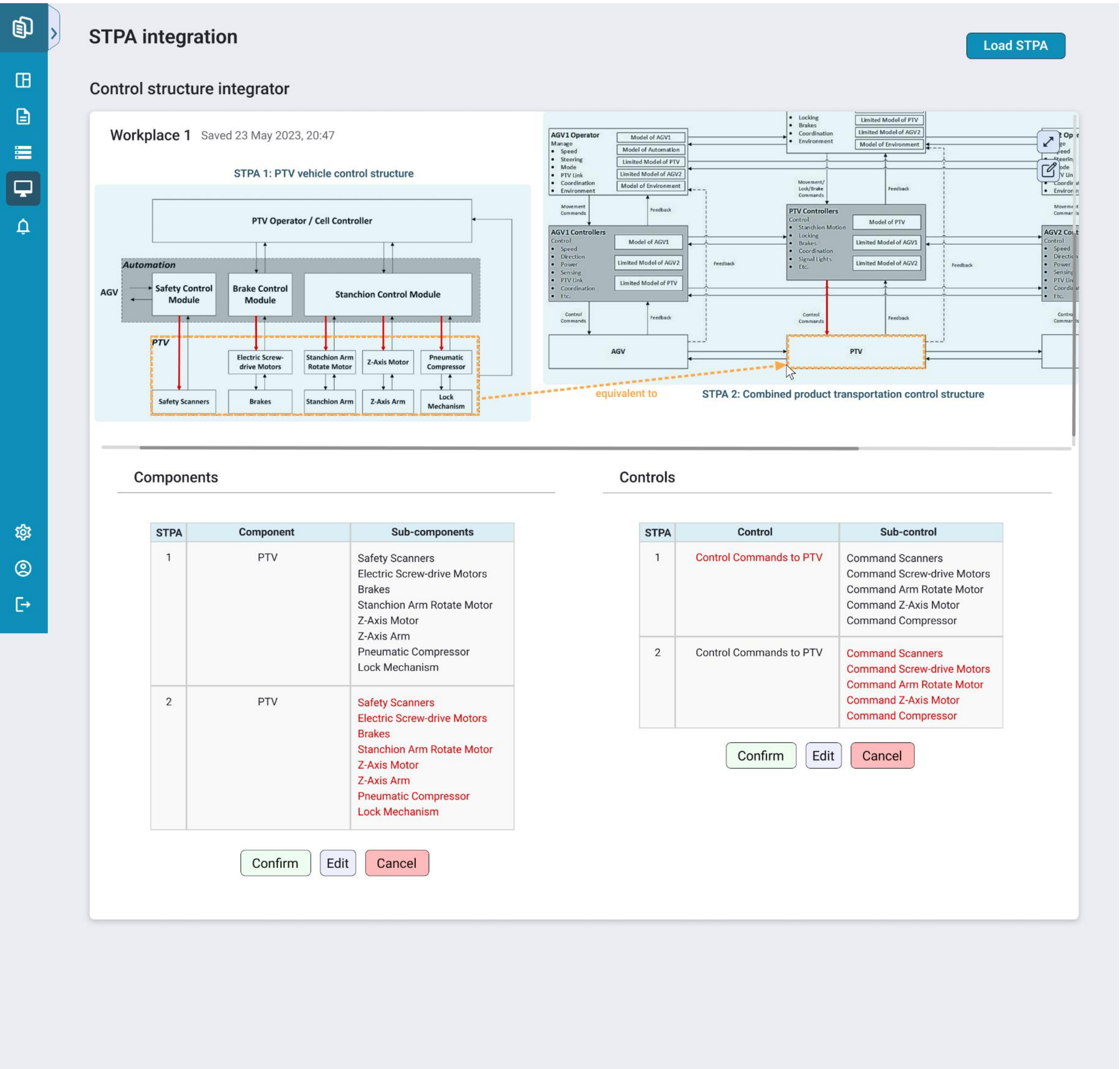
This white paper demonstrates features that can be delivered with STPA tool as a service (the STPAmaster). They stem from academic study of safety science, researching STPA and bringing improvements to aviation organizations, who demanded unique solutions not available on the market. The presented features are not exhaustive; in fact, seamless STPA integration poses diverse challenges leading to delivery of unique STPA tooling for each customer.

Reusability feature

Complex systems can be analyzed with STPA at different levels of abstraction or per their parts, producing separate artifacts. It is desirable to integrate them to avoid duplicate work in the future. The user may wish to add detailed analysis to a more abstract one, integrate overlapping analyses and/or completing them with missing components and interactions on their interfaces.



STPA integration

Control structure integrator

Workplace 1 Saved 23 May 2023, 20:47

STPA 1: PTV vehicle control structure

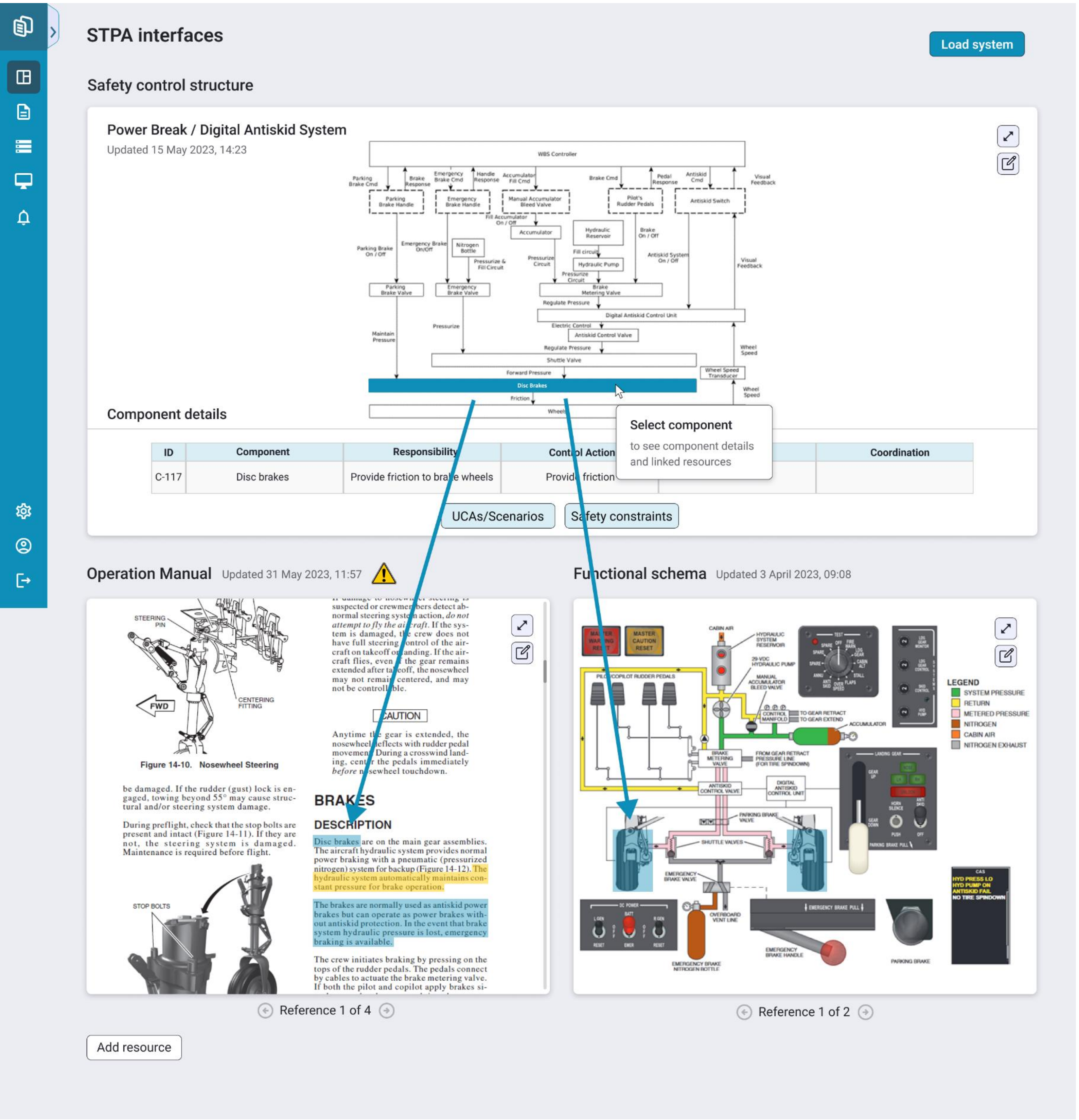
STPA 2: Combined product transportation control structure

STPA	Component	Sub-components
1	PTV	Safety Scanners Electric Screw-drive Motors Brakes Stanchion Arm Rotate Motor Z-Axis Motor Z-Axis Arm Pneumatic Compressor Lock Mechanism
2	PTV	Safety Scanners Electric Screw-drive Motors Brakes Stanchion Arm Rotate Motor Z-Axis Motor Z-Axis Arm Pneumatic Compressor Lock Mechanism

STPA	Control	Sub-control
1	Control Commands to PTV	Command Scanners Command Screw-drive Motors Command Arm Rotate Motor Command Z-Axis Motor Command Compressor
2	Control Commands to PTV	Command Scanners Command Screw-drive Motors Command Arm Rotate Motor Command Z-Axis Motor Command Compressor

Traceability feature

STPA is often executed in an iterative order, based on external resources. The outputs of the analysis may impose new requirements on the analyzed system, which may change the analyzed system in turn, leading to the next STPA iteration. It is thus important to trace external resources with STPA analysis to keep them synchronized. The user may wish to navigate from a selected part of the analysis to resources used in creating that part, with highlighted references. When external resources update, the user needs to be alerted and guided to update the STPA analysis accordingly.



STPA interfaces

Load system

Safety control structure

Power Break / Digital Antiskid System

Updated 15 May 2023, 14:23

Select component

to see component details and linked resources

Component details

ID	Component	Responsibility	Control Action		Coordination
C-117	Disc brakes	Provide friction to brake wheels	Provide friction		

UCAs/Scenarios

Safety constraints

Operation Manual Updated 31 May 2023, 11:57 ⚠

Figure 14-10. Nosewheel Steering

be damaged. If the rudder (gust) lock is engaged, towing beyond 55° may cause structural and/or steering system damage.

During preflight, check that the stop bolts are present and intact (Figure 14-11). If they are not, the steering system is damaged. Maintenance is required before flight.

suspected or crewmembers detect abnormal steering system action, *do not attempt to fly the aircraft*. If the system is damaged, the crew does not have full steering control of the aircraft on takeoff or landing. If the aircraft flies, even if the gear remains extended after takeoff, the nosewheel may not remain centered, and may not be controllable.

CAUTION

Anytime the gear is extended, the nosewheel deflects with rudder pedal movement. During a crosswind landing, center the pedals immediately *before* nosewheel touchdown.

BRAKES

DESCRIPTION

Disc brakes are on the main gear assemblies. The aircraft hydraulic system provides normal power braking with a pneumatic (pressurized nitrogen) system for backup (Figure 14-12). The hydraulic system automatically maintains constant pressure for brake operation.

The brakes are normally used as antiskid power brakes but can operate as power brakes without antiskid protection. In the event that brake system hydraulic pressure is lost, emergency braking is available.

The crew initiates braking by pressing on the tops of the rudder pedals. The pedals connect by cables to actuate the brake metering valve. If both the pilot and copilot apply brakes si-

Reference 1 of 4

Functional schema Updated 3 April 2023, 09:08

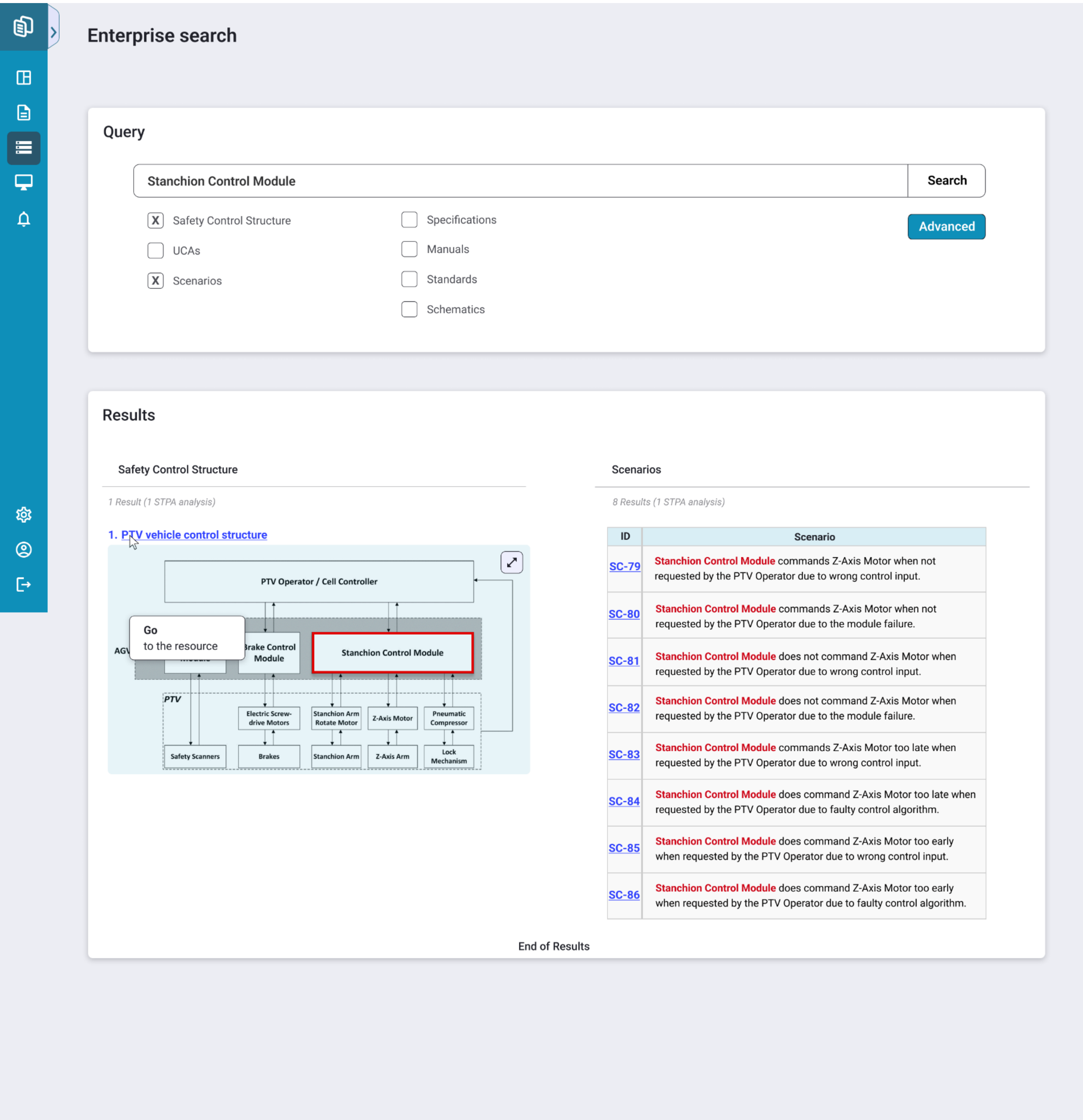
LEGEND
🟩 SYSTEM PRESSURE
🟨 RETURN
🟪 METERED PRESSURE
🟫 NITROGEN
🟧 CABIN AIR
⬜ NITROGEN EXHAUST

Reference 1 of 2

Add resource

Enterprise search feature

Over time, there may be many STPA artifacts stored in the system, making it difficult to find certain requirements, the rationale for them, etc. At the same time, the same contributory factors or contexts in unsafe control actions may repeat, each time in a slightly different form. Enterprise search feature is needed to properly identify what the user is searching for, be it in STPA artifacts or external resources. Additional feature may involve resolution of semantic inconsistencies where, for example, the same factor may be labelled differently in various STPA analyses.



Enterprise search

Query

Stanchion Control Module

☒ Safety Control Structure
□ UCAs
☒ Scenarios
□ Specifications
□ Manuals
□ Standards
□ Schematics

Results

Safety Control Structure

1 Result (1 STPA analysis)

1. PTV vehicle control structure

Scenarios

8 Results (1 STPA analysis)

ID	Scenario
SC-79	**Stanchion Control Module** commands Z-Axis Motor when not requested by the PTV Operator due to wrong control input.
SC-80	**Stanchion Control Module** commands Z-Axis Motor when not requested by the PTV Operator due to the module failure.
SC-81	**Stanchion Control Module** does not command Z-Axis Motor when requested by the PTV Operator due to wrong control input.
SC-82	**Stanchion Control Module** does not command Z-Axis Motor when requested by the PTV Operator due to the module failure.
SC-83	**Stanchion Control Module** commands Z-Axis Motor too late when requested by the PTV Operator due to wrong control input.
SC-84	**Stanchion Control Module** does command Z-Axis Motor too late when requested by the PTV Operator due to faulty control algorithm.
SC-85	**Stanchion Control Module** does command Z-Axis Motor too early when requested by the PTV Operator due to wrong control input.
SC-86	**Stanchion Control Module** does command Z-Axis Motor too early when requested by the PTV Operator due to faulty control algorithm.

End of Results