GM Presentation for Introducing STAMP/STPA Tools into Standards

SAE STPA Recommended Practice Task Force

Mark A. Vernacchia, PE

GM Technical Fellow

Principal System Safety Engineer – Propulsion Systems

MIT STAMP Workshop
March 27, 2018

GENERAL MOTORS

SAE STPA Recommended Practice Task Force - Background

- Outgrowth of meeting of automotive companies attending the MIT STAMP/STPA workshop in March 2017
- These companies have been working with STPA methodologies, some more than others
- Common desire to exchange STPA application and execution approaches and share lessons learned without compromising IP or competitive knowledge
- Interested parties worked during spring and summer of 2017 to outline possible scope, purpose and document content
- Task force to be under SAE Functional Safety Committee

SAE STPA Recommended Practice Task Force - Scope

- **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 vehicle safety-critical content
- **Relevant Landscape:** STPA to be blended with SAE Functional Safety Committee, ISO26262, and ISO SOTIF PAS initiatives
- **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 which focus areas are suited for STPA use, or for supplementing other safety evaluation tools

SAE STPA Recommended Practice Task Force – Effort Content/Structure

- Basic STPA approaches/content
- Specialized application of STPA to specific topics like HMI, software development, autonomous vehicles, cyber security, etc.
- Use of STPA within a safety process (when, how, why . .)
- How STPA compares to, and should be used with, other safety evaluations such as FTAs, FMEAs, FIAs, etc.
- Recommended practices for domain areas including scope of the analysis (what’s in, what’s out . .)
- Common glossary of terms and definitions
- Examples of actual STPA evaluations

SAE STPA Recommended Practice Task Force – Alignment in SAE Hierarchy

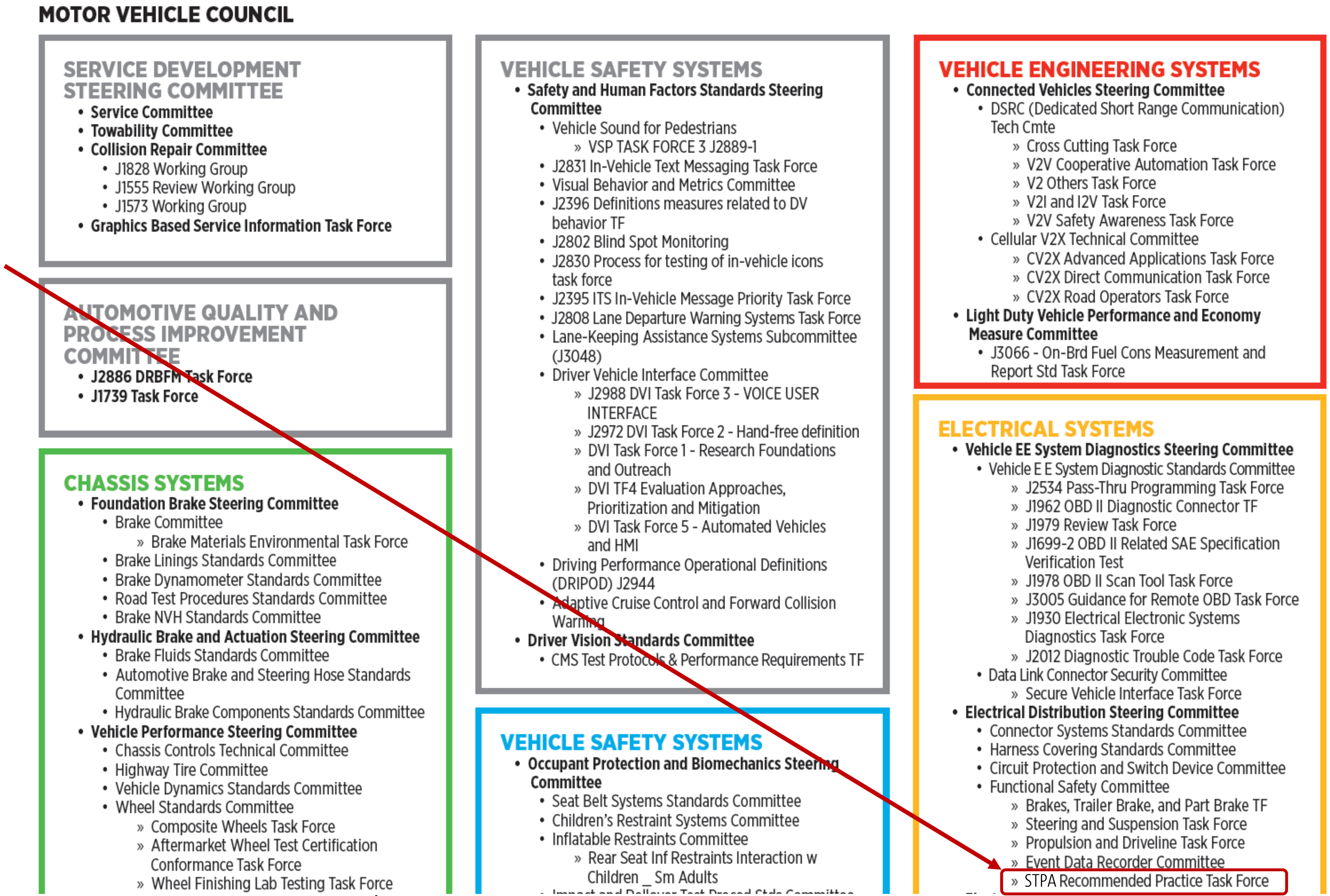
- Motor Vehicle Council
  - Electrical Systems Group
    - Electrical Distributions Steering Committee
      - Functional Safety Committee
        - STPA Recommended Practice Task Force

Initial Meeting was held on February 1st , 2018

Currently meeting every 1st and 3rd Thursday from 6 – 7 pm via Web-Ex Teleconference

SAE STPA Recommended Practice Task Force – Alignment in SAE Hierarchy

Here it is !



MOTOR VEHICLE COUNCIL

SERVICE DEVELOPMENT STEERING COMMITTEE

- **Service Committee**
- **Towability Committee**
- **Collision Repair Committee**
  - J1828 Working Group
  - J1555 Review Working Group
  - J1573 Working Group
- **Graphics Based Service Information Task Force**

AUTOMOTIVE QUALITY AND PROCESS IMPROVEMENT COMMITTEE

- **J2886 DRBFM Task Force**
- **J1739 Task Force**

CHASSIS SYSTEMS

- **Foundation Brake Steering Committee**
  - Brake Committee
    - » Brake Materials Environmental Task Force
  - Brake Linings Standards Committee
  - Brake Dynamometer Standards Committee
  - Road Test Procedures Standards Committee
  - Brake NVH Standards Committee
- **Hydraulic Brake and Actuation Steering Committee**
  - Brake Fluids Standards Committee
  - Automotive Brake and Steering Hose Standards Committee
  - Hydraulic Brake Components Standards Committee
- **Vehicle Performance Steering Committee**
  - Chassis Controls Technical Committee
  - Highway Tire Committee
  - Vehicle Dynamics Standards Committee
  - Wheel Standards Committee
    - » Composite Wheels Task Force
    - » Aftermarket Wheel Test Certification Conformance Task Force
    - » Wheel Finishing Lab Testing Task Force

VEHICLE SAFETY SYSTEMS

- **Safety and Human Factors Standards Steering Committee**
  - Vehicle Sound for Pedestrians
    - » VSP TASK FORCE 3 J2889-1
  - J2831 In-Vehicle Text Messaging Task Force
  - Visual Behavior and Metrics Committee
  - J2396 Definitions measures related to DV behavior TF
  - J2802 Blind Spot Monitoring
  - J2830 Process for testing of in-vehicle icons task force
  - J2395 ITS In-Vehicle Message Priority Task Force
  - J2808 Lane Departure Warning Systems Task Force
  - Lane-Keeping Assistance Systems Subcommittee (J3048)
  - Driver Vehicle Interface Committee
    - » J2988 DVI Task Force 3 - VOICE USER INTERFACE
    - » J2972 DVI Task Force 2 - Hand-free definition
    - » DVI Task Force 1 - Research Foundations and Outreach
    - » DVI TF4 Evaluation Approaches, Prioritization and Mitigation
    - » DVI Task Force 5 - Automated Vehicles and HMI
  - Driving Performance Operational Definitions (DRIPOD) J2944
  - Adaptive Cruise Control and Forward Collision Warning
- **Driver Vision Standards Committee**
  - CMS Test Protocols & Performance Requirements TF

VEHICLE SAFETY SYSTEMS

- **Occupant Protection and Biomechanics Steering Committee**
  - Seat Belt Systems Standards Committee
  - Children's Restraint Systems Committee
  - Inflatable Restraints Committee
    - » Rear Seat Inf Restraints Interaction w Children _ Sm Adults
  - Impact and Rollover Test Proced Stds Committee

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

SAE STPA Recommended Practice Task Force - Summary

Currently have 16 members from 11 companies

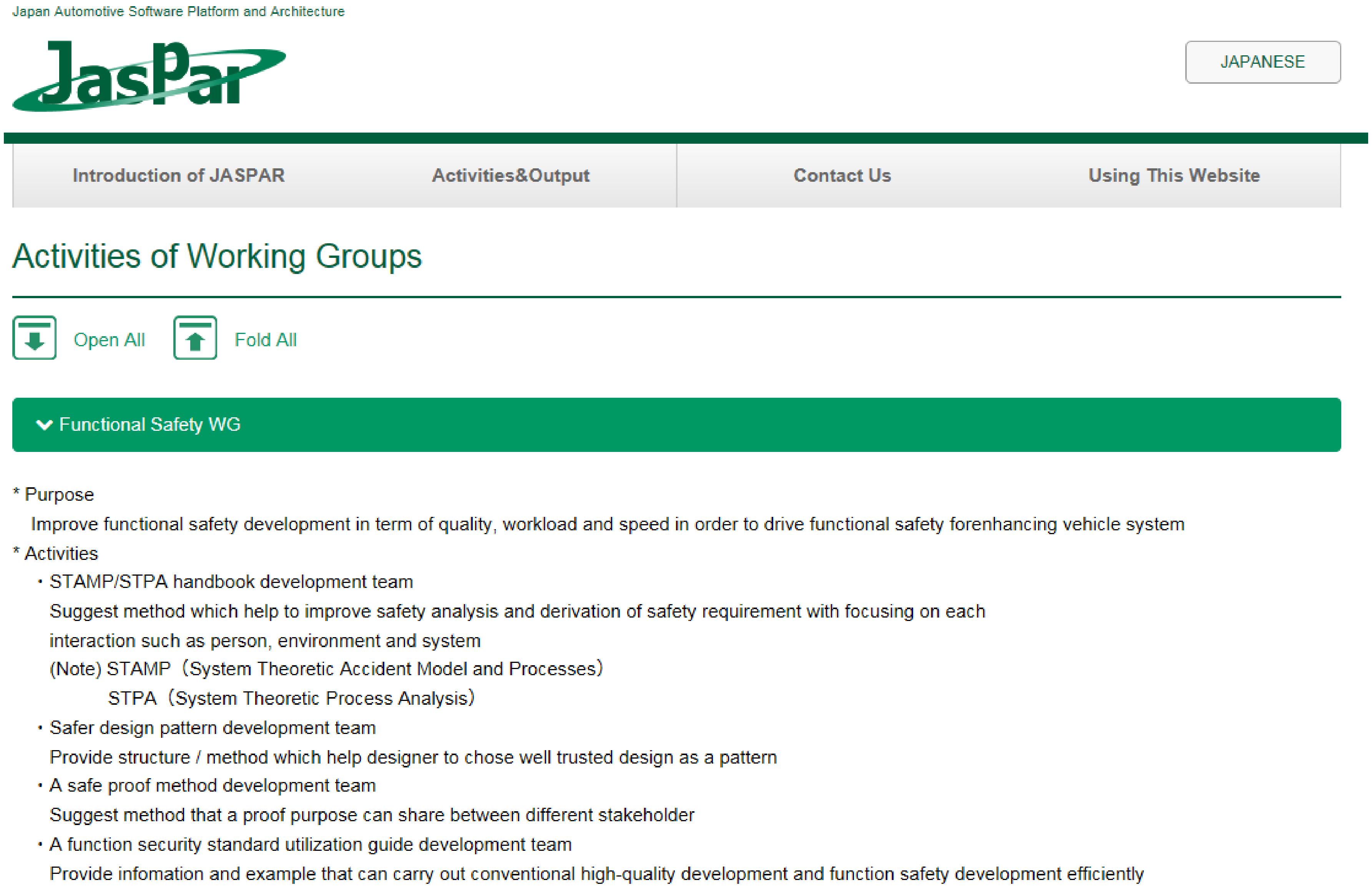
- General Motors, Ford, FCA, Nissan, Waymo, Mercedes-Benz, Toyota, Renesas (Waterloo), and MIT included in initial membership with Boeing and Rolls Royce members from SAE S-18 Committee as “liaison” members

- Exploring how to create liaison relationship with JASPAR with goal to incorporate SW perspective into effort

- 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

SAE STPA Recommended Practice Task Force - Summary



Activities of Working Groups

Functional Safety WG

* Purpose

Improve functional safety development in term of quality, workload and speed in order to drive functional safety forenhancing vehicle system

* Activities

- STAMP/STPA handbook development team
  Suggest method which help to improve safety analysis and derivation of safety requirement with focusing on each interaction such as person, environment and system
  (Note) STAMP（System Theoretic Accident Model and Processes）
  STPA（System Theoretic Process Analysis）
- Safer design pattern development team
  Provide structure / method which help designer to chose well trusted design as a pattern
- A safe proof method development team
  Suggest method that a proof purpose can share between different stakeholder
- A function security standard utilization guide development team
  Provide infomation and example that can carry out conventional high-quality development and function safety development efficiently