A CYBERSECURITY PROTECTION FRAMEWORK TO SUPPORT DUBAI'S SELF-DRIVING TRANSPORT STRATEGY

DUBAI WORLD CONGRESS
FOR SELF DRIVING TRANSPORT
October 15, 2019

Dr. Juan Pimentel
Principal Consultant



Omnex provides training, consulting and software solutions to the international market with offices in the USA, Canada, Mexico, China (PRC), Germany, India, the Middle East, and SE Asia. Omnex offers over 400 standard and customized training courses in business, quality, environmental, food safety, laboratory and health & safety management systems worldwide.

Email: info@omnex.com

Web: www.omnex.com

Omnex Introduction

- International consulting, training and software development organization founded in 1985.
- Specialties:
  - Integrated management system solutions.
  - Elevating the performance of client organizations.
  - Consulting and training services in:
    - Quality Management Systems, e.g. ISO 9001, IATF 16949, AS9100, QOS
    - Environmental Management Systems, e.g. ISO 14001
    - Health and Safety Management Systems, e.g. ISO 45001
- Leader in Lean, Six Sigma and other breakthrough systems and performance enhancement.
  - Provider of Lean Six Sigma services to Automotive Industry via AIAG alliance.

About Omnex

- Headquartered in Ann Arbor, Michigan with offices in major global markets.
- In 1995-97 provided global roll out supplier training and development for Ford Motor Company.
- Trained more than 100,000 individuals in over 30 countries.
- Workforce of over 700 professionals, speaking over a dozen languages.
- Former Delegation Leader of the International Automotive Task Force (IATF) responsible for ISO/TS16949.
- Served on committees that wrote QOS, ISO 9001, ISO 14001, ISO 45001, ISO 13485 QS-9000 and it's Semiconductor Supplement, ISO IWA 1 (ISO 9000 for healthcare).
- Supported current or previous revisions of FMEA, SPC, MSA, Sub-tier Supplier Development, Error Proofing, and Effective Problem Solving (EPS).

Omnex Key Global Offices

AMERICAS

USA - Ann Arbor, MI, San Jose, California
CANADA - Mississauga
MEXICO - Oaxaca
COLOMBIA - Bogota DC
BRAZIL - Sao Paulo

EUROPE

GERMANY - Berlin

EASTERN EUROPE

POLAND, RUSSIA, HOLLLAND, CZECH RE-PUBLIC, HUNGARY,

ASIA-PACIFIC

INDIA - Chennai (Asia Pac HQ), Pune, Delhi, Vadodara Bangalore
CHINA - Shanghai (Far East HQ), Guangzhou, Wuhan, Chongqing, Suzhou
THAILAND - Bangkok
UAE - Dubai
SINGAPORE - Singapore
MALAYSIA - Kuala Lumpur (Rep)

Dr. Juan Pimentel

Dr. Juan Pimentel is an Omnex consultant with extensive Engineering, Safety and Cybersecurity experience. He just retired as a Professor of Electrical and Computer Engineering at Kettering University. His knowledge and experience includes applied research, product development, safety and cybersecurity assessment and assurance. He is passionate about using processes and methodologies to design and manufacture products and systems with a high level of safety and security. In addition to assuring safety and cybersecurity though compliance/conformance he understands the need for reducing costs.

Dr. Pimentel has extensive experience in the oil & gas, chemical, and automotive industries, and has been a senior consultant to several institutions in Dubai and the Middle East in the areas of safety and cybersecurity of process and industrial control systems. He is the author of many papers on the safety and security of automotive systems ranging from drive-by-wire systems to ADAS to automated vehicles. He has developed and conducted professional training courses on safeguarding process control systems, safety instrumented systems (SIS), protecting industrial systems including relevant standards (IEC 61508, IEC 61511, and ISO 26262). In 2006 he edited a book for SAE on automotive safety critical systems. Just recently he completed editing a series of five books for SAE International on the “Safety of Automated Vehicles” dealing with its characterization, the use of ISO 26262, Multi-agent safety, SOTIF (Safety of the Intended Functionality), and Semiconductor safety.

Agenda

- Introduction
- Discuss the main elements of a cybersecurity protection framework for a city such as Dubai,
- Discuss novel cybersecurity threats for Self Driving vehicles involving:
  - RF technologies
  - Emerging self-driving technologies
- Discuss appropriate vulnerability handling and incident response techniques.
- Conclusions

Why Does Cybersecurity Matter?

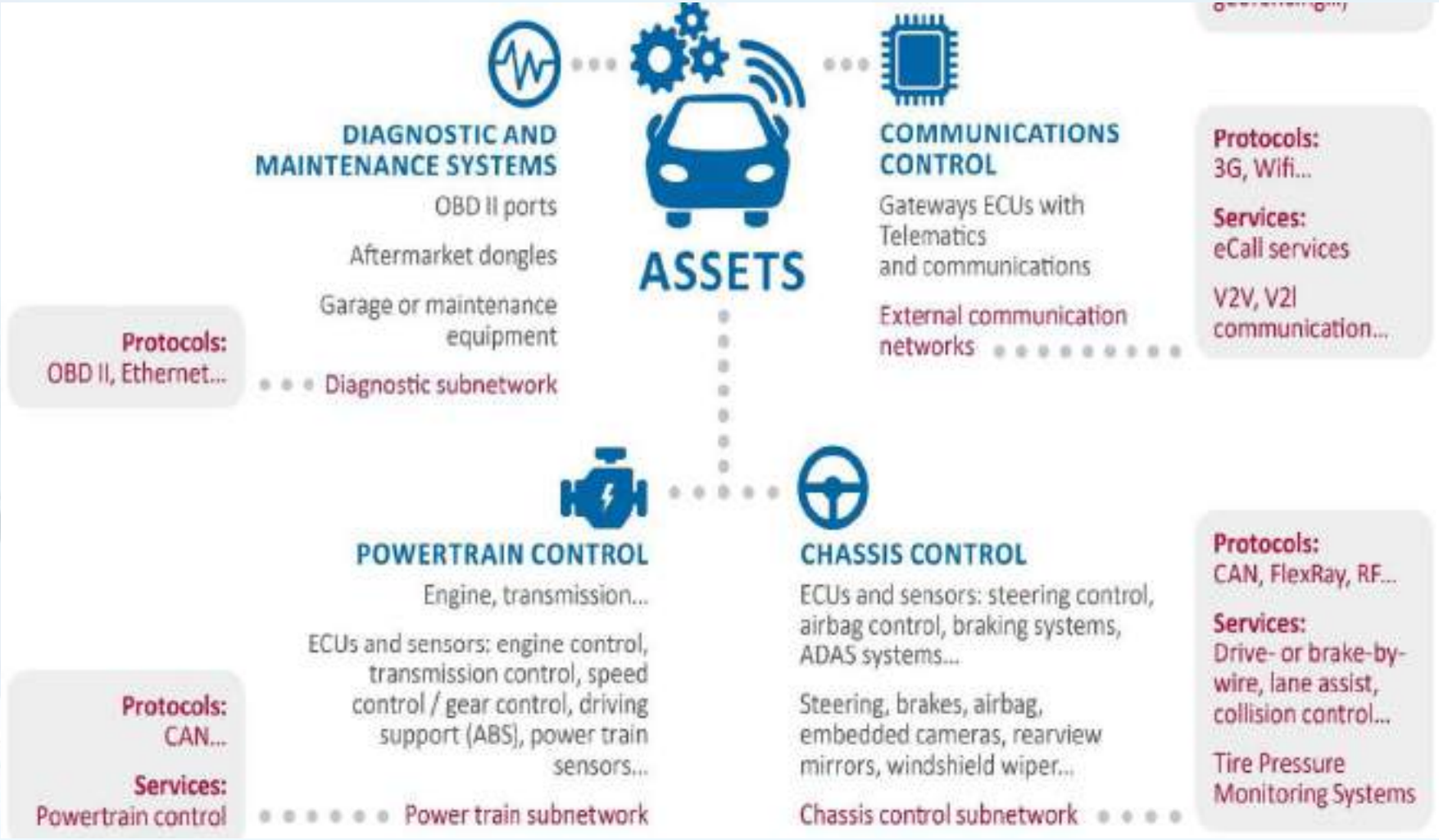
- Remote hacking of a Jeep Cherokee on a highway (2014)
- Emissions data manipulation using the OBD-II port.
- Multiple vulnerabilities of the CAN bus.
- Multiple vulnerabilities of the MCUs.
- Multiple attack vectors involving wireless channels:
  - WiFi
  - Cellular
  - BlueTooth (BT)
  - Infotainment system
  - GPS
  - Other RF channels

- Potential threats are being discovered continuously.

Cybersecurity Attack Surfaces

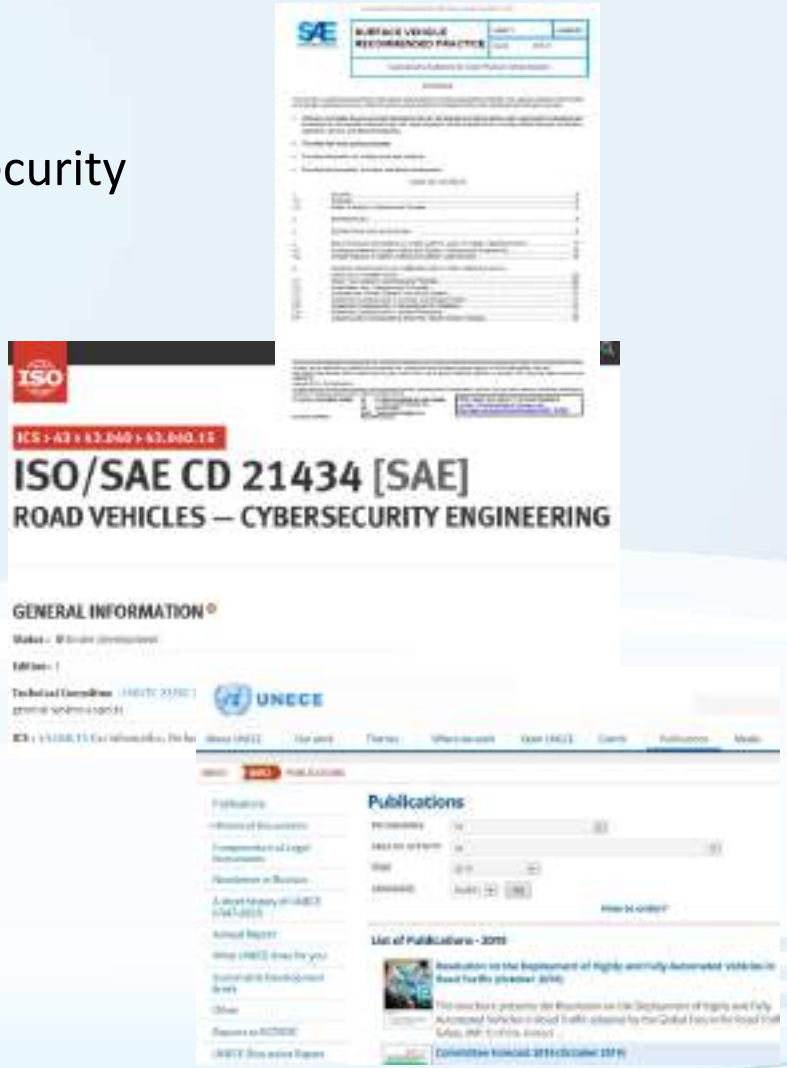
Autonomous Vehicle Assets

AV Assets (Continued)

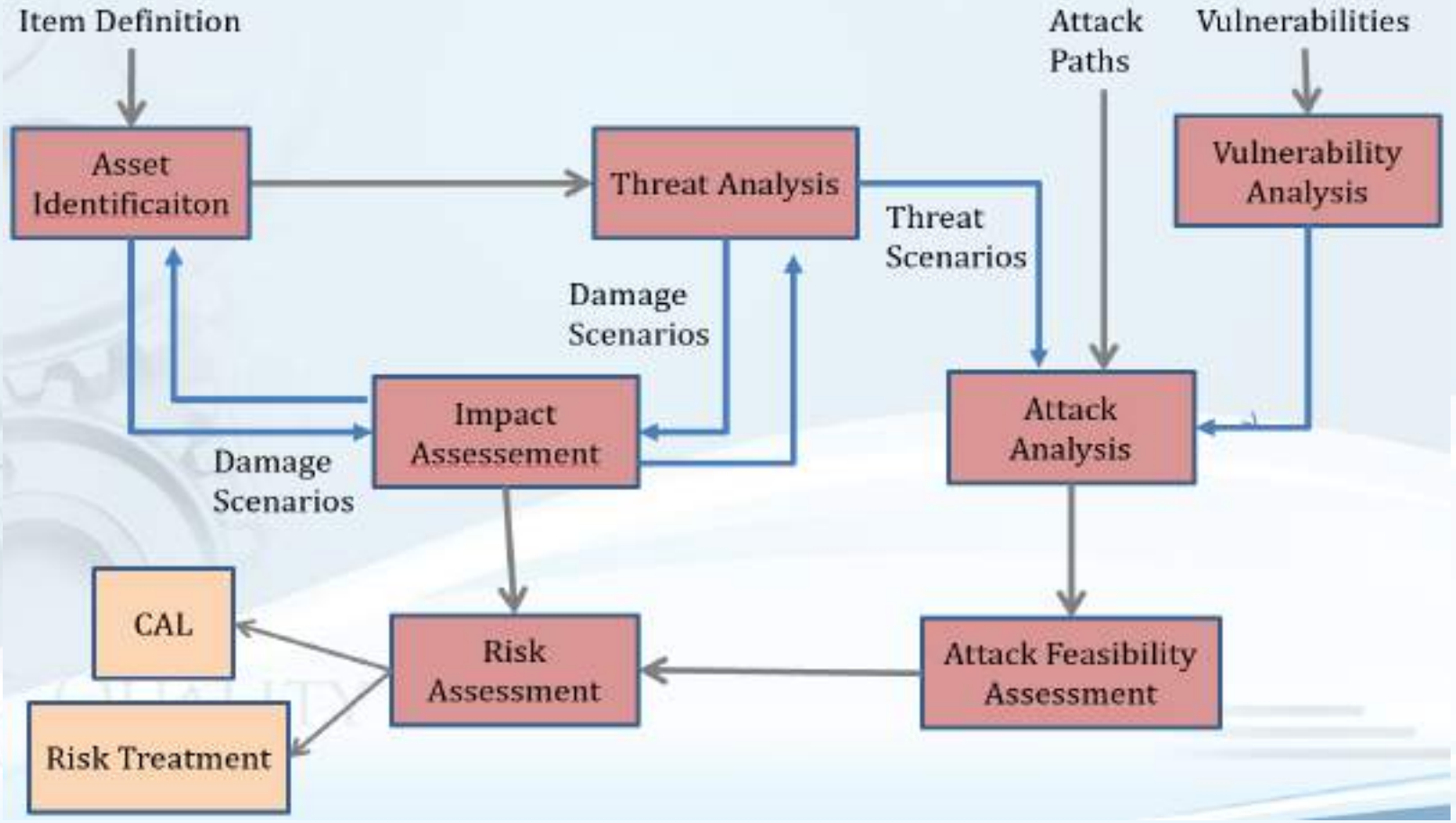


Main AV Existing Cybersecurity Frameworks

- SAE J3061
  - Recommendations for Vehicle Cybersecurity
  - Published (2016)
- ISO/SAE 21434
  - “Vehicle Cybersecurity Engineering”
  - CD Stage
- UNECE (United Nations Economic Commission for Europe) Regulation
  - Proposal Stage



ISO/SAE 21434 Cybersecurity Framework



Cybersecurity Protection Frameworks

- Dubai aims to transform 25% of the city's total mobility journeys into self-driving journeys by the year 2030.
- An outstanding challenge to this visionary strategy is cybersecurity.
- Cybersecurity attacks have the potential to be a deterrent to the self-driving benefits to the transport strategies of cities like Dubai.

- The infrastructure related technologies underlying SD vehicles introduce many threats and could lead to a perfect storm for cyber attacks.

Possible Attacks

- Cybercriminals could gain access to the computers that control the traffic lights and bring mobility to a halt by scheduling the lights to cause the worst congestion.
- Attacks aimed at changing the schedules of SD vehicles to random destinations.
- An attack on the perception system of self-driving vehicles, more specifically the radar could cause accidents.

- Attacks on city governments offices and facilities through the various wireless links of the infrastructure system.

Importance Of Frameworks

- To guarantee that their self-driving programs are not adversely affected by cyber attacks.
- Frameworks are crucial because it identifies:
  - main protection elements,
  - their relationships
  - main issues to be addressed

so that appropriate risk reduction mechanisms (or controls) can be identified and implemented.

Benefits Of Frameworks

- It can successfully guide the development and deployment of all the components of a smart city automated mobility infrastructure
- It helps a city guaranteeing the protection of assets of the multiple stakeholders including safety aspects.
- It will provide guidance, planning, and a development blueprint of the management of cybersecurity, the various risk assessment methods, service & product development, and supporting processes.

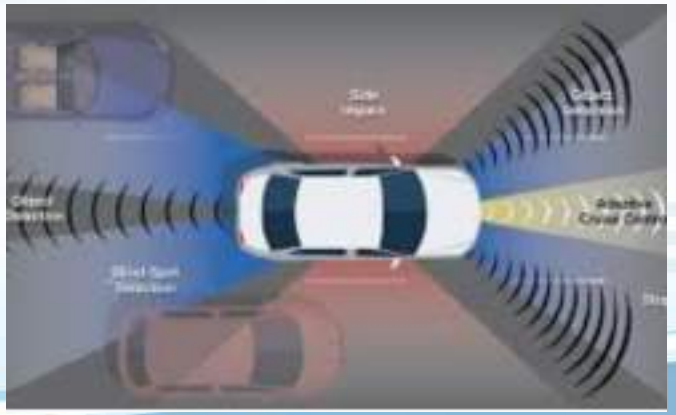
Benefits Of Frameworks (Continued)

- It can be crucial in identifying assets, threats, attacks as well as performing risk assessment and formulating effective risk management and risk reduction mechanisms or controls.
- It can be used for orchestrating a defense plan including intrusion detection systems (IDS), and incident response
- It can help with pragmatic issues a city deals with selecting vendors and suppliers, ensuring that they use appropriate cybersecurity processes and methods, and validating that the cybersecurity solutions meet the cybersecurity goals.

Top 3 Threats

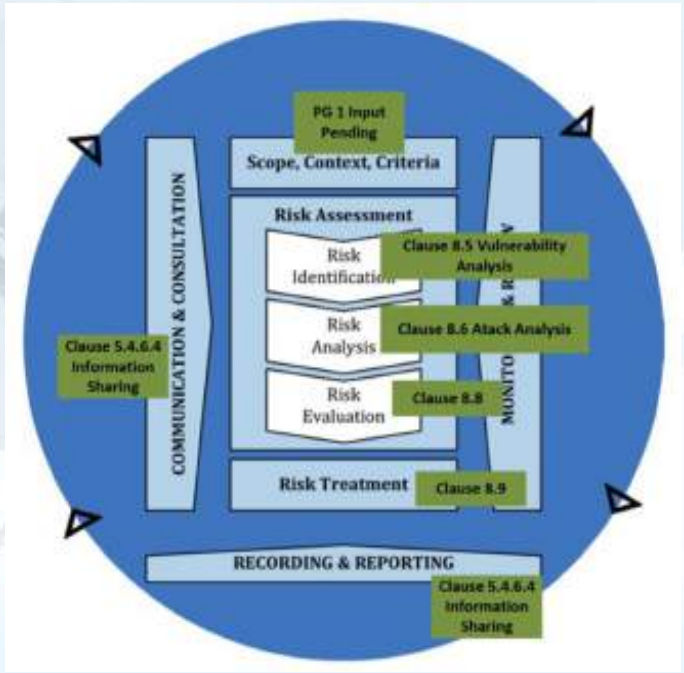
The top 3 technologies causing greatest security risks for self-driving vehicles are (Ponemon Institute):

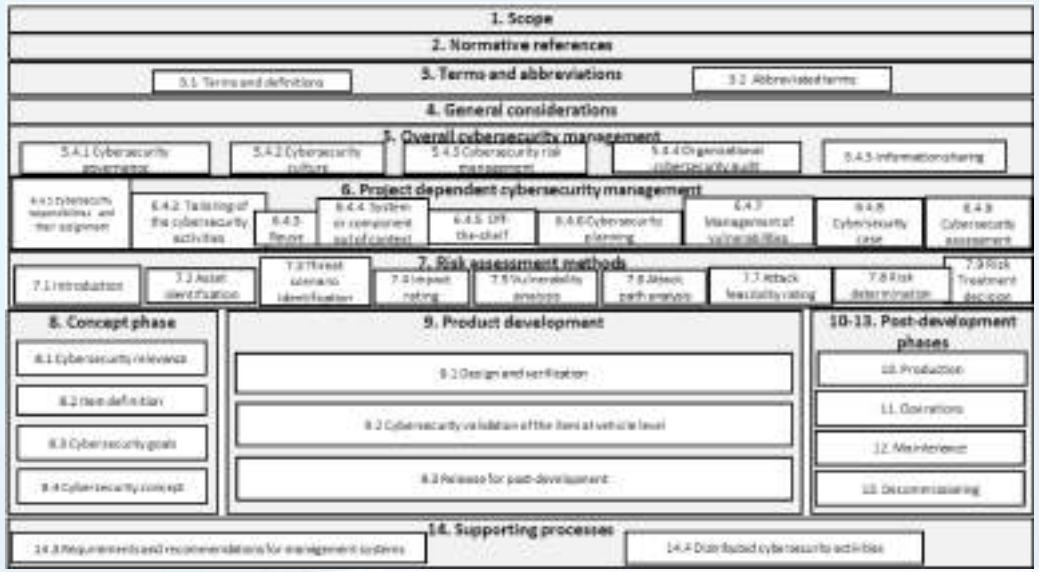
1. RF technologies
2. Telematics
3. Self-driving vehicle technologies.



A Cybersecurity Protection Framework For Dubai

- Processes
- Risk Management
- Controls

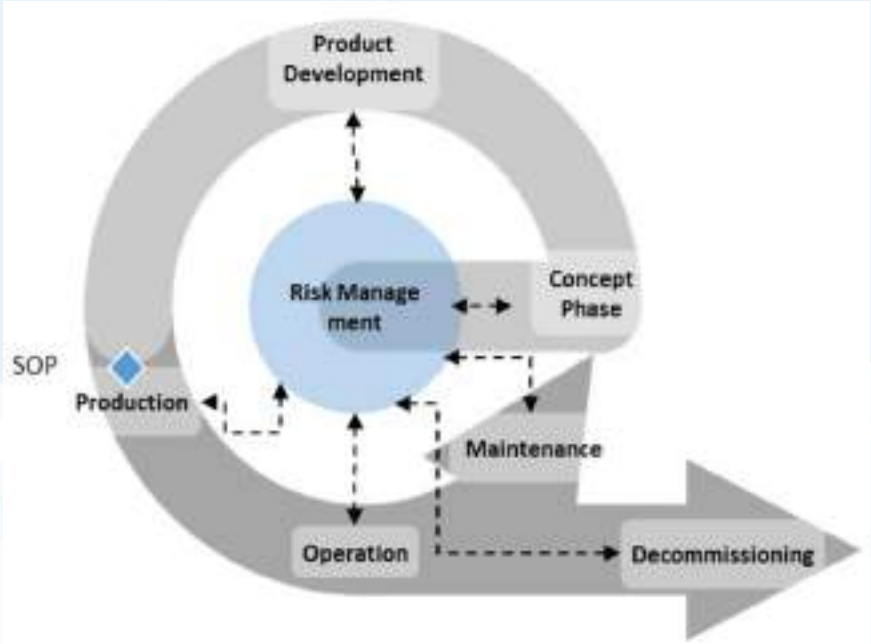




OMNEX

Protection Framework: Processes

- Flow of activities, methodologies, and procedures covering the entire lifecycle
- A process based approach has been successfully used in the design, development, and operation of quality and safety aspects of automotive and self-driving vehicles.
- Incorporated in:
  - ISO 26262 (functional safety)
  - ISO/PAS 21448 (AV safety)
  - ISO/SAE 21434 (risk management)



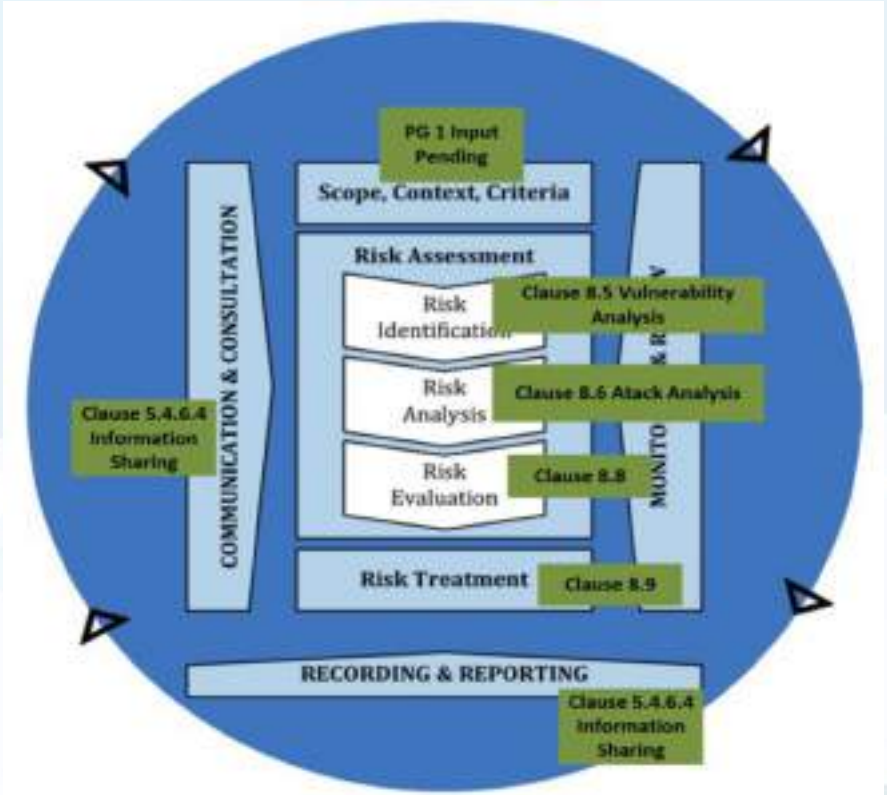
Framework: Risk Management

It involves many activities including:

- asset identification
- threat analysis
- vulnerability and attack analysis
- risk assessment
- risk reduction and treatment

Threats and vulnerabilities are intimately related to the details of the underlying technologies

- V2X (vehicle to everything)
- ADAS
- Self-Driving (automated) vehicles



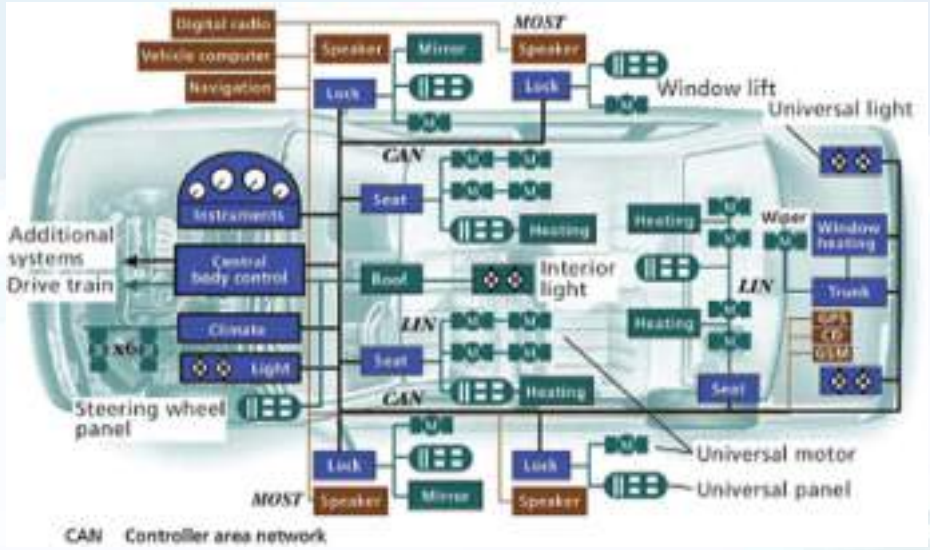
Generation Of Threats

1st Generation

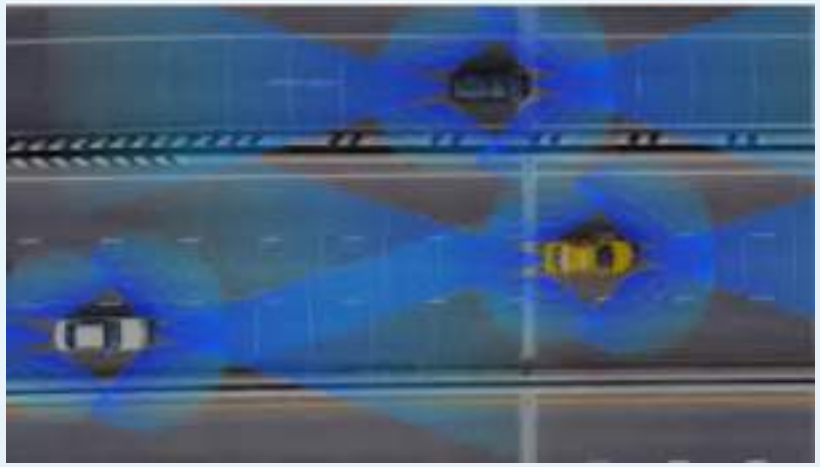
- Little or no cybersecurity protection while using technologies related to:
- In-vehicle communications (e.g., the CAN bus)
- Computing (e.g., ECUs, MCUs, GPUs, etc.)
- OBD ports
- Wireless communications (e.g., WiFi, Bluetooth)
- Infotainment
- Telematics systems, etc.

2nd Generation

- Attacking systems that use advanced or emerging technologies
- RF communications
- ADAS & self-driving vehicle technologies



Novel Threats: SD-Vehicles



Threats related to attacking the:

- Computing system
- Power sub-systems
- New in-vehicle networks
- Perception system
  - Cameras
  - Lidar
  - Radar
  - IMU (Inertial Measurement Unit), GPS, etc.

Attacks on the Radar System

  - Jamming
  - Spoofing
  - Interference

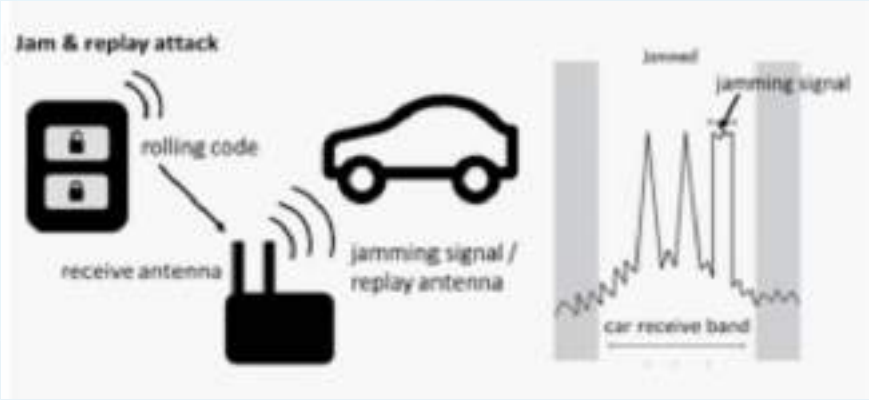
Novel Threats: RF Technologies

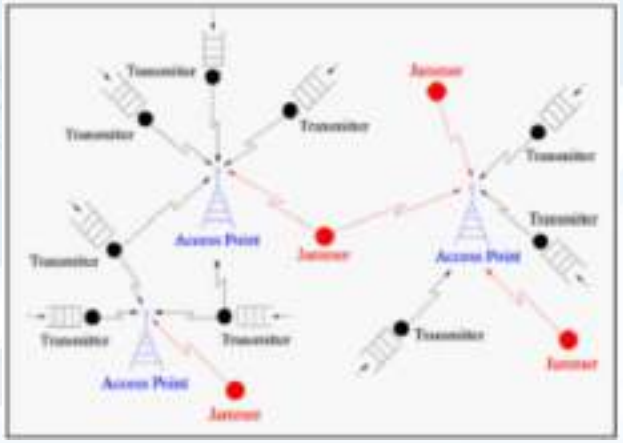
Not just threats involving WiFi or Bluetooth (BT) but:

- ZigBee (IEEE 802.15.4)
- other WiFi standards (e.g., IEEE 802.11af)
- LoRa (long range communications)
- DSRC (Dedicated Short Range Communications)
- V2X (Vehicle to vehicle, vehicle to infrastructure, etc)
- Cellular (e.g., 3G, 4G, 5G)
- Tire monitoring systems
- Keyless entry

Novel Threats: RF Attacks

- Jamming
- Replay attacks
- Evil-twin attack
- Wardriving
- Sniffing





IoT and IoR Vulnerabilities

Internet of Radio (IoR)

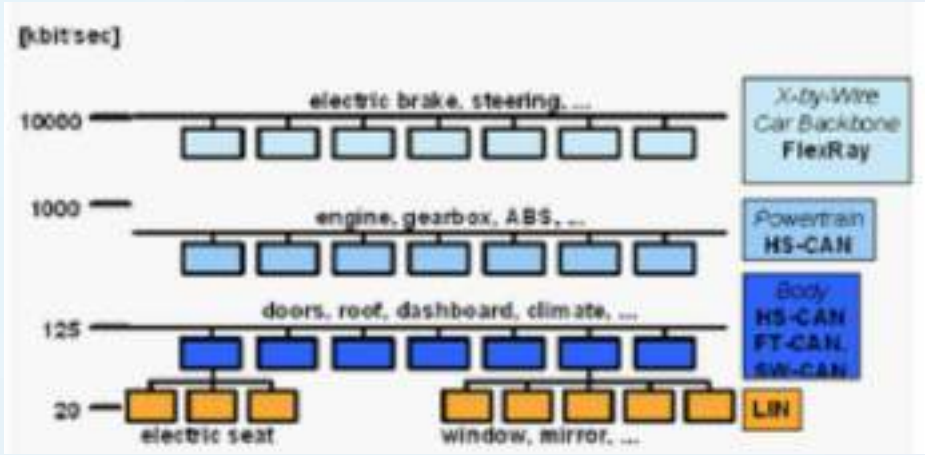
- All wireless protocols related to the various Internet architectures including IoT

IoR Vulnerabilities

- Rogue cell towers
- Rogue Wi-Fi hotspot
- Vulnerable wireless devices
- Eavesdropping/surveillance devices
- Unapproved IoT emitters.

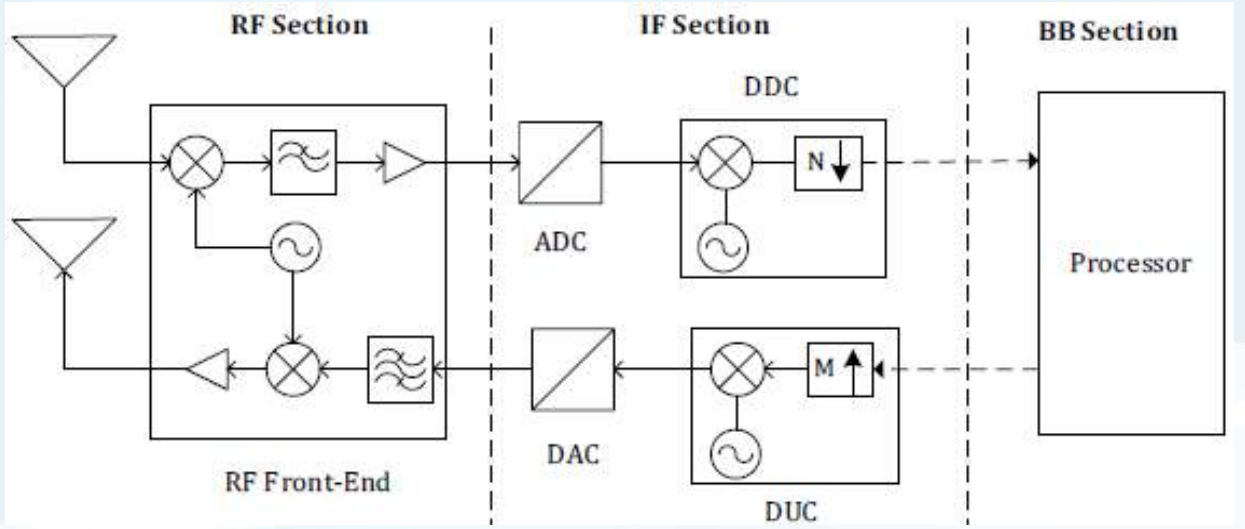
Vulnerability Handling And Incident Response

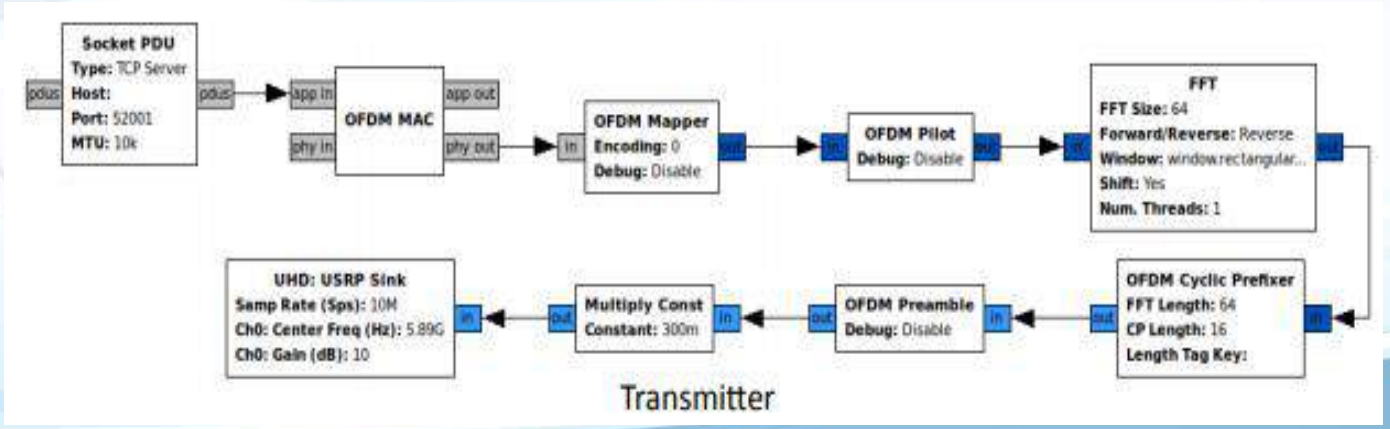
- Traditional embedded protection devices:
  - Hardware and software filters
  - Network segmentation
  - Virtual private networks
  - Secure wireless communication links
- Adhoc electronics components primarily used for penetration testing.
- General purpose radio technologies such as SDR (software defined radio)



Software Defined Radio (SDR)

Generic RF transmitter and receiver pair, software configurable and/or programmed





Conclusions

Main elements of a cybersecurity protection framework:

- Process: ISO 26262, ISO/SAE 21434
- Risk management: Threats, vulnerabilities, attacks
- Controls

Top 3 technologies with the greatest security risk:

1. RF technologies
2. Telematics
3. Self-driving vehicle technologies

- Threats and vulnerabilities discussed involving RF and self-driving technologies (e.g., Radar)
- SDR suggested to support vulnerability handling and IR.
- CS protection framework should include controls to address:
- 1st Gen Vulnerabilities: MCUs, CAN bus, Power, Infot, Telematics
- 2nd Generation Vulnerabilities: RF, SDR, IoT, IoR

SMART CITY AUTONOMOUS MOBILITY ENABLERS

Integrated Frameworks

Agenda

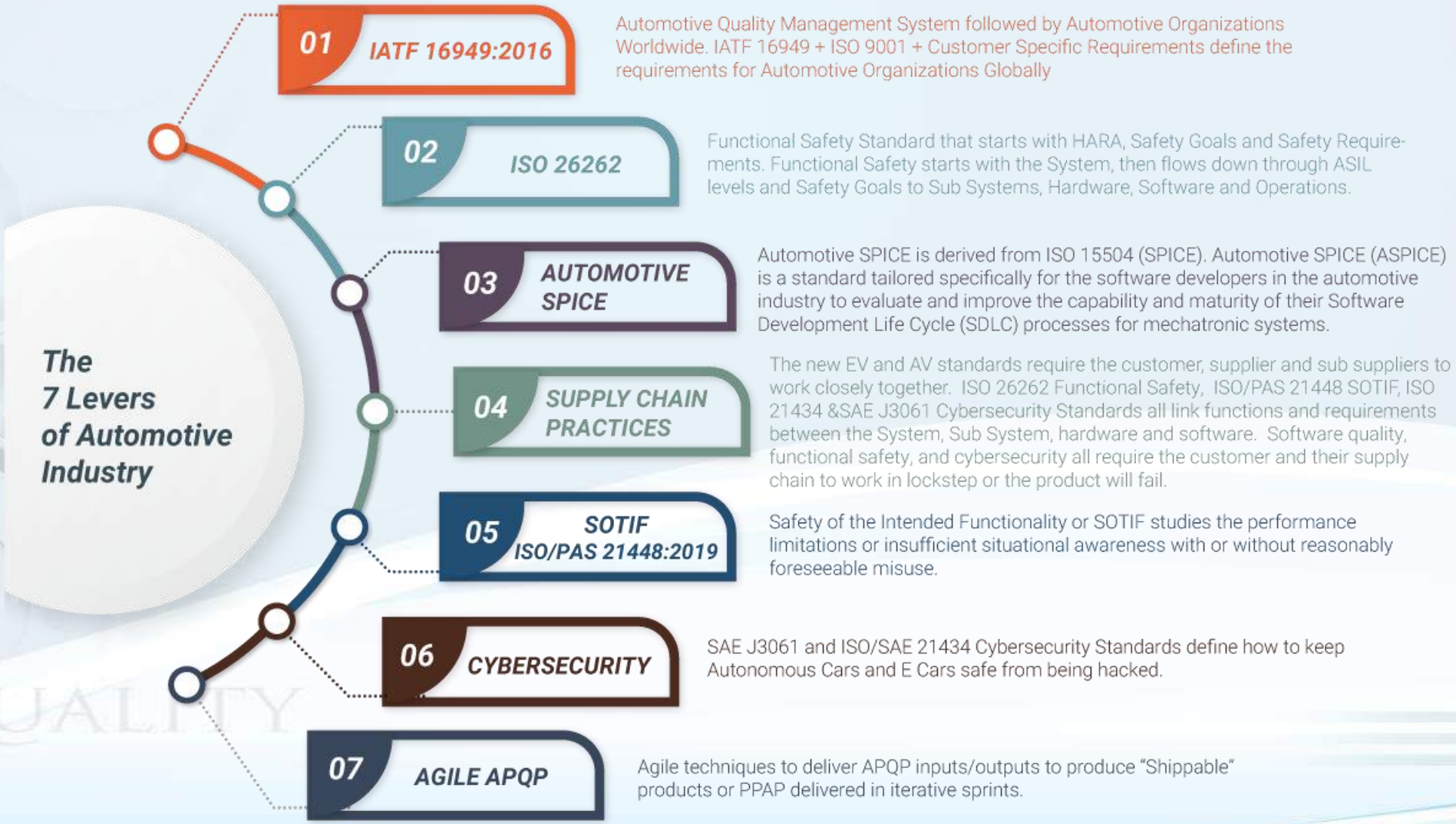
- Introduction
- Smart City Autonomous Mobility Ecosystem Stakeholders
- Enablers of the NEW Automotive Industry
- 7-Levers of the NEW Automotive Industry
- Integrated Frameworks for Autonomous Mobility
- Integrating ISO 26262 and ASPICE
- Omnex Integrated Frameworks (Software)
- Conclusions

Smart City Autonomous Mobility Ecosystem Stakeholders

- City Governments
- Transport and Communications authorities
- Mass transportation systems
- Automated taxis, busses, trains
- Self-Driving vehicle manufacturers
- Telecommunication system providers
- Telecommunication service providers
- Infrastructure system developers
- Automated mobility service providers
- Infrastructure service providers
- Products, tool, and technology suppliers

Smart City Automated Mobility Ecosystem Stakeholders

Enablers of the NEW Automotive Industry



OMNEX

Enablers of the NEW Automotive Industry

IATF 16949

- A hallmark of services, implementations, deployments, and operations of automated mobility is quality.
- QMS/PMS (quality management system/process management system)
- IATF 16949 could be tailored for automated mobility.

ISO 26262/IEC 61508/IEC 61511

- Enables functional safety in industrial sectors ranging from programmable controllers to automotive to automated vehicles.
- Many systems, products, or devices needed in automated mobility need to be designed with the highest level of safety.

AUTOMOTIVE SPICE (ASPICE)

- Services, applications, deployments, and implementation of automated mobility will require a great deal of software.
- It can be adapted for automated mobility.

Enablers of the NEW Automotive Industry

SUPPLY CHAIN PRACTICES

- Similar to automotive, autonomous mobility will require many customers, suppliers, contractors to work together.

SOTIF (ISO/PAS 21448)

- Complementary to ISO 26262 for self-driving vehicles.
- Addresses issues posed by functional insufficiencies and misuse situations.
- Highly relevant for perception systems of self-driving vehicles.

CYBERSECURITY (ISO/SAE 21434)

- Addresses issues with cyber threats & protects assets from attacks.

AGILE APQP

- Advanced product quality planning (APQP) is a framework of procedures and techniques used to develop products in industry, particularly in the automotive industry.
- This standard can be adapted to develop services for autonomous mobility.

Integrated Frameworks: Autonomous Mobility

- None of the automotive standards by themselves will suffice.
- Autonomous mobility will require several standards (enablers) for successful implementations.
- There is a need to use/apply several standards simultaneously in an integrated and coordinated fashion.
- Omnex offers services that integrates the standards in the “7-Levers” in an integrated fashion.
- These services are complemented by enterprise software to support some of the standards.

Hardware & Software are Introducing New Hazards in Vehicles

Software Now To Blame For 15 Percent Of Car Recalls

- *Bengt Halvorson, The Car Connection, June 2, 2016*

The number of software-related issues,…Automotive Warranty & Recall Report 2016, software-related recalls have gone from less than 5 percent of recalls in 2011 to 15 percent by the end of 2015….there have been 189 distinct software recalls issued over five years—covering more than 13 million vehicles…141 of these presented a higher risk of crashing."

Automotive Safety Moves Into Semiconductors

– James Morra, Electronic Design, 21st July 2017

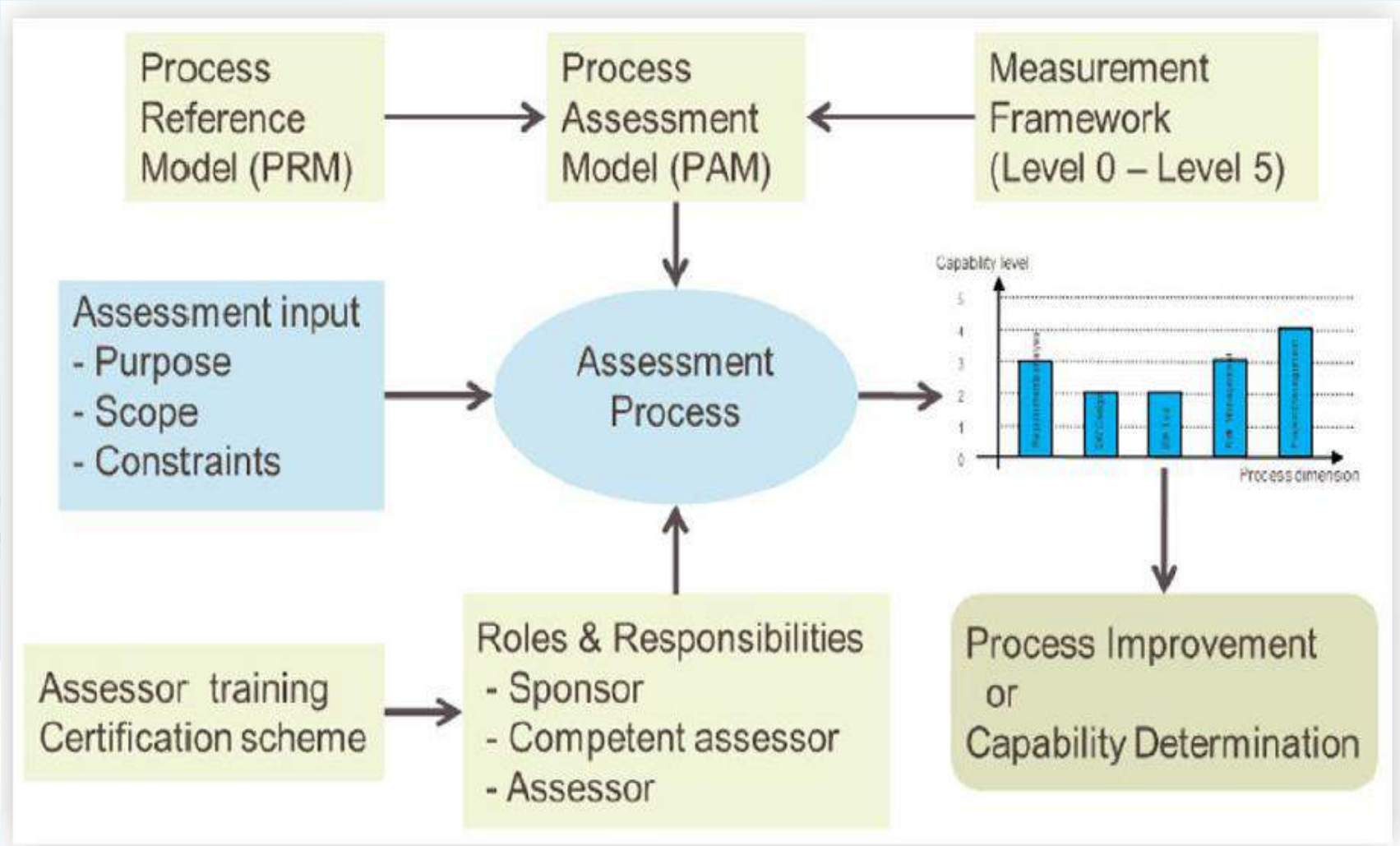
"…The [Automakers] industry has drafted the ISO26262 standard to make an industry rooted in mechanical engineering more safety conscious. The chip industry is adjusting, partly to avoid liability for self-driving car malfunctions and partly to hedge against costly recalls…"

The new electronics, hardware and software introduce new faults, some that are multi point. Functional Safety addresses these in software and hardware.

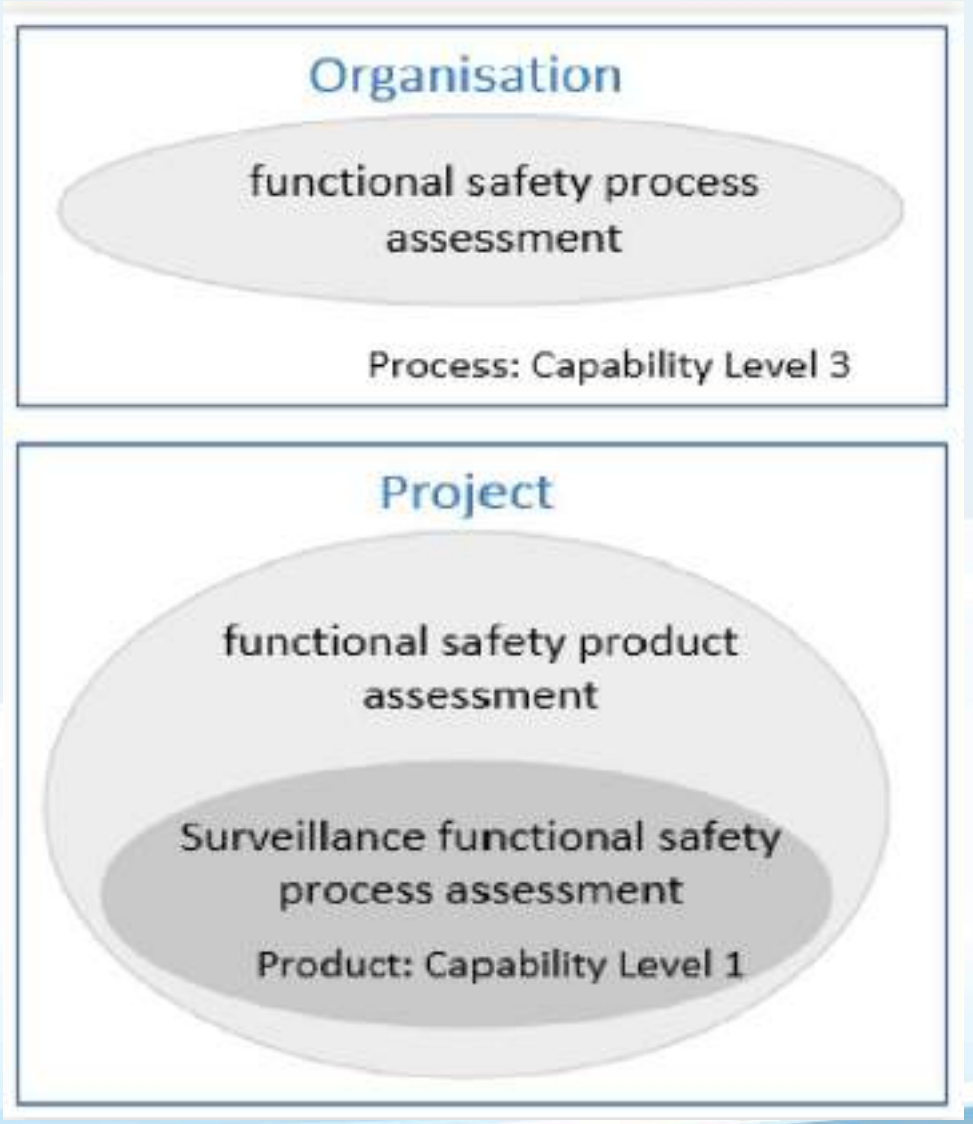
Integrating ISO 26262 And ASPICE

- Involve processes for safety (ISO 26262) and software quality assurance (ASPICE)
- ISO 26262 refers to ASPICE for software quality assurance while SPICE refers to ISO 26262 for functional safety (FS).
- There is a need to perform together the Functional Safety audit with an Automotive SPICE assessment in a coordinated fashion.
- ASPICE assessment alone is not sufficient for this purpose.
- Thus a dedicated process assessment model (PAM), complementary to ASPICE, is necessary to specifically audit the processes prescribed by ISO 26262.
- Omnex has implemented such PAM and integrated with the ISO 26262 processes.
- Thus, a combined FS Audits and ASPICE Assessments can be performed in a coordinated and integrated way.

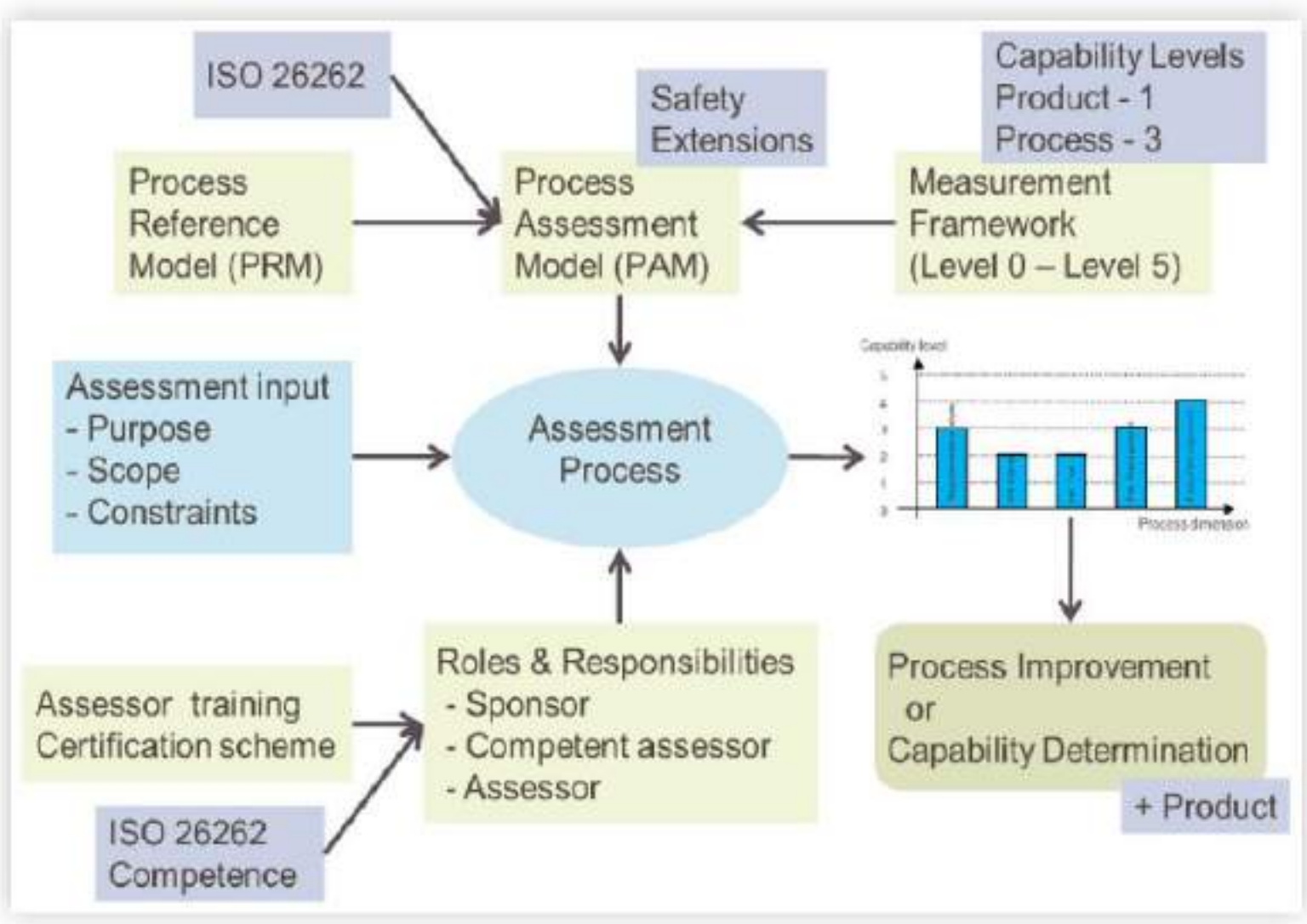
ASPICE Assessment Process



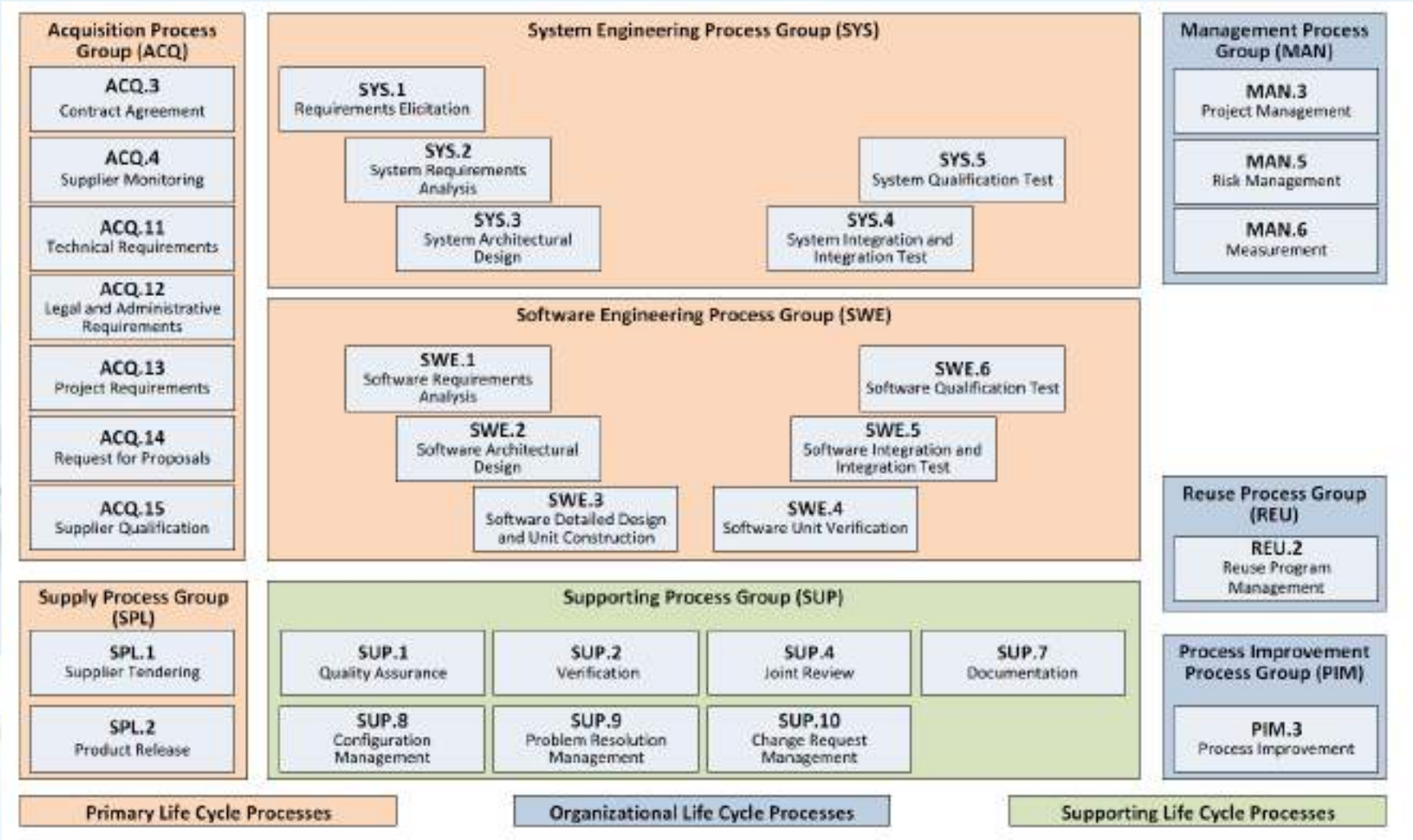
Functional Safety Product & Process Assessment



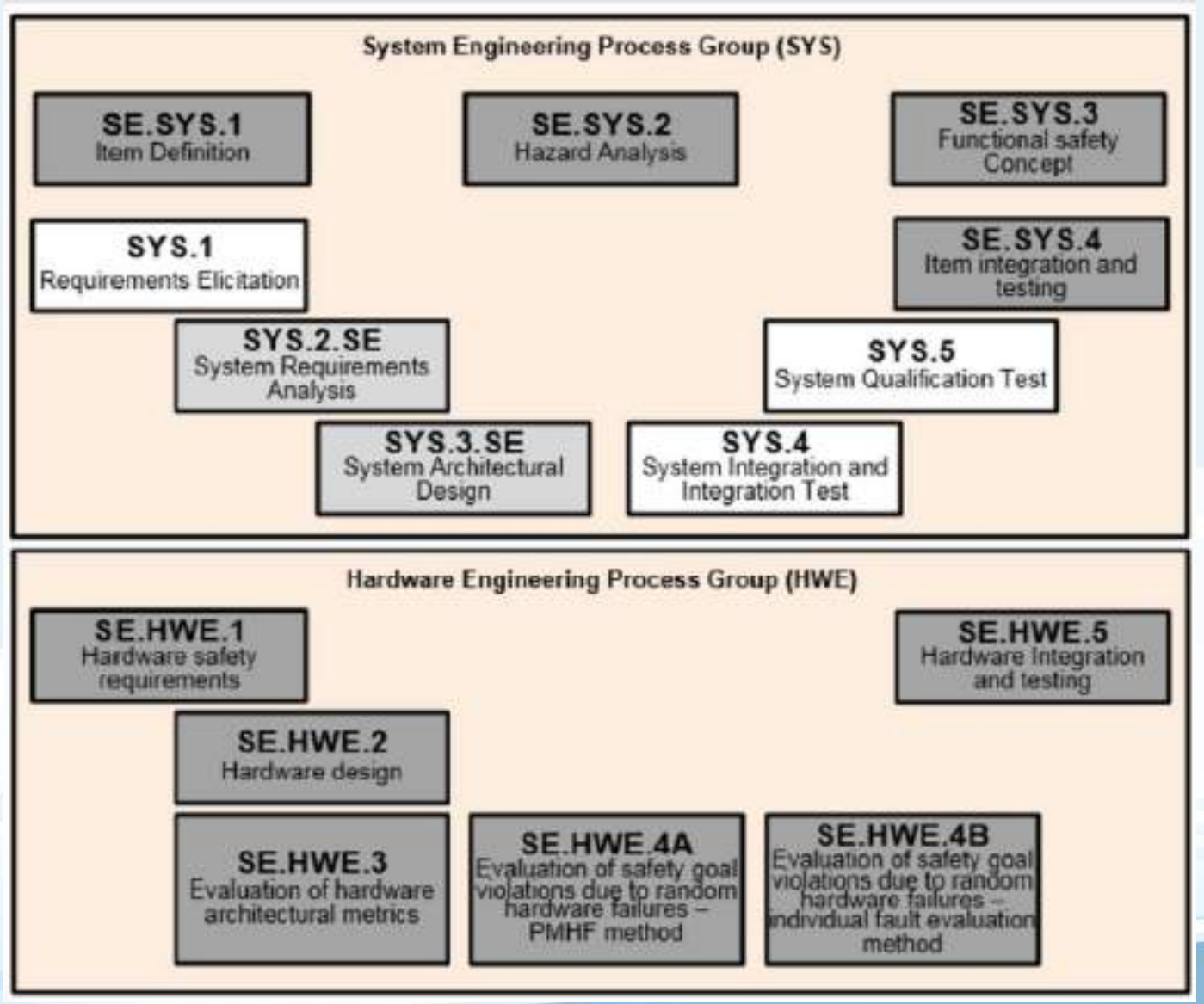
Integrated Assessment Process



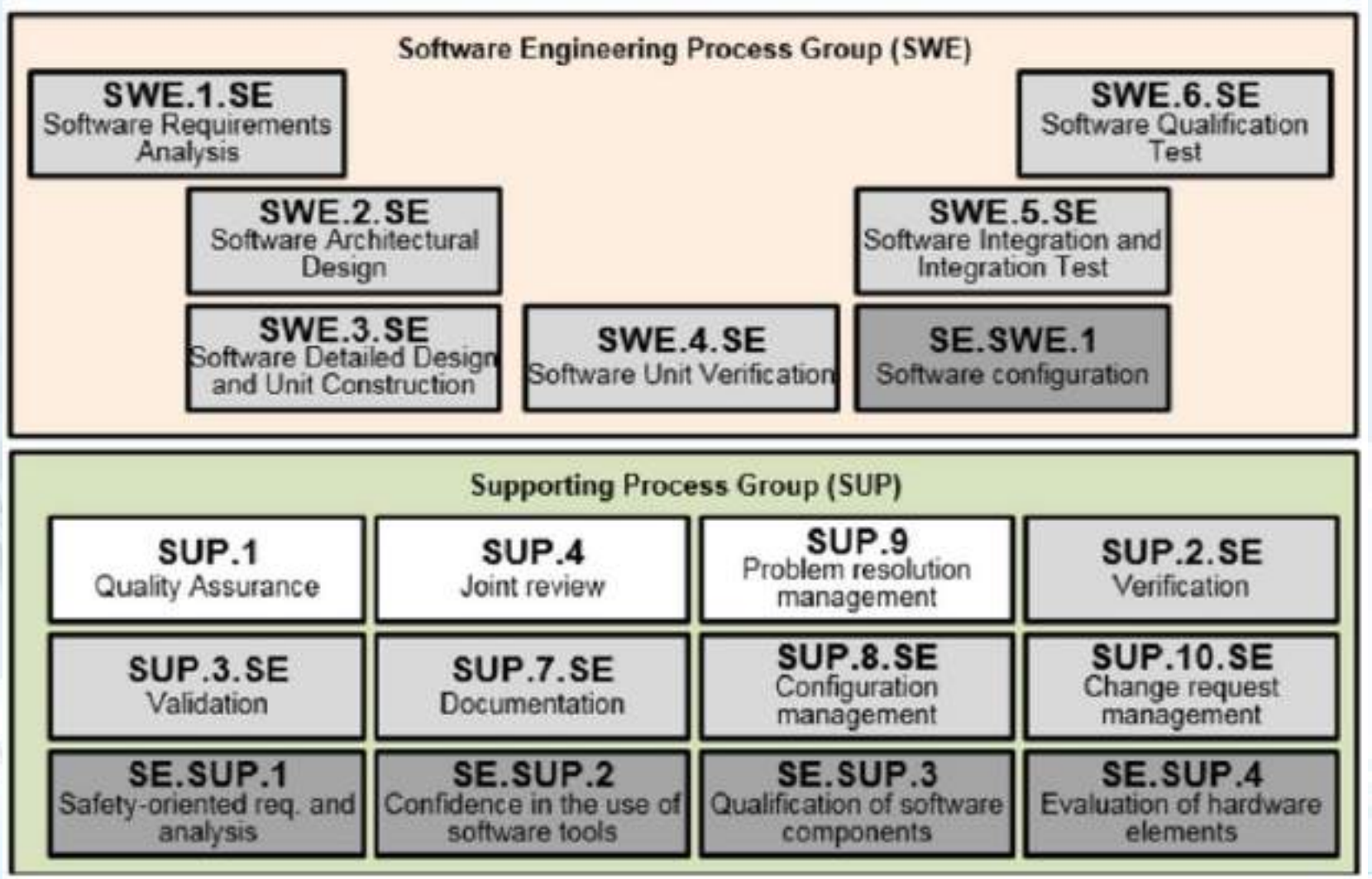
Automotive SPICE (ASPICE): Original



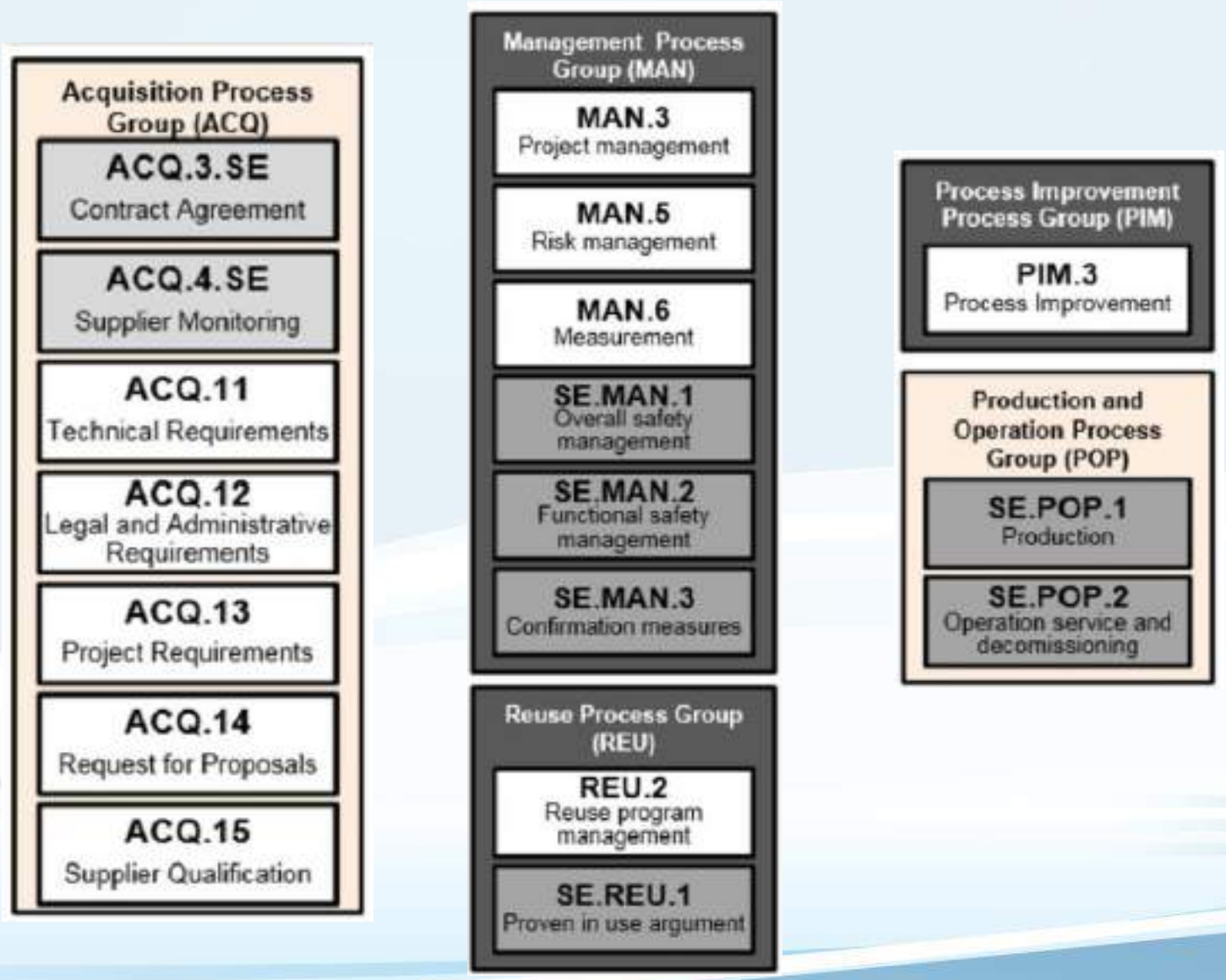
SS 7740 Process Map



SS 7740 Process Map (Continued)

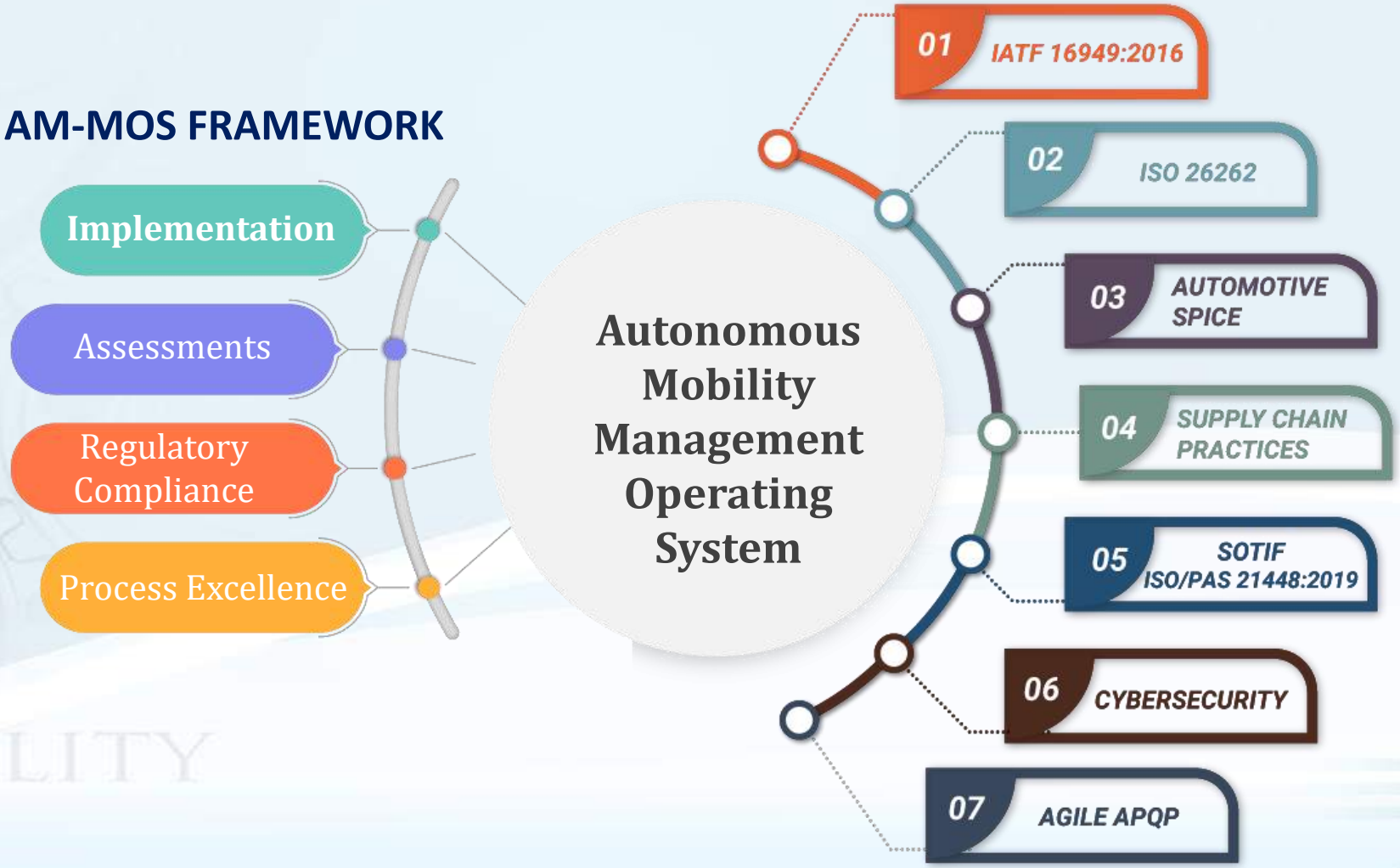


SS 7740 Process Map (Continued)

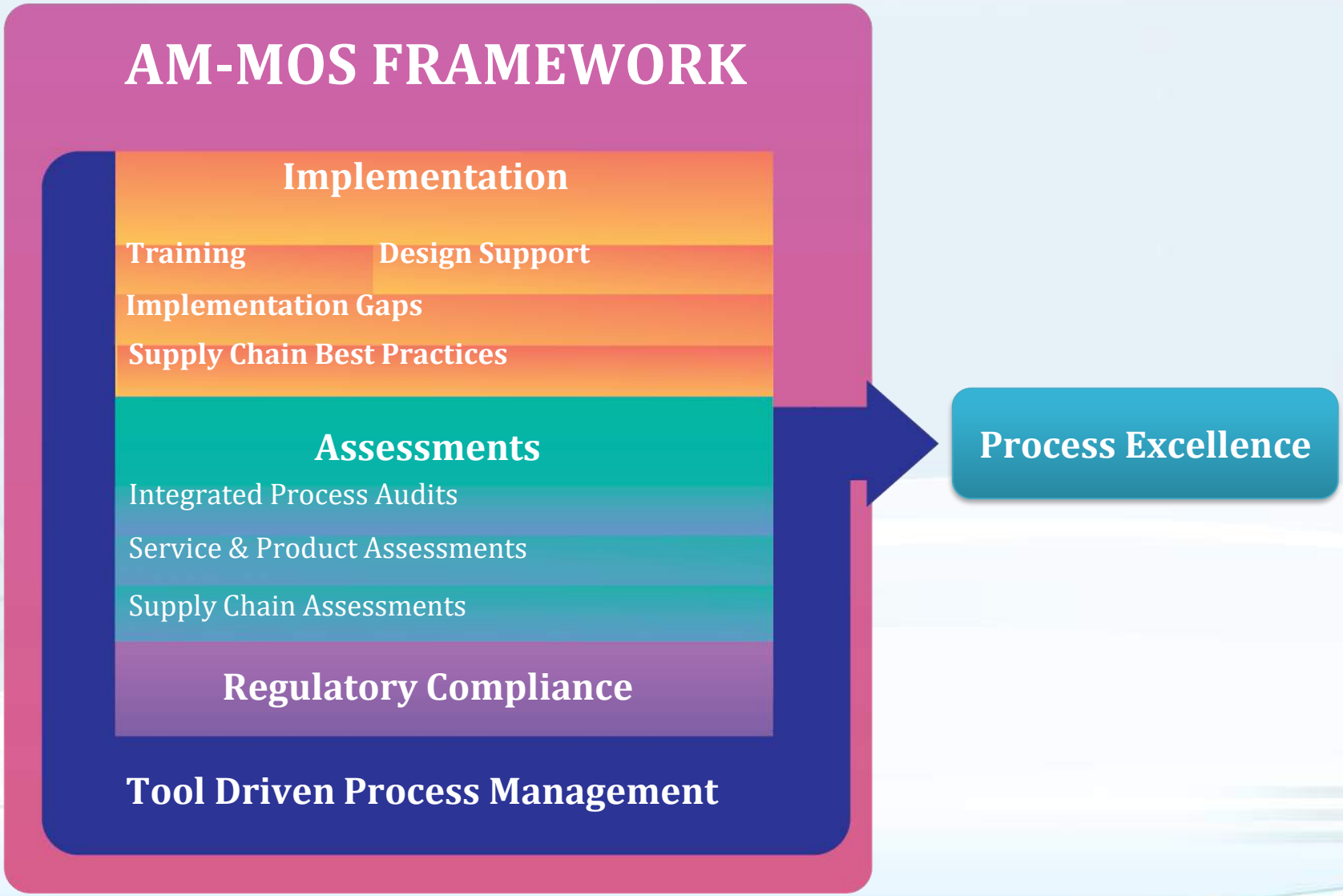


Omnex Solution: Autonomous Mobility – Management Operating System (AM-MOS)

AM-MOS FRAMEWORK



Omnex Solution: Autonomous Mobility - MOS



Omnex AM-MOS Enterprise Software

Conclusions

- Smart City Autonomous Mobility Ecosystem Stakeholders need to cooperate and work in a coordinated fashion.
- 7-Levers of the NEW Automotive Industry:
  - IATF 16949
  - ISO 26262/IEC 61508/IEC 61511
  - AUTOMOTIVE SPICE (ASPICE)
  - SUPPLY CHAIN PRACTICES
  - SOTIF (ISO/PAS 21448)
  - CYBERSECURITY (ISO/SAE 21434)
  - AGILE APQP
- Integrated Frameworks for Autonomous Mobility: Omnex AM-MOS
  - 7-Levers of the NEW Automotive Industry can be adapted for autonomous mobility in an integrated fashion
- Omnex has integrated the 7-Levers of the NEW Automotive Industry into AM-MOS with Enterprise Software.
- Omnex provides Training, Consulting & Software of integrated frameworks