Integration of STPA into GM System Safety Process

Mark A. Vernacchia, PE

GM Technical Fellow

Principal System Safety Engineer – Propulsion Systems

MIT STAMP Workshop
March 27, 2018

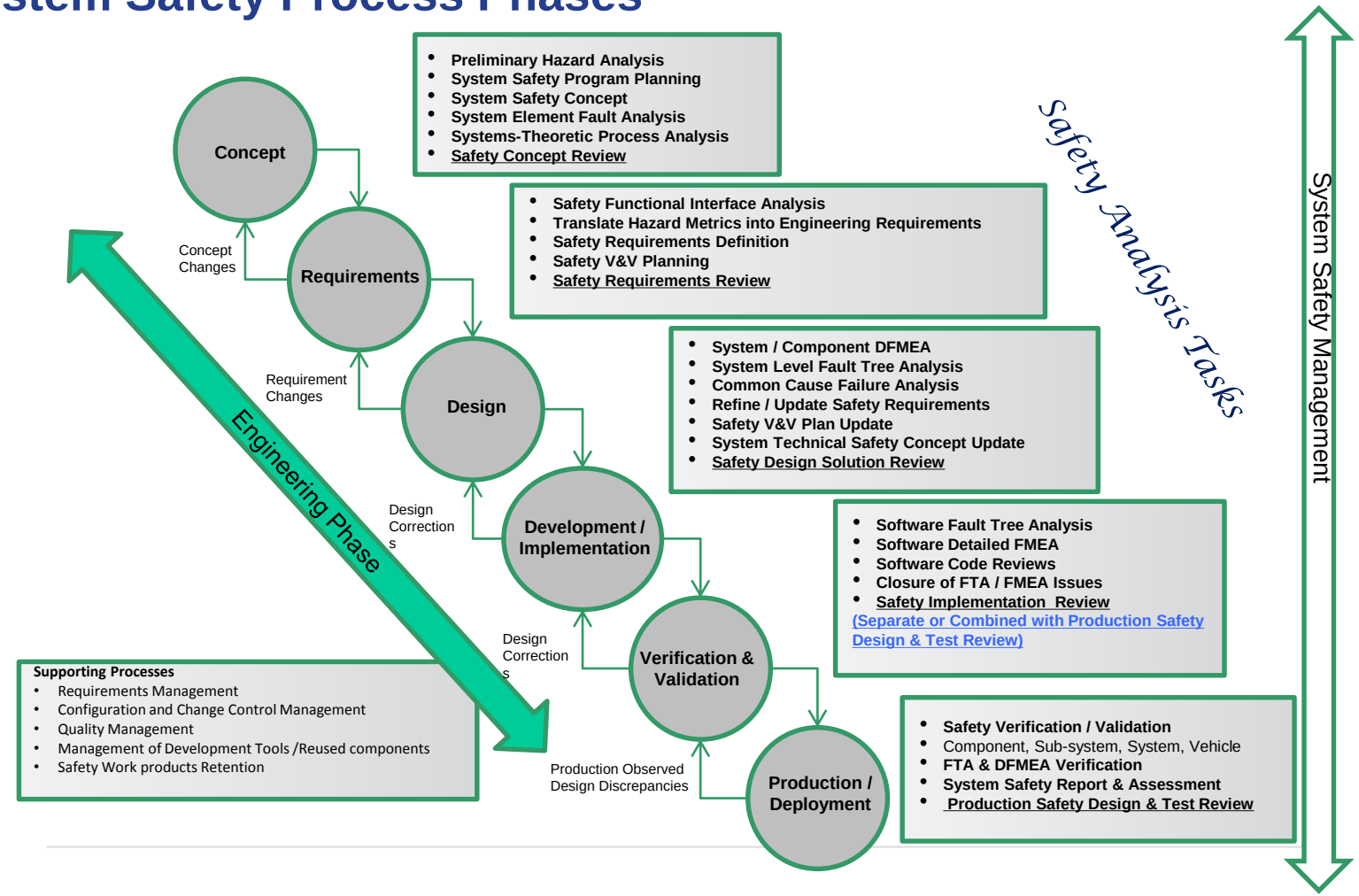
Integration of STPA into GM System Safety Process

- *Why Do This?*
  - *ISO26262 does not sufficiently address the evaluation of human behavior as part of its process as thoroughly as GM desires for HMI*
  - *This is an instance of the GM strategy to incorporate the “best of the best” from system safety sources outside of GM*

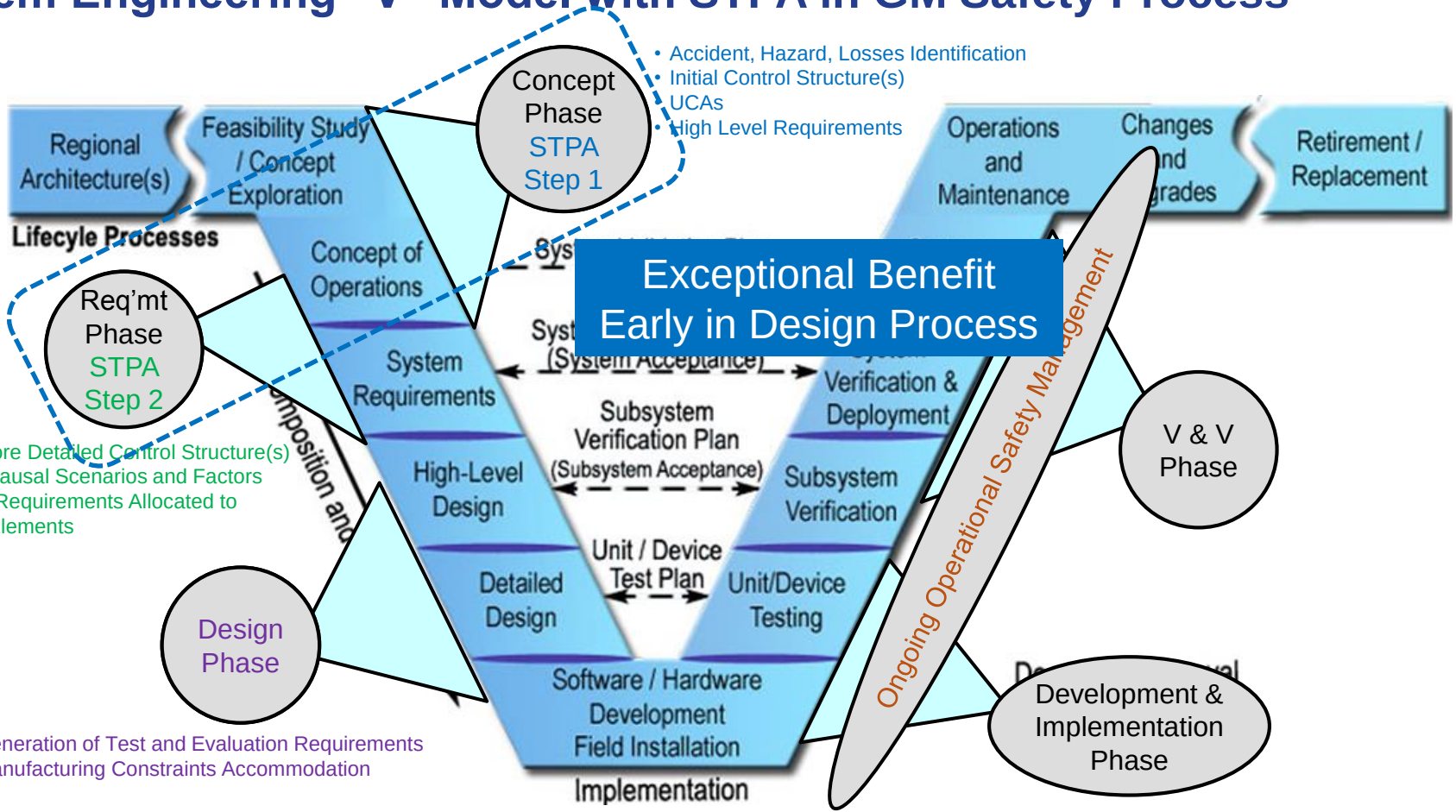
Integration of STPA into GM System Safety Process

- *STPA evaluations are currently being done on safety critical systems containing driver Human-Machine Interaction (HMI) functions*
- *List of safety critical systems with human-machine interactions includes, but is not limited to, systems such as:*
  - *Ignition Systems*
  - *ETRS (Shift by Wire) Shifting Devices*
  - *Electric Park Brake Controls*
  - *Adaptive Cruise Controls*
  - *Headlamp Switches*
  - *Trailer Brake Switches*
  - *Seat Switches*

GM System Safety Process Phases



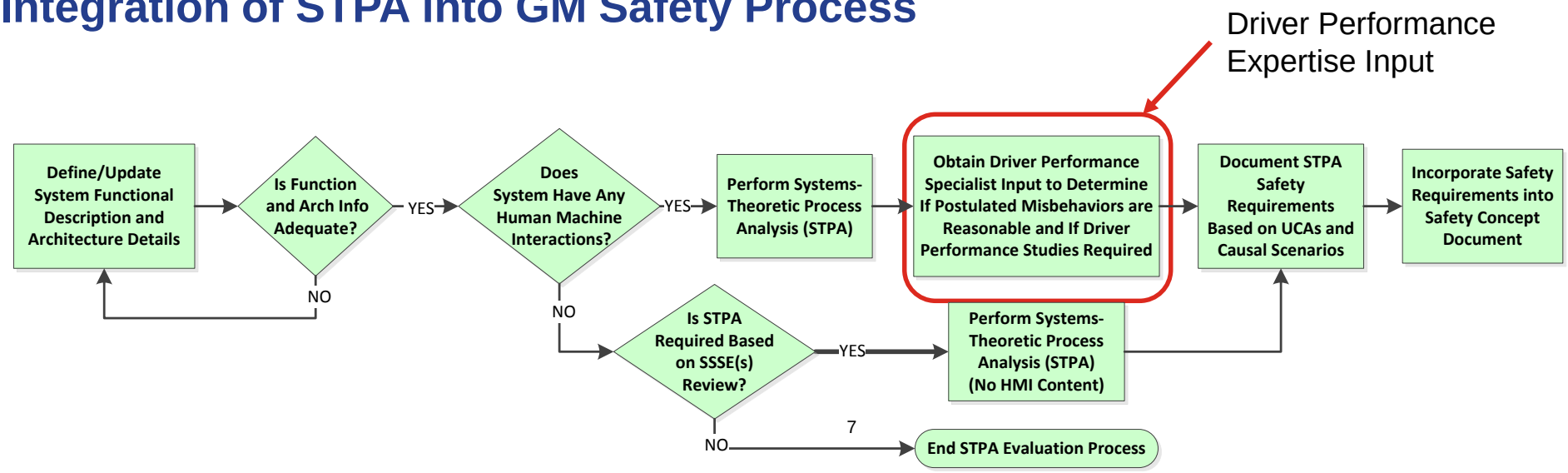
System Engineering "V" Model with STPA in GM Safety Process



Integration of STPA into GM Safety Process – HMI Critical Applications

- *PHA / HARA are performed before initiating STPA evaluation*
- *The "System" and "System Functions" activities that describe and/or define either physical or function architecture, intended system functions and expected behaviors are to be available before initiating any STPA evaluation*

Integration of STPA into GM Safety Process

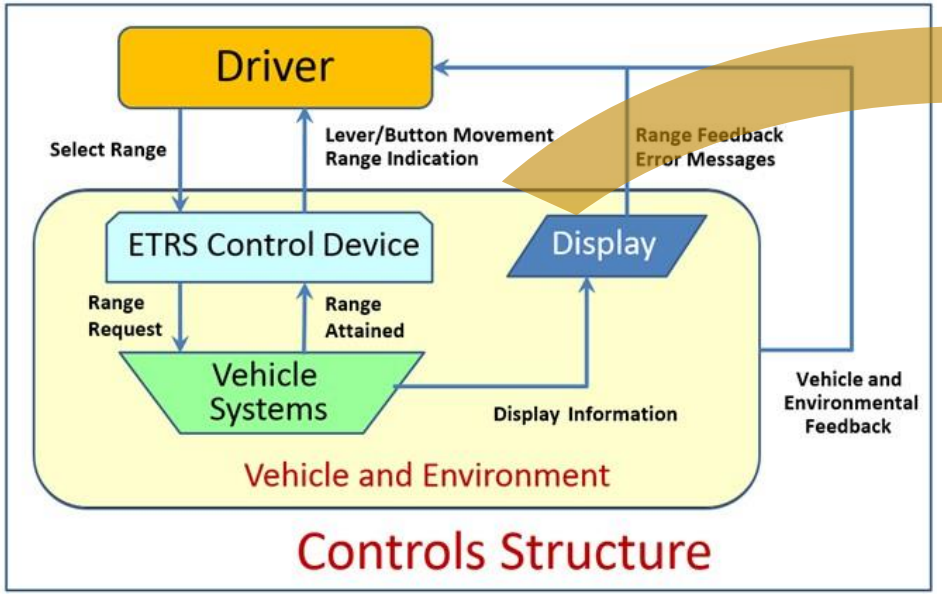


Driver Performance Expertise input is essential to determine plausible driver misbehaviors and to assess if performance studies or clinics are required

Integration of STPA into GM Safety Process – ETRS Example

Integration of STPA into GM Safety Process – ETRS Example

Define system content (control structure) and the interactions between the driver and the system



STPA ACTIVITIES

Determine possible causal scenarios that could result in any UCA

37 UCAs Defined

100 Potential Causal Scenarios Defined

UCA	Potential C
UCA1: Driver does not put car in Park on hill	Driver is distracted, or in a panic mode, or is rushing to decide to get into park
UCA1: Driver does not put car in Park on hill	Driver already thinks the car is in Park because of a previous action
UCA1: Driver does not put car in Park on hill	Driver thinks it is already in Park because belief the vehicle will do it automatically
UCA1: Driver does not put car in Park on hill	Driver cannot find Park
UCA1: Driver does not put car in Park on hill	Driver performs prior habitual actions leads to not selecting Park in this vehicle (Prior Learned Behavior)
UCA1: Driver does not put car in Park on hill	System feedback is confusing to driver

STPA ACTIVITIES

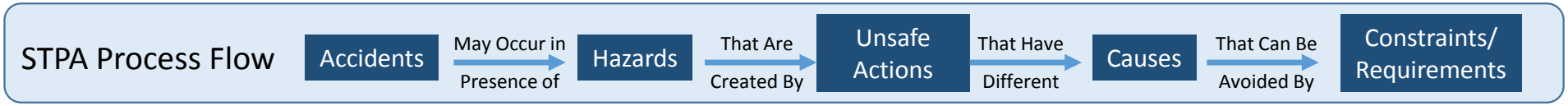
Condense functional and design constraints into requirements

Meets FMVSS Requirements 101, 102, and 114
Buttons, Knobs, Levers Must Be "Mono-Stable" (momentary activation)
Brake, plus two motions, necessary to exit Park; P => N (Safe)
One motion from D => N (Easy)
Two Motions to get to Reverse from any "Drive" gear (D,L,M)
Controls are clearly identified and obvious, easily accessible
Park button easy to find

Incorporation of STPA Requirements into Appropriate Sub-System and Component Specification Documents And into Design Center “Best Practices”

Integration of STPA into GM Safety Process – ETRS Example

- *Understanding requirements linkage to potential hazardous states allowed "Design Center" teams to accommodate safety requirements (data driven)*



- *STPA derived requirements 2018 GMC Terrain Push-Button design:*
  - *Different motions to obtain Drive or Reverse versus Neutral or Park*
  - *Pull buttons for any propulsion range selection (Reverse and Drive)*
  - *One motion (push to get easily to Park or to Neutral)*
  - *Buttons laid out in familiar, expected pattern (PRNDL)*
  - *Buttons do not latch, instead are mono-stable*
  - *Software content to manage inappropriate shift requests while at speed*
  - *Auto-park capability if vehicle not placed in Park when required*

Integration of STPA into Concept Phase of GM Safety Process - Results

“I spent 20 minutes trying to overcome the GMC shifter’s electronic safeguards. I tried stupid human tricks like shifting a moving vehicle into park and opening the door to step out it while it was still in gear. It’s dangerous to call anything foolproof, because fools are so persistent, but on first inspection the new shifter sure comes close.”

“It’s a risk when you redo a system and move away from something everybody knows how to operate,” IHS Markit senior analyst Stephanie Brinley said after testing the system. “It seems very intuitive,” Brinley said. “GMC built a system with which mistakes should be infrequent and minor.”

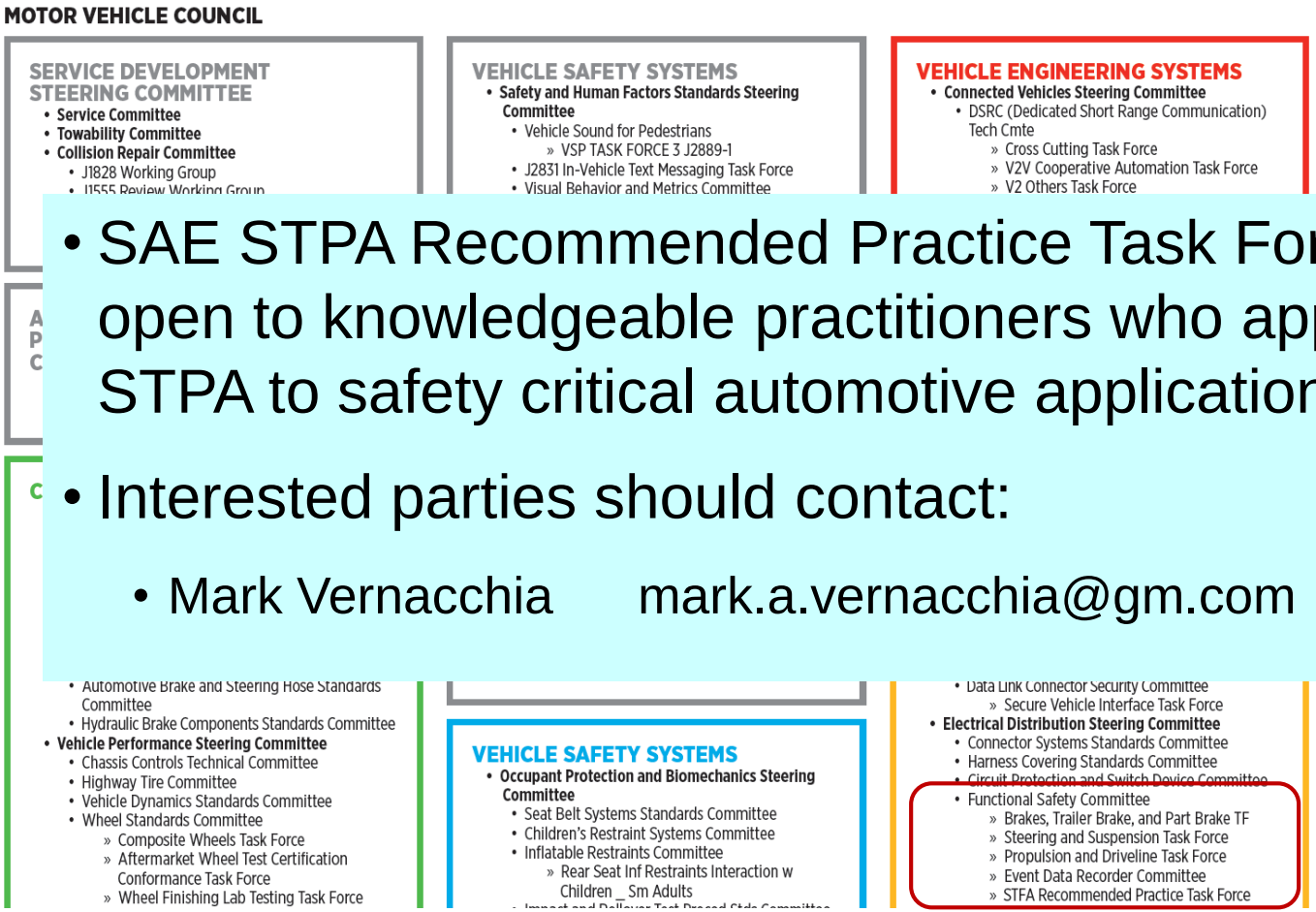
Mark Phelan ,
Detroit Free Press
Auto Critic
Published 10:38 p.m. ET July 1, 2017 **Updated 4:24 p.m. ET July 2, 2017**

http://www.freep.com/story/money/cars/mark-phelan/2017/07/02/gmc-2018-terrain-suv/441807001/
for video and full article

Integrate STPA into GM Safety Process – Key Points

- *STPA now part of formal GM Safety Process for HMI projects*
- *STPA generated requirements are captured in Safety documents and allocated into formal requirement document(s)*
- *STPA content and generated requirements have been used to drive production released design content and functions*
- *SAE STPA Recommended Practice task force formed under SAE Functional Safety Committee to provide both educational materials and recommended practices in regards to how STPA may be applied within a safety assessment process focusing on automotive vehicle safety-critical content*

Integrate STPA into GM Safety Process – SAE STPA Task Force



- SAE STPA Recommended Practice Task Force is open to knowledgeable practitioners who apply STPA to safety critical automotive applications
- Interested parties should contact:
  - Mark Vernacchia mark.a.vernacchia@gm.com

Here it is !