Industry Standards

SAE STPA Recommended Practice Task Force Update

J3187 – Applying System Theoretic Process Analysis (STPA) to Automotive Applications

Mark A. Vernacchia

GM Technical Fellow

Principal System Safety Engineer – Propulsion Systems

MIT STAMP Workshop
July 29, 2020

SAE STPA Task Force - Recap

Scope of this effort intends to provide both educational materials and recommended practices in regards to how STPA may be applied within a safety assessment process focusing on automotive safety-critical content

Purpose of this workgroup is to align industry (automotive/ aerospace) best practices and translate them across the automotive industry regarding the implementation and use of STPA within automotive controls, automotive HMI, and autonomous driving applications, and to explore focus areas suited for STPA use, or for supplementing other safety tools

J3187 – Applying System Theoretic Process Analysis (STPA) to Automotive Applications

- Liaison relationship with JASPAR - incorporate SW perspective
- Task Force has created Working Groups and Topics:
  - Group 1 – Basic STPA Approach, Recommended Practices, Lessons Learned
  - Group 2 – SOTIF and STPA
  - Group 2 – HMI and STPA
  - Group 2 – MBSE and STPA
  - Group 3 –High Level Use of STPA within Safety Process & STPA with Other Safety Evaluation Methods
  - Examples – Aerospace, Automotive, Automotive HMI, MBSE, SOTIF
  - Glossary

Currently have 61 members - 33 organizations

SAE STPA Task Fo
Functional Safety

SAE has provided this Draft document f
transmitted in any matter outside of the

SU
RE

Scope of this effort intends to
Theoretic Process Analysis (S
safety-critical content.

Purpose of this workgroup is
automotive industry regarding
autonomous driving applicatior

Contents

DRAFT
SAE International

SAE STPA Task Force - Functional Safety Committee Activities – Group 2 HMI

6. GROUP 2 – HUMAN-MACHINE INTERACTION (HMI) AND STPA

6.1 Introduction

This section describes STPA approaches to evaluate human-machine interaction (HMI) that Task Force STPA practitioners have found effective when conducting an STPA system safety evaluation.

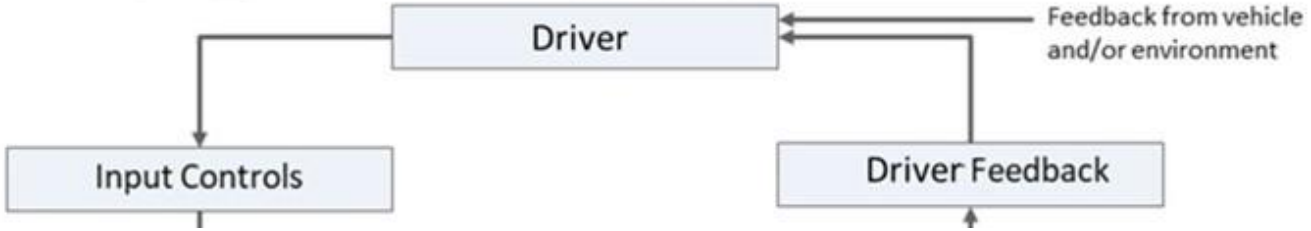
Objective data aids in, and is sometimes necessary for, the accommodation of safety requirements into human-machine interaction devices. Engineering teams responsible for the functional aspects and the design studio aspects of the human-machine interactions devices face pressures from many different perspectives such as cost, timing, and safety content. As such, discussions that do not include objective data may tend to become discussions where only opinions, interpretations, and perspectives drive decisions. Objective data should be diverse and relevant. The decision is likely to include a tradeoff of the different perspectives mentioned above so it's important to get objective data about all the aspects that are compared.

Add to this the fact that groups making human-machine interaction design decisions may not possess the skill set and experience of human factors scientists or researchers.

The challenge is how to obtain data easily understood by typical functional and design team engineers that support associated safety requirements to be included in the functional and design specifications. One solution is to associate requirements with causal scenarios that could lead to unsafe control actions resulting in hazardous conditions/accidents

STPA is useful when evaluating systems that contain expected driver and machine interactions as it enables the "driver" (or "vehicle occupant(s)") to be incorporated in the control structure as a functional element. In this context the driver has certain expected "functions" to perform that are evaluated as part of the guideword driven unsafe control action assessment portion of STPA Step 1. Once this was done, the possible causal scenarios that could lead to these unsafe control actions are evaluated and the constraints and/or requirements necessary to prevent or manage these causes to an acceptable risk level are defined.

The driver now becomes part of the STPA control structure as illustrated in Figure 16 below.



SAE STPA Task Force - Functional Safety Committee Activities – Group 2 HMI

The driver now becomes part of the STPA control structure as illustrated in Figure 16 below.

Human expansion construct focuses on three areas, the Mental Model Updates, the driver's Mental Models themselves, and the Control Action Selection. Figure 18 shows a more detailed view of these three areas. (FRANCE, March 2017)

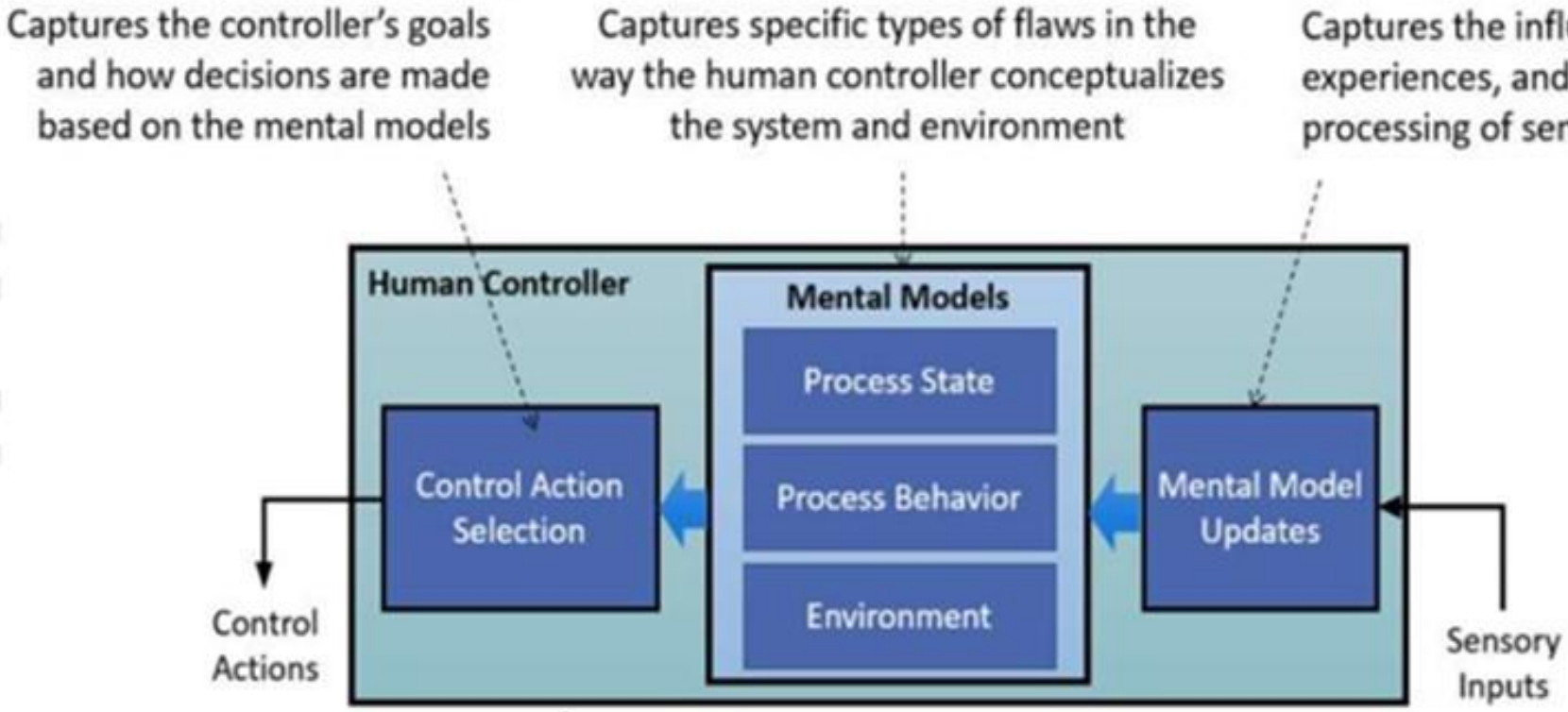
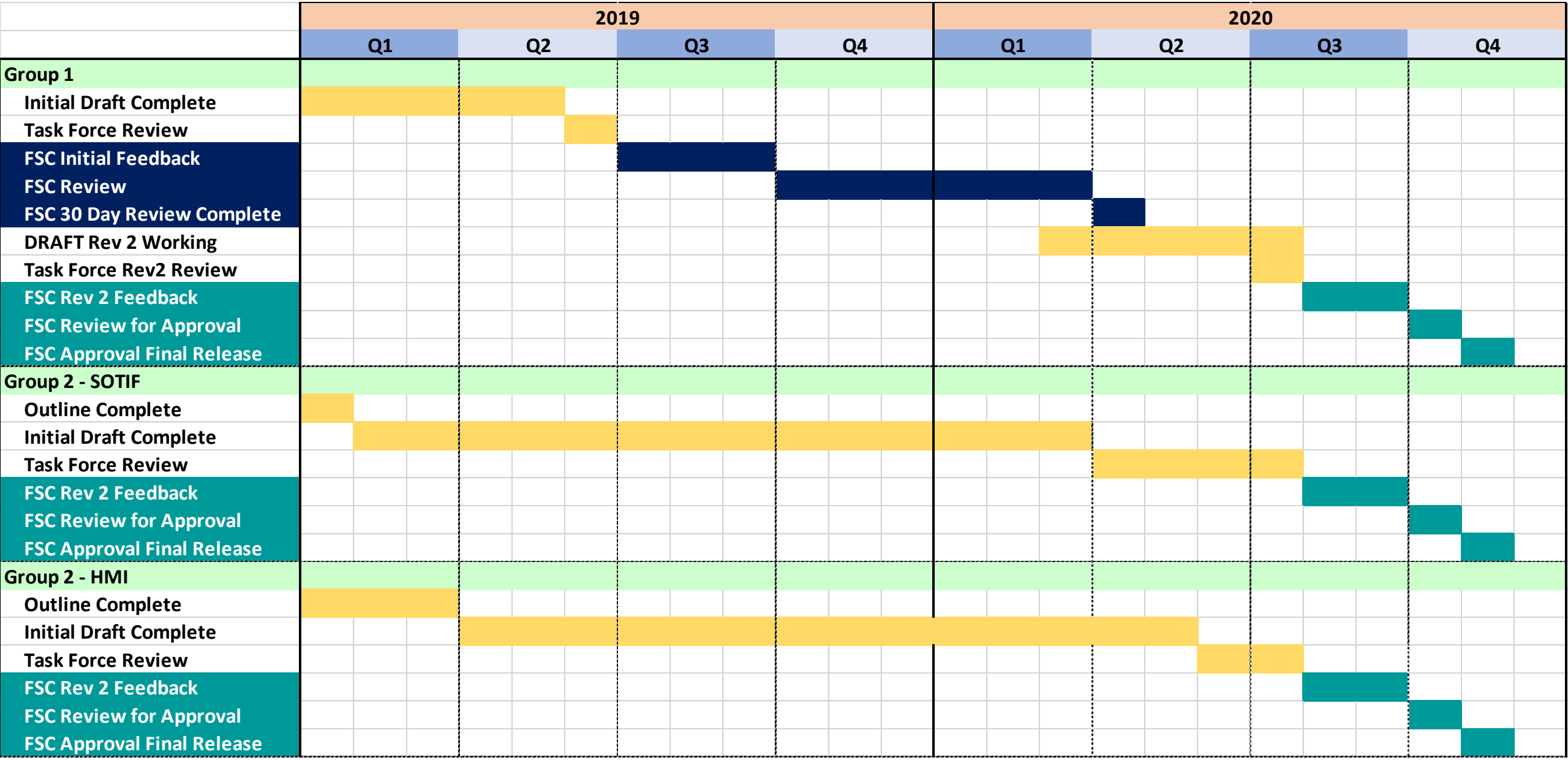
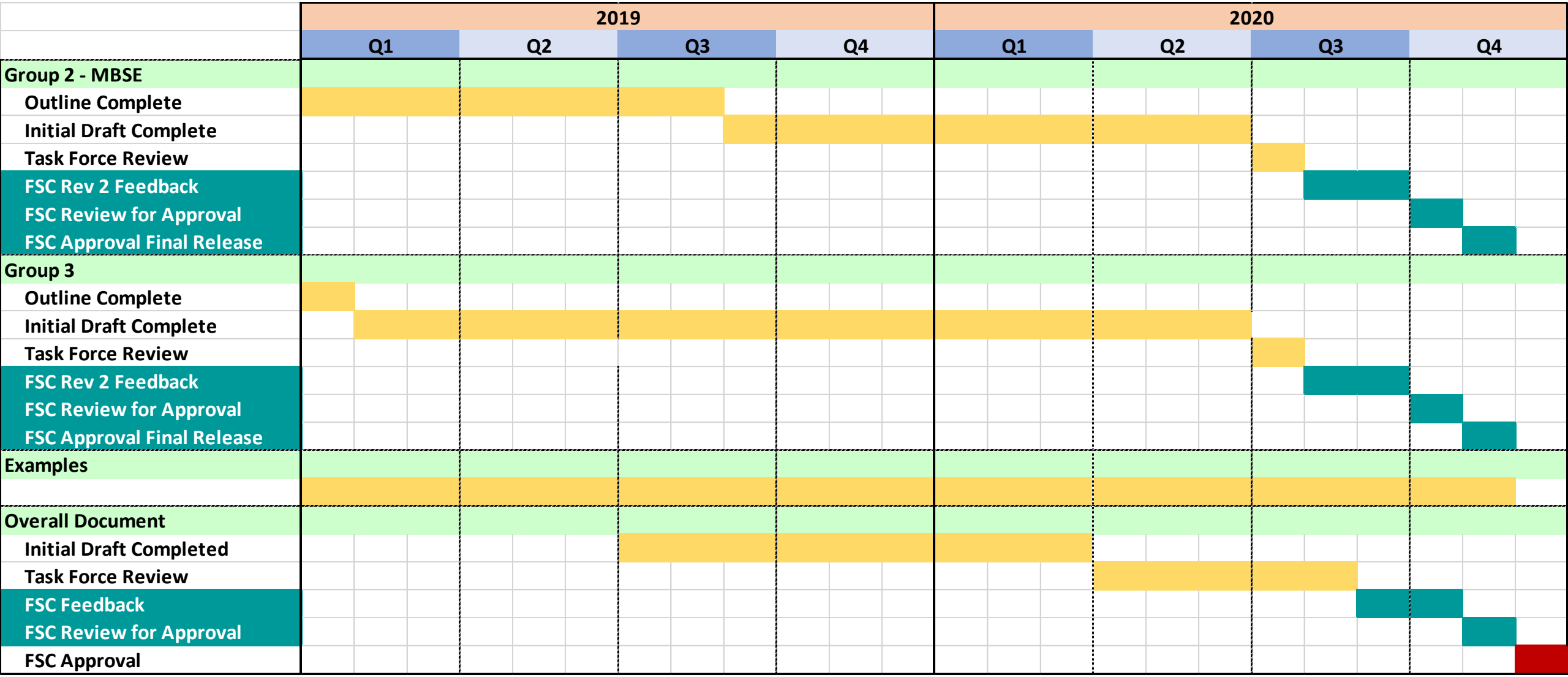


Figure 18: Detailed View of Human Expansion (FRANCE, March 2017)

SAE STPA Task Force – Schedule Outline



SAE STPA Task Force – Schedule Outline



Official Balloting Q1 2021

Backup

J3187 – Applying System Theoretic Process Analysis (STPA) to Automotive Applications

- SAE STPA Recommended Practice Task Force is open to knowledgeable practitioners who apply STPA to safety critical automotive applications

- Interested parties should contact:

mark.a.vernacchia@gm.com

J3187 – Applying System Theoretic Process Analysis (STPA) to Automotive Applications

Currently have 61 members - 33 organizations

- Nissan
- FCA
- Ford
- General Motors
- Waymo
- Toyota
- Mercedes-Benz USA
- MIT
- Luminar Technologies
- Boeing
- Rolls Royce
- WMG - Univ Warwick
- Zenuity
- SAE ORAD Working Group
- Edge Case Research
- VOLPE (US Depart of Trans)
- Jaguar Land Rover
- Continental (Germany)
- Magna Electronics Inc
- NVIDIA
- APTIV
- SAE Members
- Codethink
- Siemens PLM Software
- Autonomous Solutions
- Dura Automotive
- Exida
- Encoresemi
- Elektrobit
- SZ DJI Technology Co., Ltd.
- Autonomous Intelligent Drvg
- Cummins Inc
- Valeo

SAE STPA Task Force

Initial Feedback on Draft of Group 1 Document Aug 2020

- Feedback on content clarity, flow, and presentation desired

Initial Feedback on Draft of Group 2 HMI Content Q3 2020

- Feedback on content clarity, flow, and presentation desired

Initial Feedback on Draft of Group 3 Document Q3 2020

- Feedback on content clarity, flow, and presentation desired

Latest J-3187 document on FSC website have both Group 1 content (ready for review) and DRAFT Group 2 HMI content

SAE STPA Task Force - Recap

Under SAE Functional Safety Committee (under "ELECTRICAL SYSTEMS" box under the "Electrical Distribution Steering Committee"

SAE S-18 Aircraft & System Development and Safety Assessment Committee is working on a similar recommended practices document – Task Force has liaison members on S-18

SAE STPA Task Force Functio

Functional Safety Committee

Committee | Main | WIP | Documents | Committee Work Area | Roster | Ballots | Email

SAE Members Only | Email link to this page

Work Area for Functional Safety Committee

J-3187 -- SAE STPA Recommended Practice Task Force

Add: Folder | File | Topic

Posted	Delete	Edit	Replies	Latest
J-3187 SAE STPA Recom Practice DRAFT - Groups 1 -- 2-HMI Consolidated - 16apr20 Mon Apr 20 2020 9:41 AM EDT by Mark Vernacchia	D	Edit	0	Discuss Download
J-3187 SAE STPA Recommended Practice DRAFT - Groups 1 -- 2-HMI - 31mar20 Thu Apr 16 2020 9:29 AM EDT by Mark Vernacchia	D	Edit	0	Discuss Download
J-3187 SAE STPA Recommended Practice Updated DRAFT - 17dec19 Mon Feb 17 2020 3:06 PM EST by Mark Vernacchia	D	Edit	0	Discuss Download
Group 1 Feedback Form Tue Nov 19 2019 8:01 AM EST by Mark Vernacchia	D	Edit	0	Discuss Download
J-3187 SAE STPA Recommended Practice DRAFT - 07nov19 Tue Nov 19 2019 8:01 AM EST by Mark Vernacchia	D	Edit	0	Discuss Download

SAE STPA Task Force - Functional Safety Committee Activities – Group 2 HMI

This had led to an enhancement to the STPA approach that helps to understand three important constructs. Figure 17 shows the "human extension" (FRANCE, March 2017) integrated into a generic representation of the control structure.

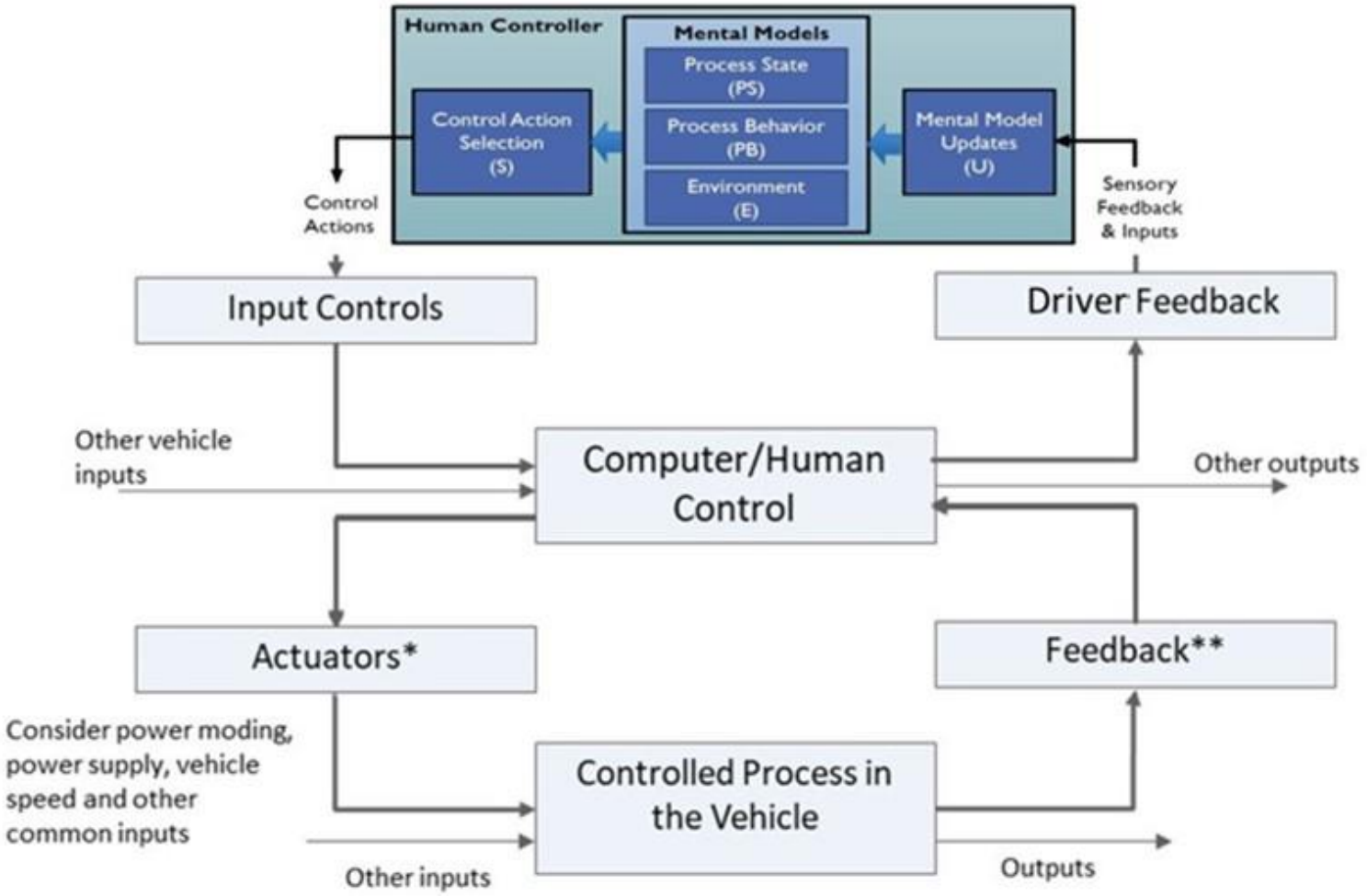
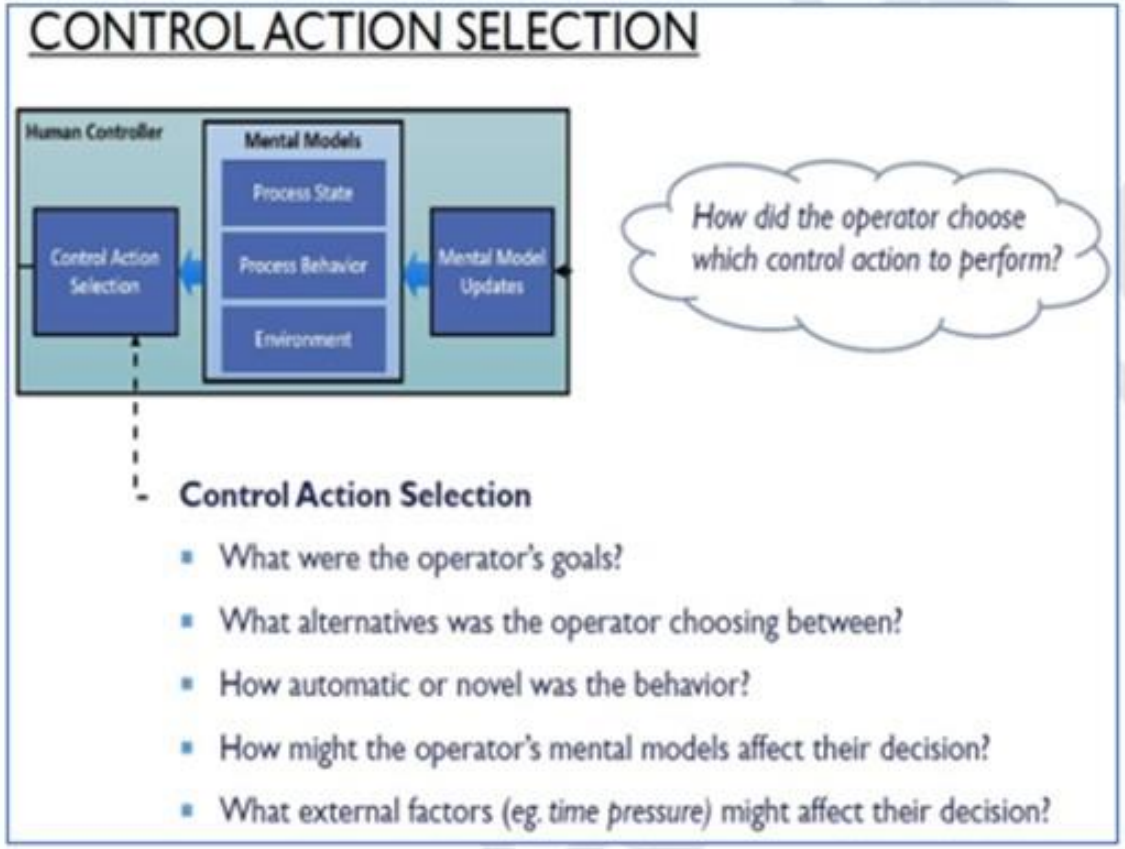


Figure 17: Human Expansion of Driver Element in Control Structure

SAE STPA Task Force - Functional Safety Committee Activities – Group 2 HMI



Control Action Selection
What were operator's goals?
To drive the vehicle
To have propulsion become active without physical button
To be able to turn the vehicle <OFF>
To allow the vehicle "run" after leaving the vehicle
What alternatives was the operator choosing between?
Turn vehicle <OFF>
Activate <Let Run> option
How automatic or novel was the behavior?
Very automatic to enable propulsion - no driver action
Very novel to turn vehicle <OFF>
Very novel to allow vehicle to continue to run <Let Run>
How might operator's mental models affect decisions?
Mental model of how to start car may impact driver interaction
MM of how to turn vehicle <OFF> may influence driver interaction
MM of how to get to <ACC> may influence driver interaction
MM of how to turn vehicle <OFF> at speed may influence driver interaction
External factors that might affect decision?
Vehicle automatically goes into propulsion with specific driver action
Vehicle automatically shuts <OFF> only after driver exits

Figure 28: Human Expansion Representation Example Questions and Answers

SAE STPA Task Force
Functional Safety Committee Activities – Group 1

3.12 LESSONS LEARNED

- Leverage systems engineering principles
  - Guidance (or examples) on how to create control structure by using systems engineering foundations
- Begin with simple control structures and then go deeper
  - Explain what to capture the system or function and how to create control structure as a recommendation
    - Provide examples of control structure; Hierarchical layered structure vs non- layered structure. This may help STPA beginners to understand which control structure is more verifiable
- Use STPA early in engineering design process
- Identify and engage a "chief system architect" for the system under review if available
- Use collateral from existing safety process tasks to avoid repeating in STPA. (For example, GM uses PHA and HARA to identify potential accidents and hazards and to assess their associated risk levels. This info can be inserted into STPA process to avoid parallel development of same info.)
- Leverage STPA outputs in Verification and Validation test plans and text cases
- STPA can complement, rather than replace, other methods – independent check, look at safety problem from multiple viewpoints.
  - For example, HAZOP may identify hazards based on function, while STPA may identify hazards based on unsafe control actions. These hazard identification techniques can be performed independently. Comparing the results can (1) make sure neither method overlooked a hazard, and (2) help develop more rigorous definitions of hazards (i.e., what does the hazard cover/not cover)
- Incorporation of safety requirements into appropriate technical documents for system content design, supplier provided entities, and validation test cases and planning
- Visualize the Loss Scenarios
  - Even if the UCA occurrence scenarios are complex due to interactive interference, it is possible to explain systematically in an easily understandable way by summarizing them from the control flow viewpoint. It is effective as safety argument.

The visualized loss scenario is helpful to plan the verification & validation such as to prepare the testing environments and to generate test cases

3.13 "Questions to Prepare for STPA"

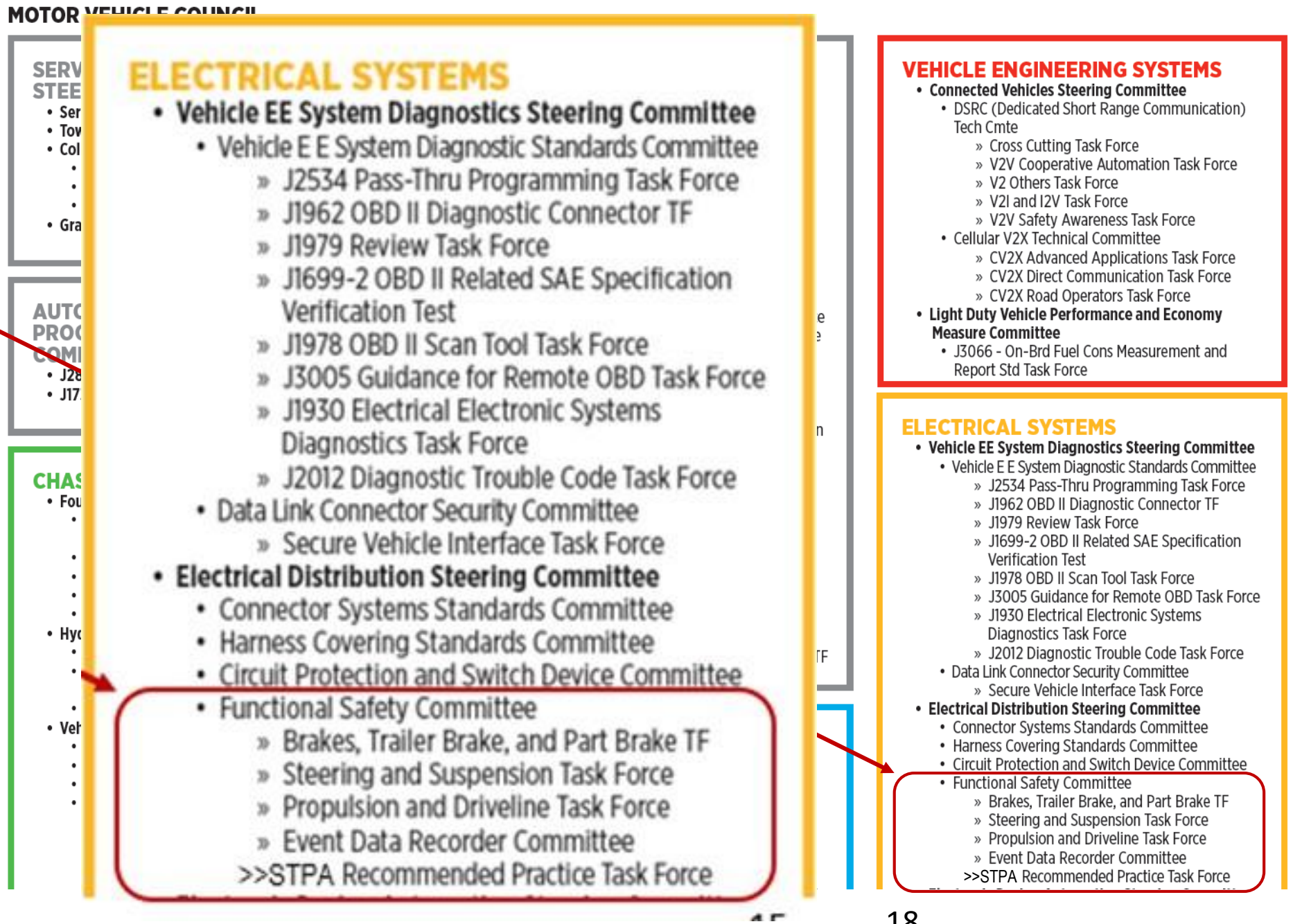
- What is the goal or mission of the system?
- What does the system look like from architecture, functional, process, or controls structure perspective?
- Is there an operational description of the system's expected functions, behaviors, capabilities and interactions with other systems, users, and human operators over expected operating scenarios?
- What are the required and expected functions for each of the system elements?
- Is there a priority of command to be maintained between different sub-systems during normal operation? Example would be holding vehicle stationary on hill with brakes and then wanting to accelerate up the hill, when are brake commands prioritized above accelerator pedal commands?
- What accidents is the system capable of causing?
- What are the hazardous conditions that may lead to any of these accidents?

3.14 "Questions While Performing STPA"

- What happens to the system when a system element fails or misbehaves?
- Does the resulting system behavior create potentially hazardous condition(s)?
- What are the risks and risk assessment associated with these potential hazards?
- Which part of the system assumes the failed/misbehaving element's functions?
- What are the resulting system capabilities after the failure /misbehavior?
- Do these resulting system capabilities create new/other potentially hazardous situations?
- Are these resulting system capabilities sufficient to achieving system goals/missions?
- What are required diagnostic strategies and level of rigor are necessary to detect failures or misbehaviors?
- What are the mitigation strategies and actions necessary to transition the system from a detected failed/misbehaving state to a known acceptable safe state?
- Based on the severity and exposure factors of the risk assessment (and potential operator controllability where applicable), is the residual risk acceptable?

DRAFT International © SAE International

Here it is !


MOTOR VEHICLE COUNCIL
ELECTRICAL SYSTEMS
• Vehicle EE System Diagnostics Steering Committee
• Vehicle E E System Diagnostic Standards Committee
» J2534 Pass-Thru Programming Task Force
» J1962 OBD II Diagnostic Connector TF
» J1979 Review Task Force
» J1699-2 OBD II Related SAE Specification Verification Test
» J1978 OBD II Scan Tool Task Force
» J3005 Guidance for Remote OBD Task Force
» J1930 Electrical Electronic Systems Diagnostics Task Force
» J2012 Diagnostic Trouble Code Task Force
• Data Link Connector Security Committee
» Secure Vehicle Interface Task Force
• Electrical Distribution Steering Committee
• Connector Systems Standards Committee
• Harness Covering Standards Committee
• Circuit Protection and Switch Device Committee
• Functional Safety Committee
» Brakes, Trailer Brake, and Part Brake TF
» Steering and Suspension Task Force
» Propulsion and Driveline Task Force
» Event Data Recorder Committee
>>STPA Recommended Practice Task Force
VEHICLE ENGINEERING SYSTEMS
• Connected Vehicles Steering Committee
• DSRC (Dedicated Short Range Communication) Tech Cmte
» Cross Cutting Task Force
» V2V Cooperative Automation Task Force
» V2 Others Task Force
» V2I and I2V Task Force
» V2V Safety Awareness Task Force
• Cellular V2X Technical Committee
» CV2X Advanced Applications Task Force
» CV2X Direct Communication Task Force
» CV2X Road Operators Task Force
• Light Duty Vehicle Performance and Economy Measure Committee
• J3066 - On-Brd Fuel Cons Measurement and Report Std Task Force
ELECTRICAL SYSTEMS
• Vehicle EE System Diagnostics Steering Committee
• Vehicle E E System Diagnostic Standards Committee
» J2534 Pass-Thru Programming Task Force
» J1962 OBD II Diagnostic Connector TF
» J1979 Review Task Force
» J1699-2 OBD II Related SAE Specification Verification Test
» J1978 OBD II Scan Tool Task Force
» J3005 Guidance for Remote OBD Task Force
» J1930 Electrical Electronic Systems Diagnostics Task Force
» J2012 Diagnostic Trouble Code Task Force
• Data Link Connector Security Committee
» Secure Vehicle Interface Task Force
• Electrical Distribution Steering Committee
• Connector Systems Standards Committee
• Harness Covering Standards Committee
• Circuit Protection and Switch Device Committee
• Functional Safety Committee
» Brakes, Trailer Brake, and Part Brake TF
» Steering and Suspension Task Force
» Propulsion and Driveline Task Force
» Event Data Recorder Committee
>>STPA Recommended Practice Task Force

18