C1000, C8330, C7000	**Descendant subtree(s)**	C6100, C6200
Description			
Artifacts	None	**Glossary Terms**	None



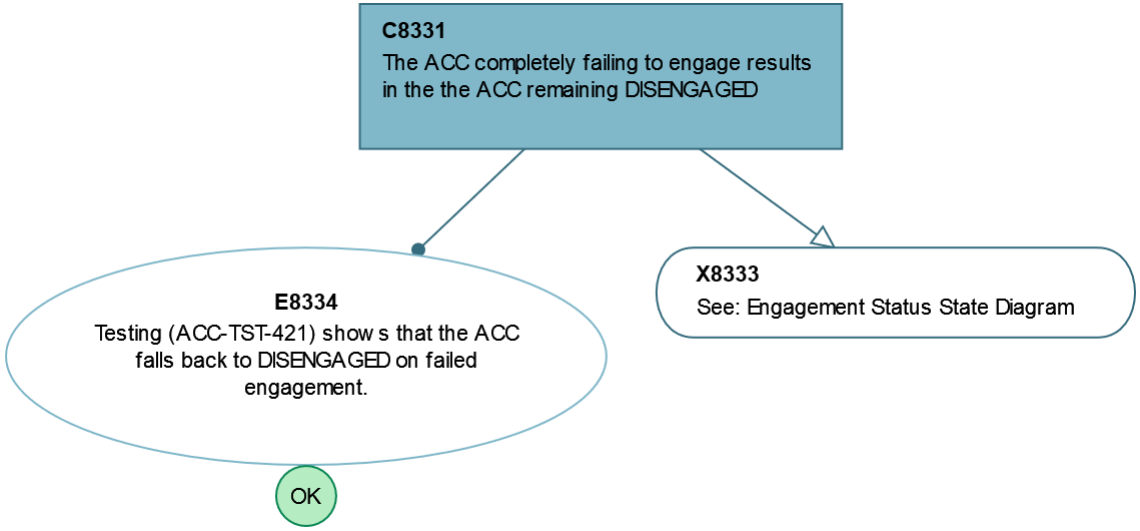
C6100 - Per SR-1010 and SR-1020, the ACC will not request braking or engine torque except when in the ENGAGED state.			
Parent subtree(s)	C6000	**Descendant subtree(s)**	None
Description			
Artifacts	E6112: Interlock FMEA	**Glossary Terms**	None



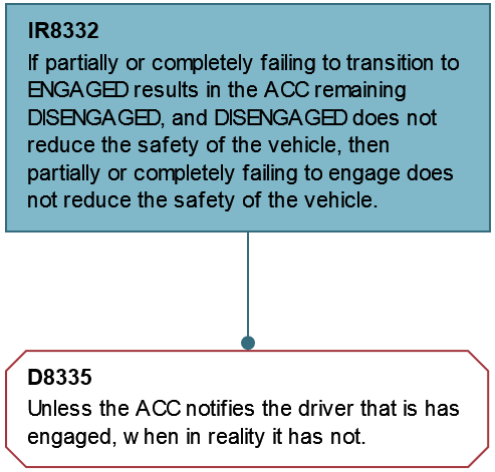
C6200 - The ACC can only affect the vehicle through braking and engine torque.			
Parent subtree(s)	C6000	**Descendant subtree(s)**	None
Description			
Artifacts	E6221: Safety Manual Requirements	**Glossary Terms**	None



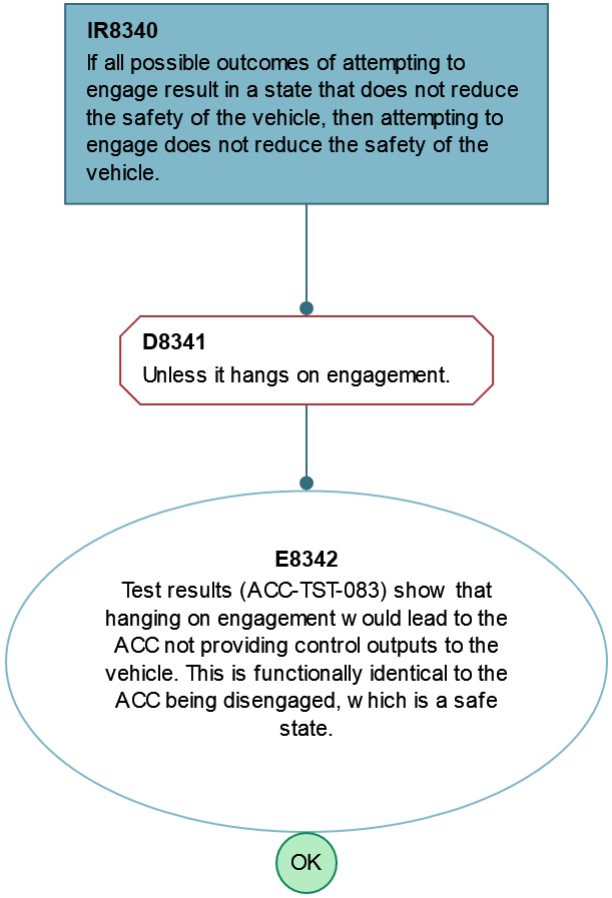
C8331 - The ACC completely failing to engage results in the the ACC remaining DISENGAGED			
Parent subtree(s)	C8330	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



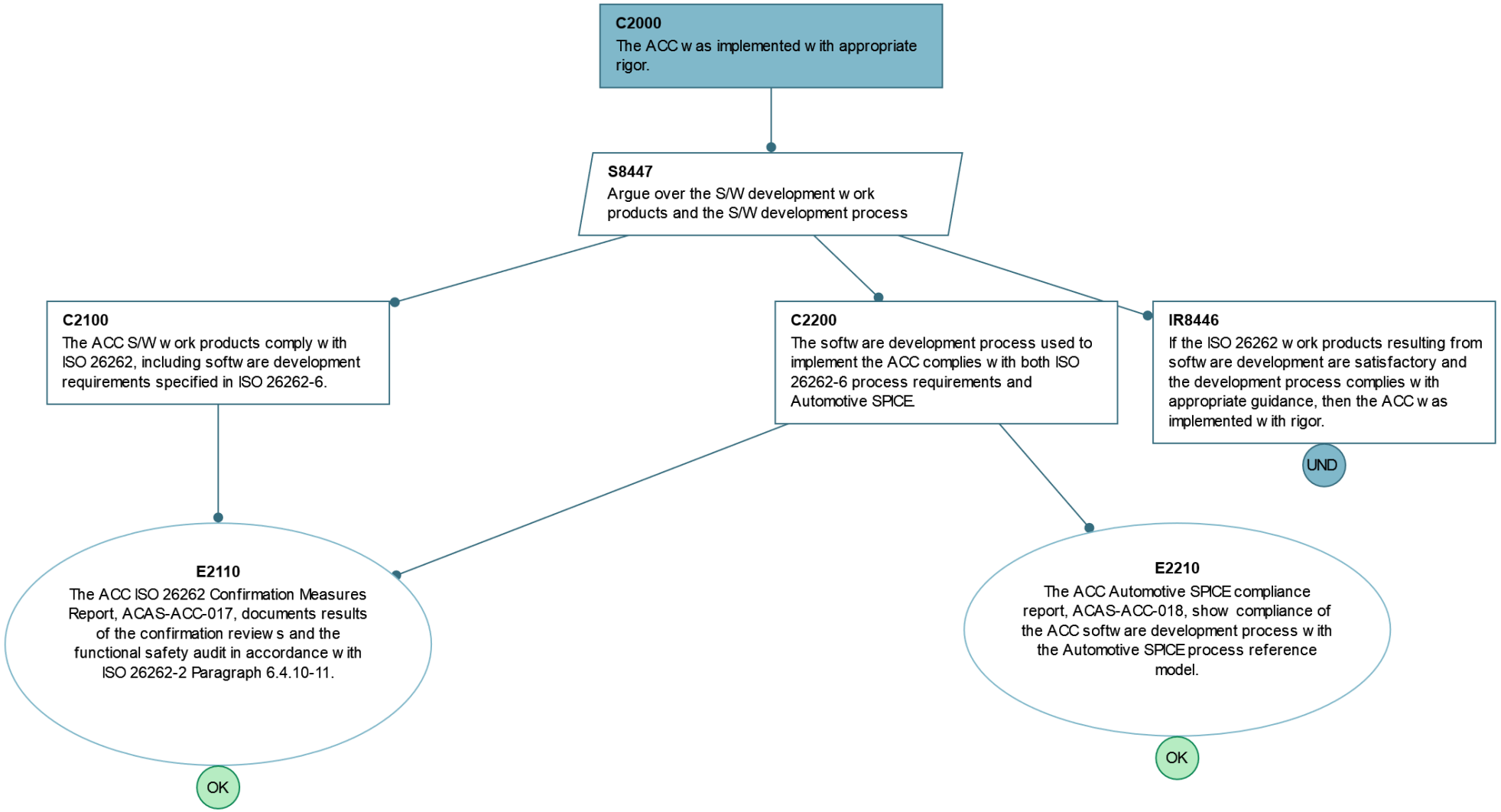
IR8332 - If partially or completely failing to transition to ENGAGED results in the ACC remaining DISENGAGED, and DISENGAGED does not reduce the safe...			
Parent subtree(s)	C8330	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



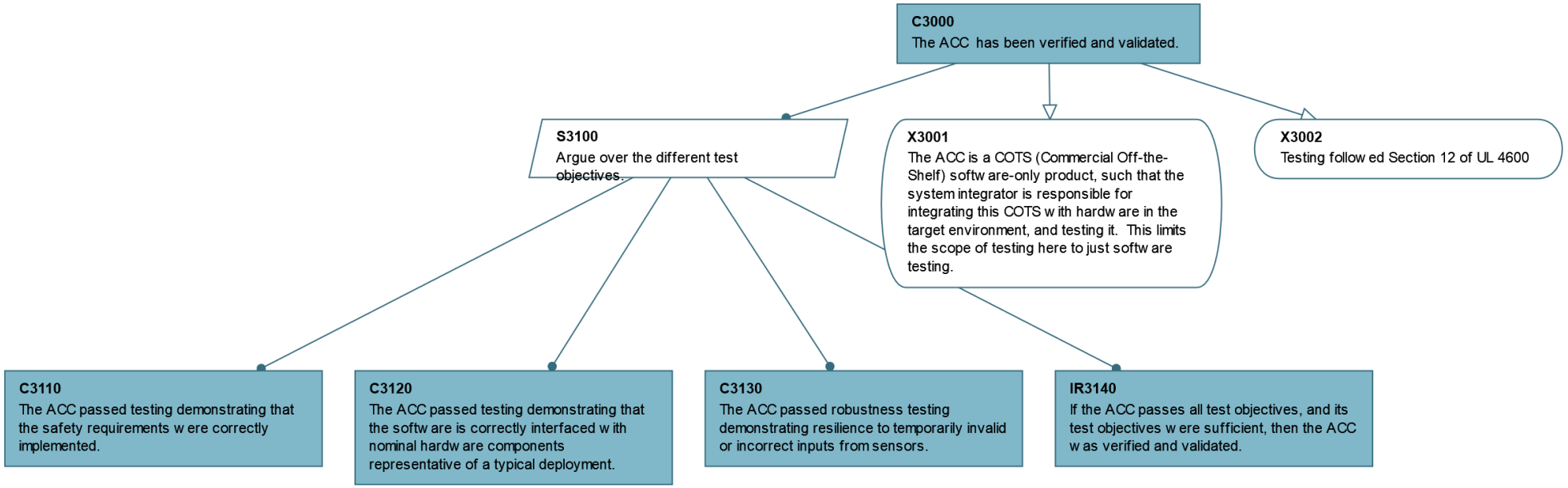
IR8340 - If all possible outcomes of attempting to engage result in a state that does not reduce the safety of the vehicle, then attempting to engage...			
Parent subtree(s)	C8300	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



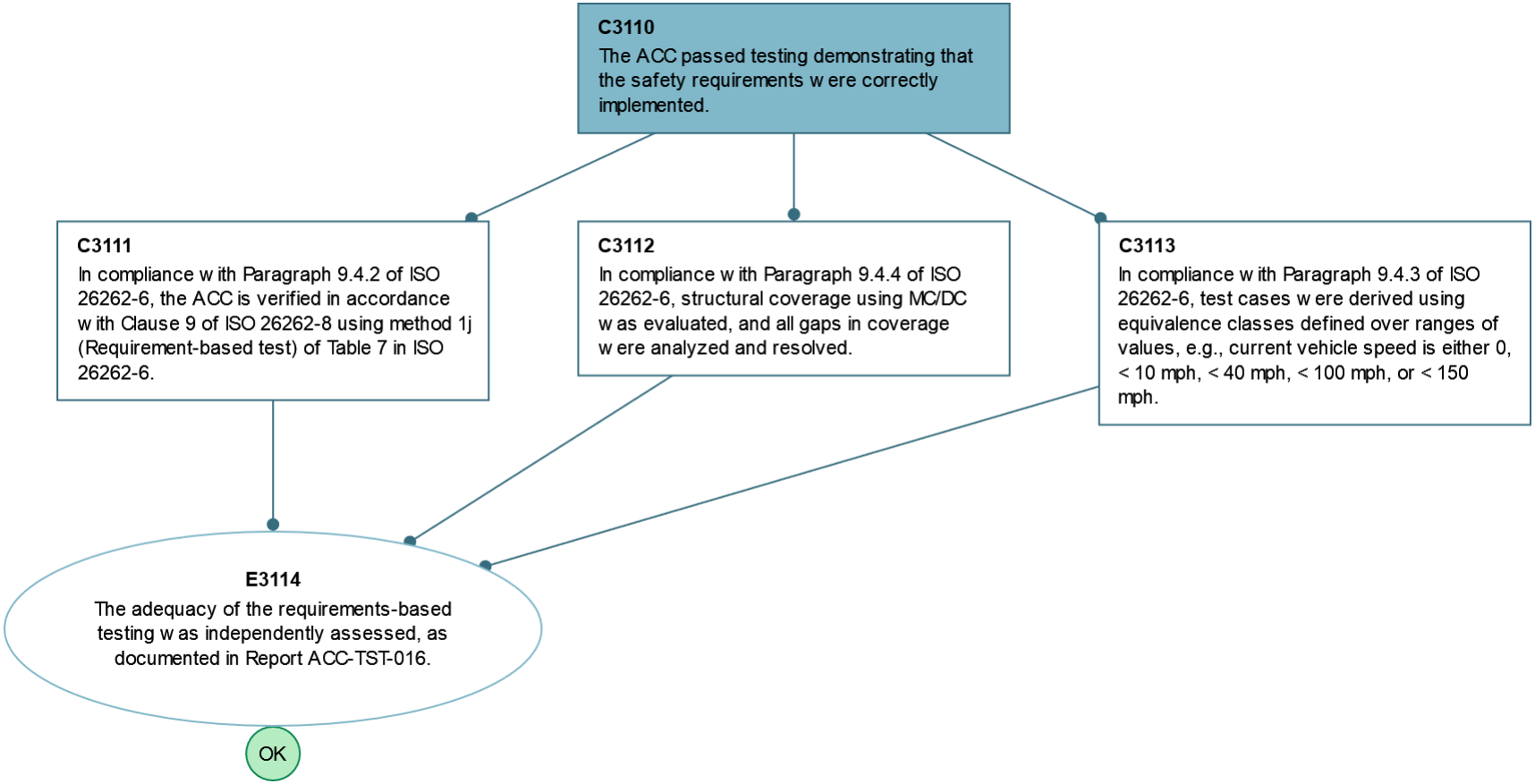
C2000 - The ACC was implemented with appropriate rigor.			
Parent subtree(s)	S0100	**Descendant subtree(s)**	None
Description			
Artifacts	C2100: ISO 26262; C2200: A-SPICE; E2210: A-SPICE	**Glossary Terms**	None



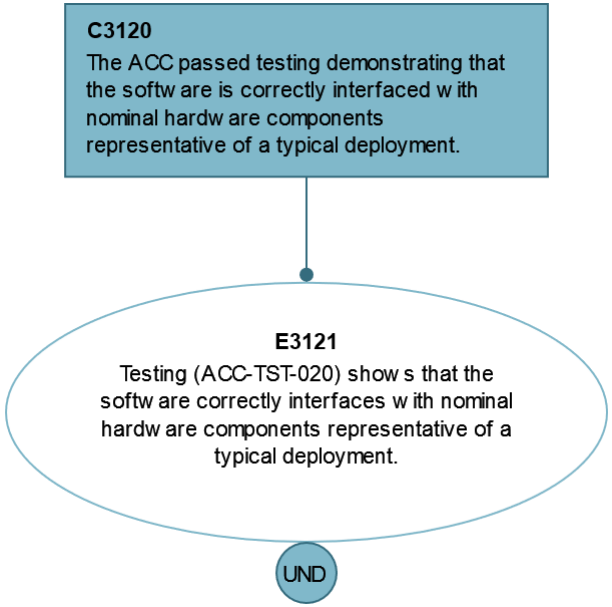
C3000 - The ACC has been verified and validated.			
Parent subtree(s)	S0100	**Descendant subtree(s)**	C3110, C3120, C3130, IR3140
Description	This was inspired by an email Jeff sent in March 2022		
Artifacts	X3002: UL 4600	**Glossary Terms**	None



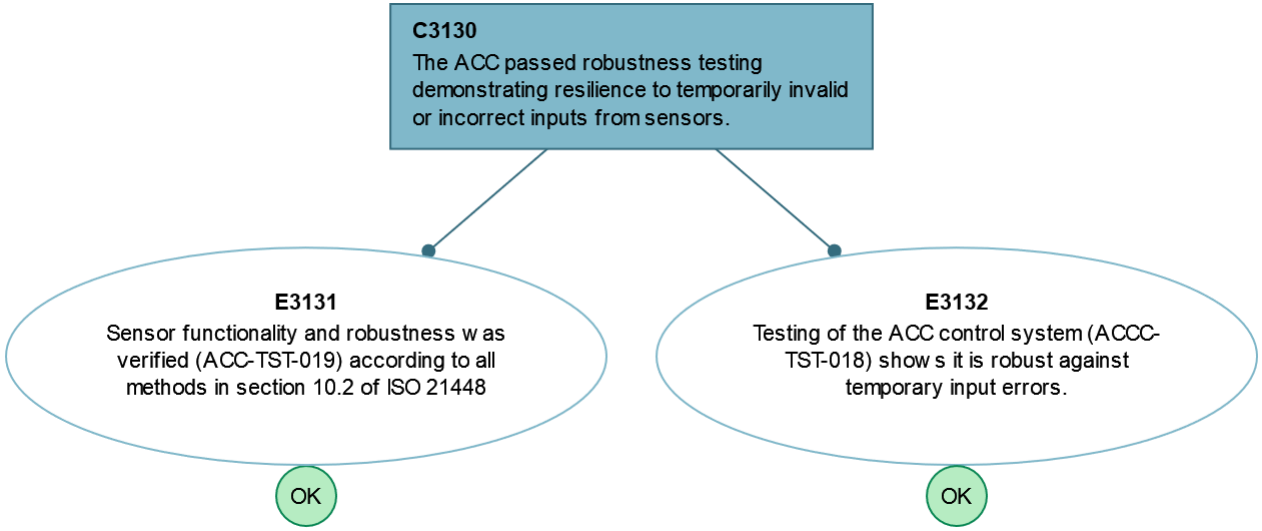
C3110 - The ACC passed testing demonstrating that the safety requirements were correctly implemented.			
Parent subtree(s)	C3000	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



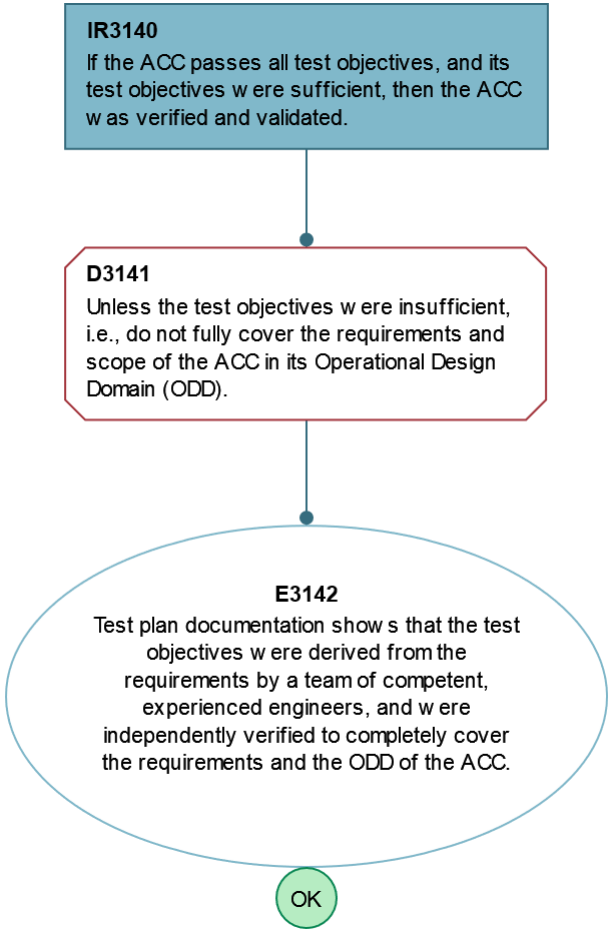
C3120 - The ACC passed testing demonstrating that the software is correctly interfaced with nominal hardware components representative of a typical ...			
Parent subtree(s)	C3000	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



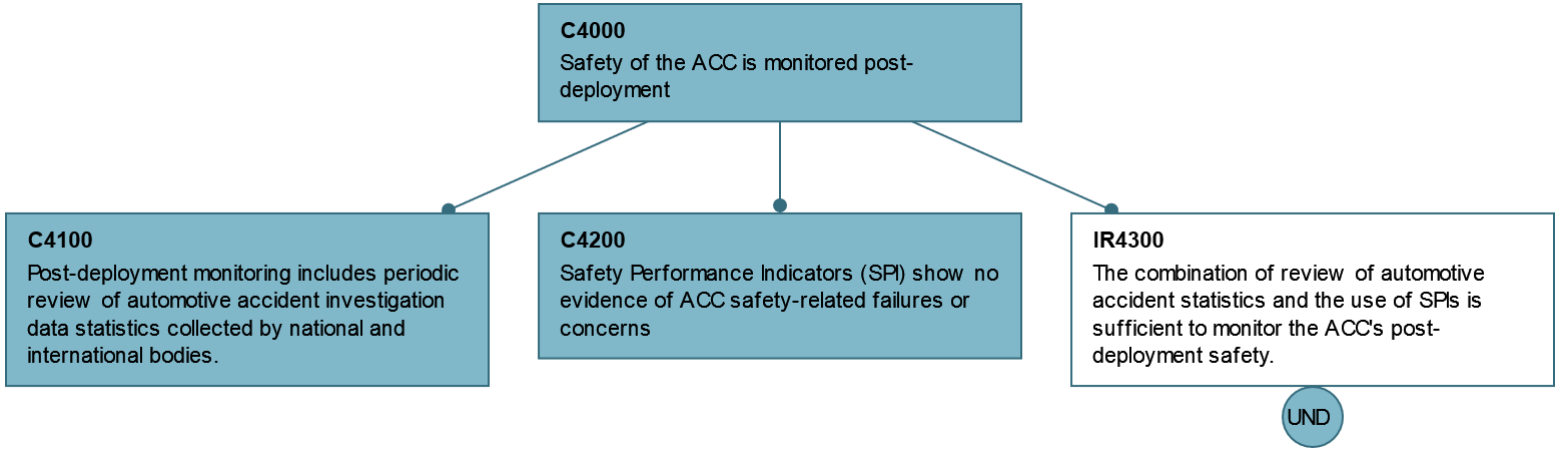
C3130 - The ACC passed robustness testing demonstrating resilience to temporarily invalid or incorrect inputs from sensors.			
Parent subtree(s)	C3000	**Descendant subtree(s)**	None
Description			
Artifacts	E3131: ISO 21448, Test Results	**Glossary Terms**	None



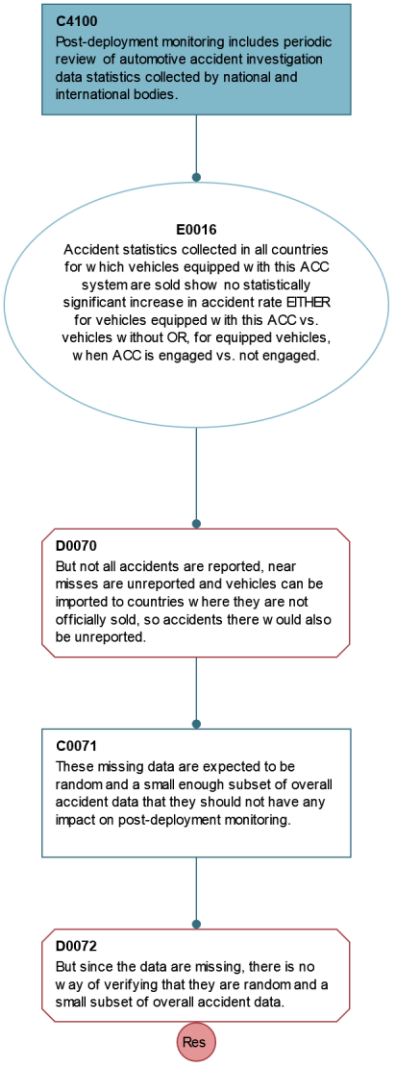
IR3140 - If the ACC passes all test objectives, and its test objectives were sufficient, then the ACC was verified and validated.			
Parent subtree(s)	C3000	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



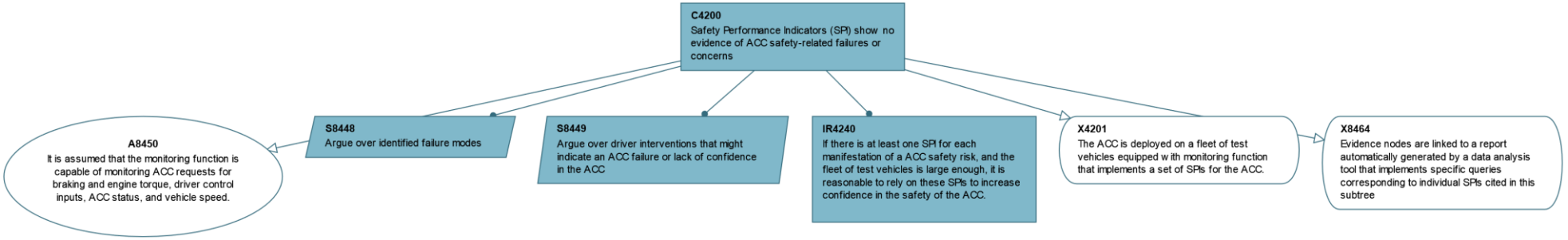
C4000 - Safety of the ACC is monitored post-deployment			
Parent subtree(s)	S0100	**Descendant subtree(s)**	C4100, C4200
Description			
Artifacts	None	**Glossary Terms**	None



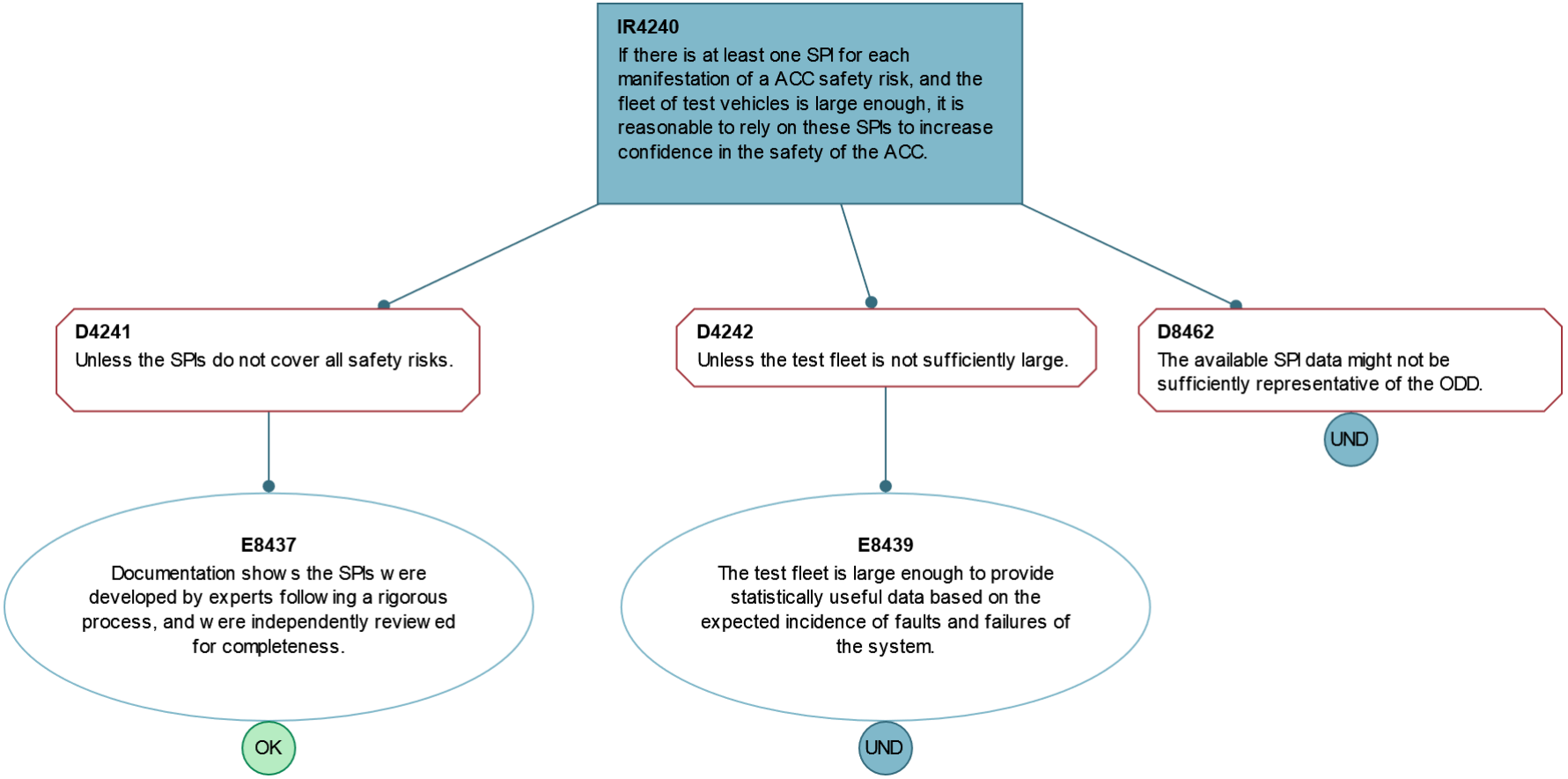
C4100 - Post-deployment monitoring includes periodic review of automotive accident investigation data statistics collected by national and internati...			
Parent subtree(s)	C4000	**Descendant subtree(s)**	None
Description	This residual doubt is acceptably small. i.e. The likelihood of the missing data: 1. Being statistically significantly different from the collected data; 2. Being a large enough portion of the total data to affect the conclusion; and 3. Indicating a safety issue is acceptably low.		
Artifacts	E0016: Post-deployment Accident Statistics	**Glossary Terms**	None



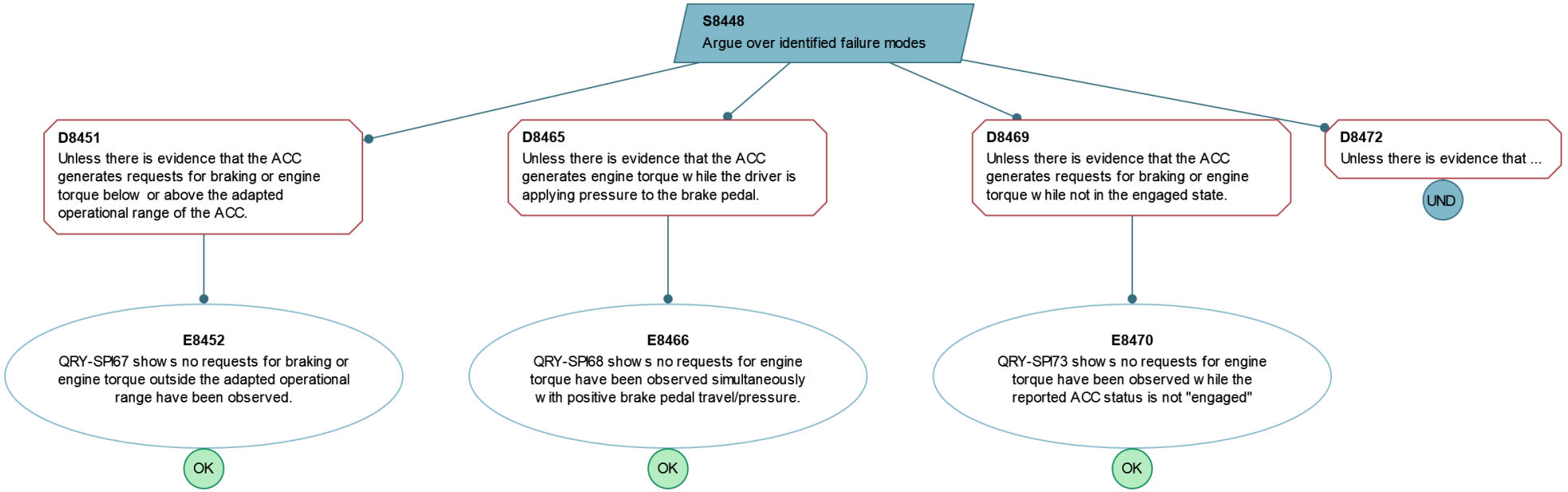
C4200 - Safety Performance Indicators (SPI) show no evidence of ACC safety-related failures or concerns			
Parent subtree(s)	C4000	**Descendant subtree(s)**	IR4240, S8448, S8449
Description			
Artifacts	None	**Glossary Terms**	None



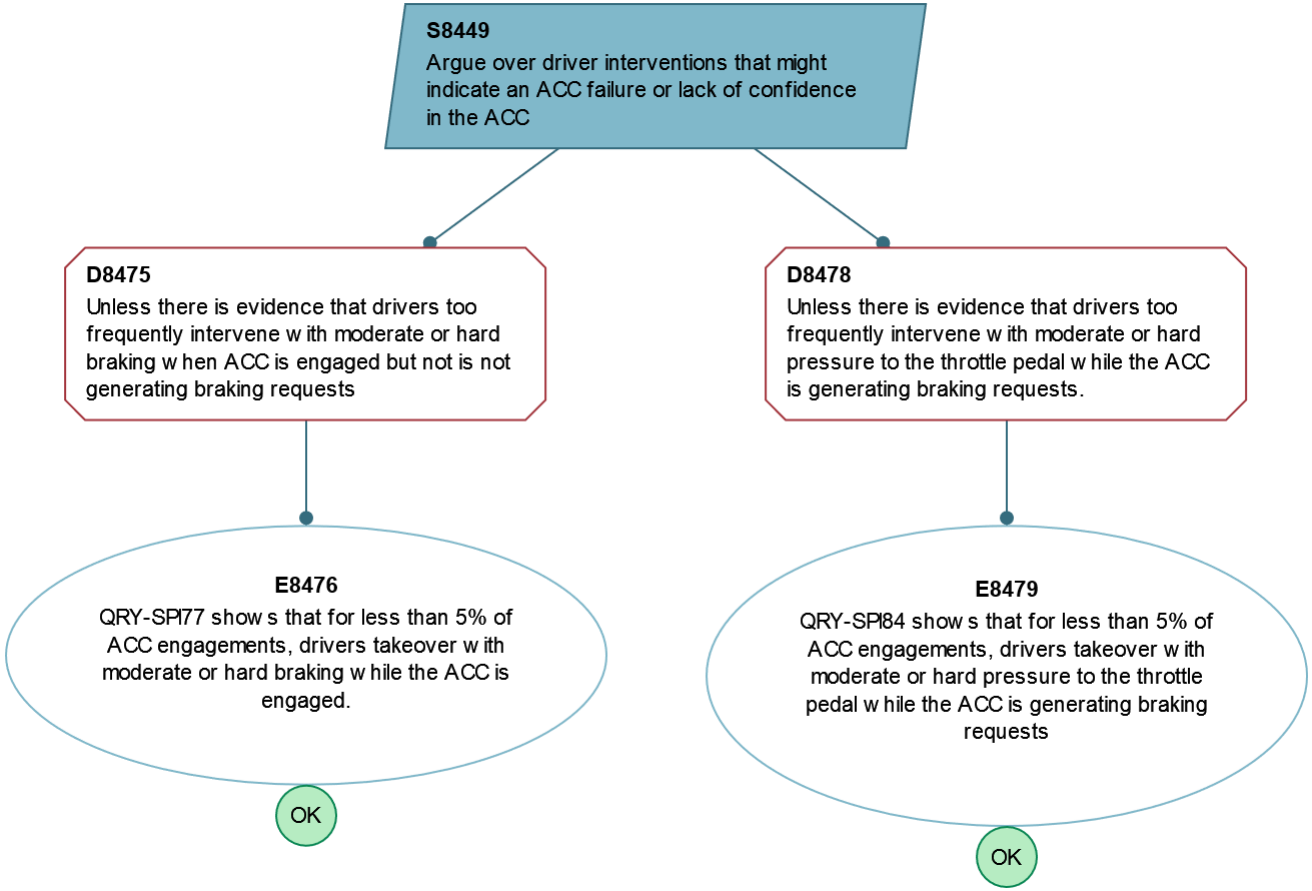
IR4240 - If there is at least one SPI for each manifestation of a ACC safety risk, and the fleet of test vehicles is large enough, it is reasonable t...			
Parent subtree(s)	C4200	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



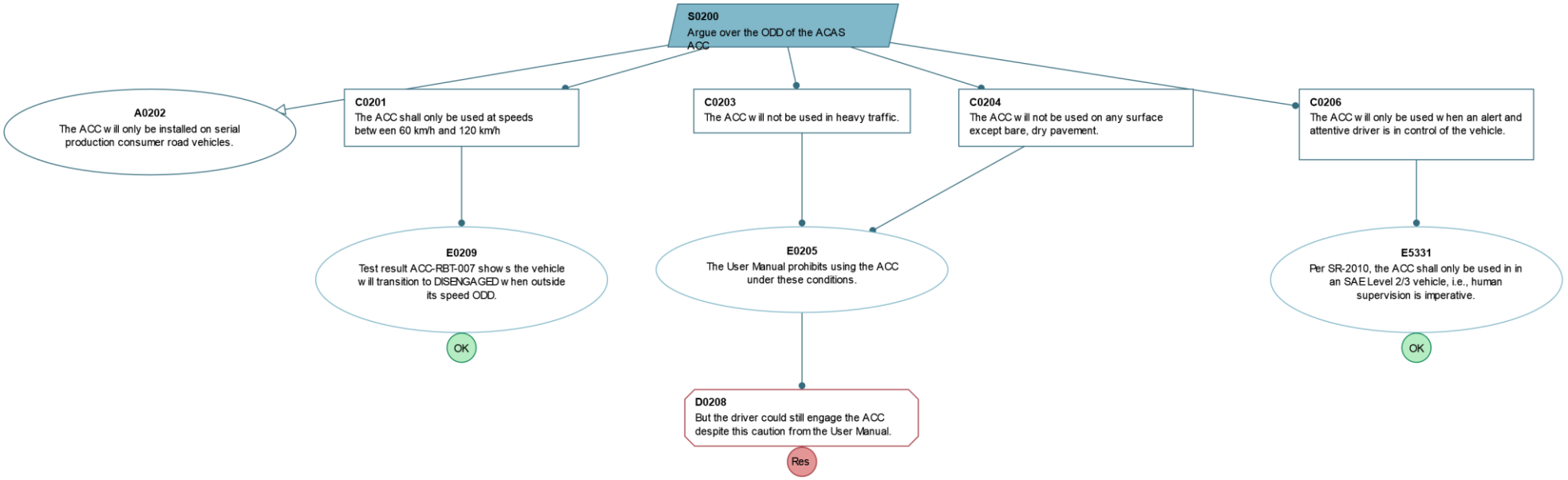
S8448 - Argue over identified failure modes			
Parent subtree(s)	C4200	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



S8449 - Argue over driver interventions that might indicate an ACC failure or lack of confidence in the ACC			
Parent subtree(s)	C4200	**Descendant subtree(s)**	None
Description			
Artifacts	None	**Glossary Terms**	None



S0200 - Argue over the ODD of the ACAS ACC			
Parent subtree(s)	C0001	**Descendant subtree(s)**	None
Description			
Artifacts	A0202: Safety Manual Requirements; E5331: Safety Manual Requirements	**Glossary Terms**	None



Artifacts

Name	ISO 26262
Description	Road Vehicles - Functional Safety
References	C2100
Link	ISO 26262
Version	None
Status	None
Date updated	None

Name	ACC Functional Design
Description	Block diagram showing data flow through the ACAS ACC.
References	
Link	ACC Functional Design
Version	None
Status	None
Date updated	None

Name	Project Description
Description	Document describing the ACAS ACC's ODD, basic functionality and high-level architecture.
References	C7211, X5043, IR5030
Link	Project Description
Version	None
Status	None
Date updated	None

Name	ACC Engagement Module FTA
Description	Fault Tree showing failure modes and probabilities for the ACC Engagement Module
References	E7106
Link	ACC Engagement Module FTA
Version	None
Status	None
Date updated	None

Name	ISO 21448

Description	Road vehicles - Safety of the intended functionality
References	E3131
Link	ISO 21448
Version	None
Status	None
Date updated	None

Name	UL 4600
Description	Standard for Safety for the Evaluation of Autonomous Products
References	X3002
Link	UL 4600
Version	None
Status	None
Date updated	None

Name	User Manual
Description	Instructions for the user, including when use is appropriate and cautioning that the user must always be alert and engaged. Keep your hands on the steering wheel and remain alert at all times. Do not engage the ACC in heavy traffic. Do not engage the ACC when the road is icy, wet or otherwise slippery.
References	C7211, IR5030
Link	User Manual
Version	None
Status	None
Date updated	None

Name	Safety Requirements
Description	List of safety requirements for the ACAS ACC, as number SHALL statements. Also includes a glossary of defined terms.
References	
Link	Safety Requirements
Version	None
Status	None
Date updated	None

Name	Max Acceleration-Deceleration Authority FTA

Description	Fault tree analyzing the failure modes and probabilities of the Max Acceleration-Deceleration Authority
References	E5621
Link	Max Acceleration-Deceleration Authority FTA
Version	None
Status	None
Date updated	None

Name	Safety Manual Requirements
Description	Requirements for the ACC's integration into the end-product vehicle.
References	E6221, E5331, A0202
Link	Safety Manual Requirements
Version	None
Status	None
Date updated	None

Name	Interlock FMEA
Description	Failure Modes and Effects Analysis for the ACC interlock
References	E6112
Link	Interlock FMEA
Version	None
Status	None
Date updated	None

Name	Engagement-Disengagement State Diagram
Description	Block diagram showing the ACC's states, and conditions for it to transition between states.
References	IR1500
Link	Engagement-Disengagement State Diagram
Version	None
Status	None
Date updated	None

Name	Test Results
Description	Document Containing Test Results

References	E8211, E5701, E5922, E5622, E1524, E3131
Link	Test Results
Version	None
Status	None
Date updated	None

Name	Post-deployment Accident Statistics
Description	Accident statistics collected in countries in which ACAS ACC-equipped vehicles are deployed.
References	E0016
Link	Post-deployment Accident Statistics
Version	None
Status	None
Date updated	None

Name	A-SPICE
Description	None
References	C2200, E2210
Link	A-SPICE
Version	None
Status	None
Date updated	None

Glossary

No Glossary Terms

Issues

No Issues

Comments

No Comments

END