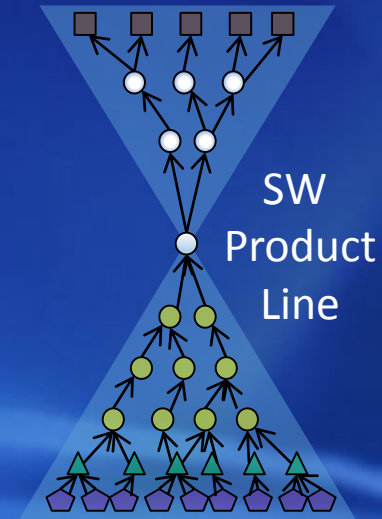


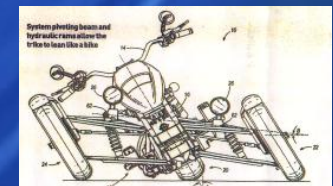
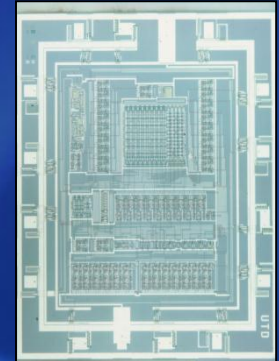
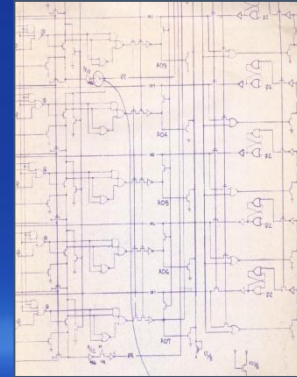
Outline

- Introduction
- Requirements Development for Automotive SW Product Lines
- GM R&D Experiences with Requirements Development for the SuperCruise Feature
- Summary



About Me – Dr. Joseph D'Ambrosio

- Automotive Industry 25+ years
 - GM, Delphi
 - Research, Advance Development, Product Development
 - Model-Based Sys. & SW Development, Safety-Critical Systems, Cyber Security, By-Wire Systems, Vehicle Control Systems, VLSI Design & Tools, Testing
 - ISO Technical Expert – ISO 26262 Automotive Functional Safety Standard
- PhD University of Michigan – EE Design Methods / Optimization
- 50+ publications, 7 patents



ISO 26262 Safety Life Cycle		
1. Introduction		
2. Functional Safety Goals		
3. Safety Analysis		
4. Safety Requirements		
5. Safety Design		
6. Safety Verification		
7. Safety Validation		
8. Safety Management		
9. Safety Review		
10. Safety Change Management		
11. Safety Configuration Management		
12. Safety Documentation		
13. Safety Training		
14. Safety Communication		
15. Safety Reporting		
16. Safety Closure		
1. Introduction	1.1 Purpose	1.2 Scope
2. Functional Safety Goals	2.1 Functional Safety Goals	2.2 Safety Goals
3. Safety Analysis	3.1 Safety Analysis	3.2 Safety Analysis
4. Safety Requirements	4.1 Safety Requirements	4.2 Safety Requirements
5. Safety Design	5.1 Safety Design	5.2 Safety Design
6. Safety Verification	6.1 Safety Verification	6.2 Safety Verification
7. Safety Validation	7.1 Safety Validation	7.2 Safety Validation
8. Safety Management	8.1 Safety Management	8.2 Safety Management
9. Safety Review	9.1 Safety Review	9.2 Safety Review
10. Safety Change Management	10.1 Safety Change Management	10.2 Safety Change Management
11. Safety Configuration Management	11.1 Safety Configuration Management	11.2 Safety Configuration Management
12. Safety Documentation	12.1 Safety Documentation	12.2 Safety Documentation
13. Safety Training	13.1 Safety Training	13.2 Safety Training
14. Safety Communication	14.1 Safety Communication	14.2 Safety Communication
15. Safety Reporting	15.1 Safety Reporting	15.2 Safety Reporting
16. Safety Closure	16.1 Safety Closure	16.2 Safety Closure



Warren, MI



SHANGHAI, CHINA



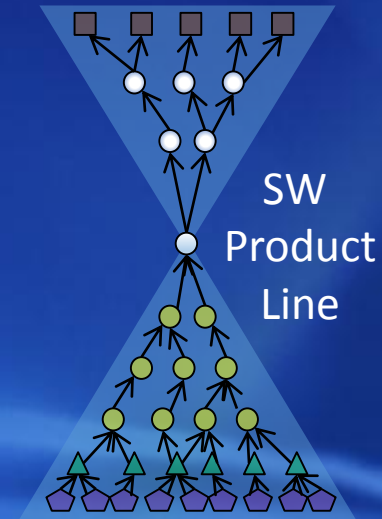
PALO ALTO, CA



HERZLIYA, ISRAEL

Outline

- Introduction
- Requirements Development for Automotive SW Product Lines
- GM R&D Experiences with Requirements Development for the SuperCruise Feature
- Summary



General Motors

Electrical, Controls and Software



- GM has one of the most complex systems and software product line engineering challenges in the world
 - 3000 contributing engineers
 - 300 hierarchical subsystems
 - Thousands of variant features
 - 100 Million lines of code
 - Millions of product instances per year
 - Tens-of-thousands of unique product variants
 - Dramatic increase in variation due to new propulsion systems and active safety
 - Global diversity in legislative regulations
 - Extreme economic and competitive pressures
 - Product line and feature set evolves annually
 - 15 concurrent development streams



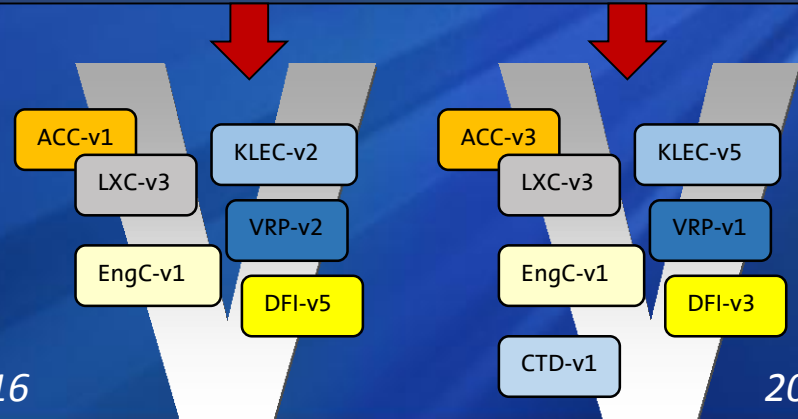
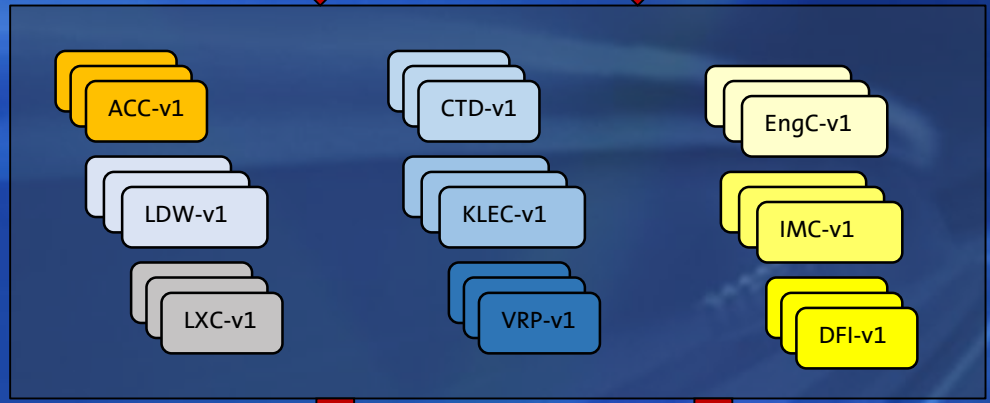
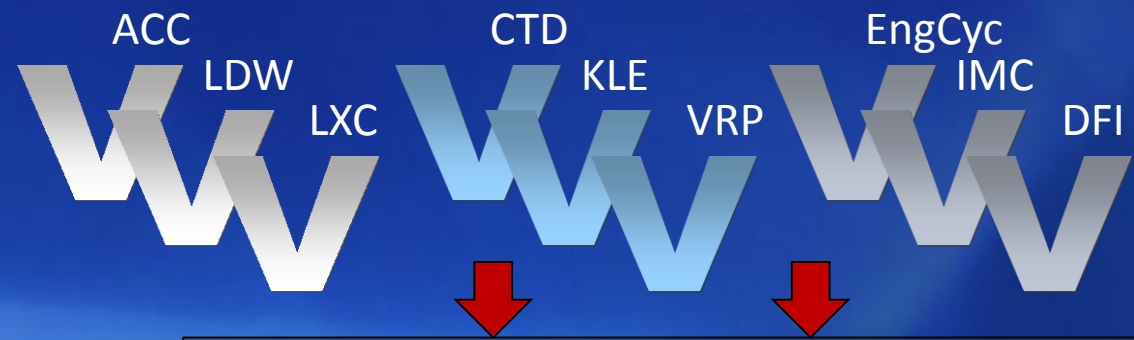
GM Enables massive Reuse through Software Product Lines

- A Product Line is a set of systems sharing a common, managed set of features that are developed from a common set of core assets in a prescribed way
- Why Product Line over Products for GM Embedded Software?
 - As much as an 85% reduction in effort for a second (third, fourth, etc.) application
 - As much as a 70% reduction in field claims overall

Product Line Engineering

Features

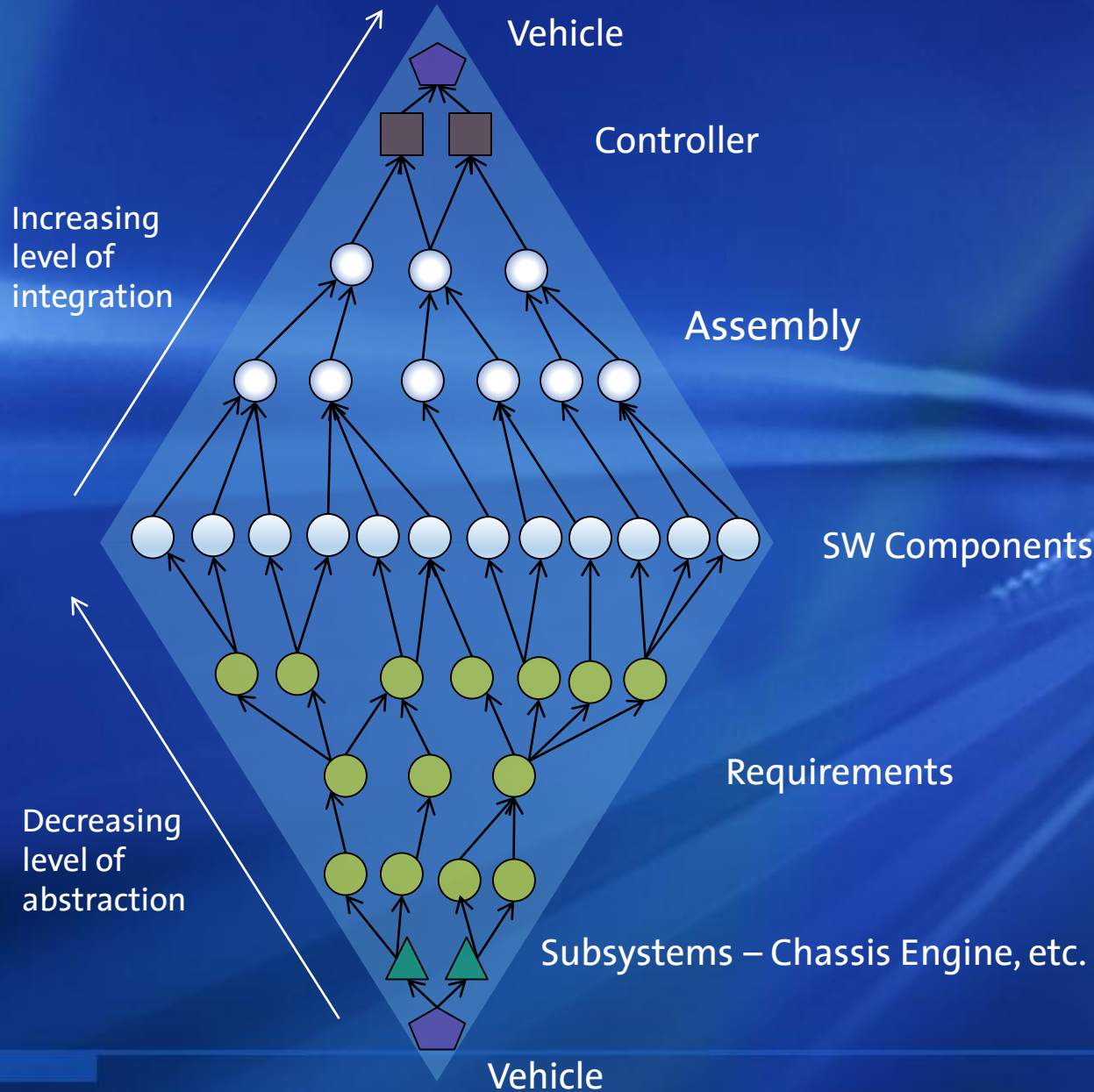
Electrical Architecture



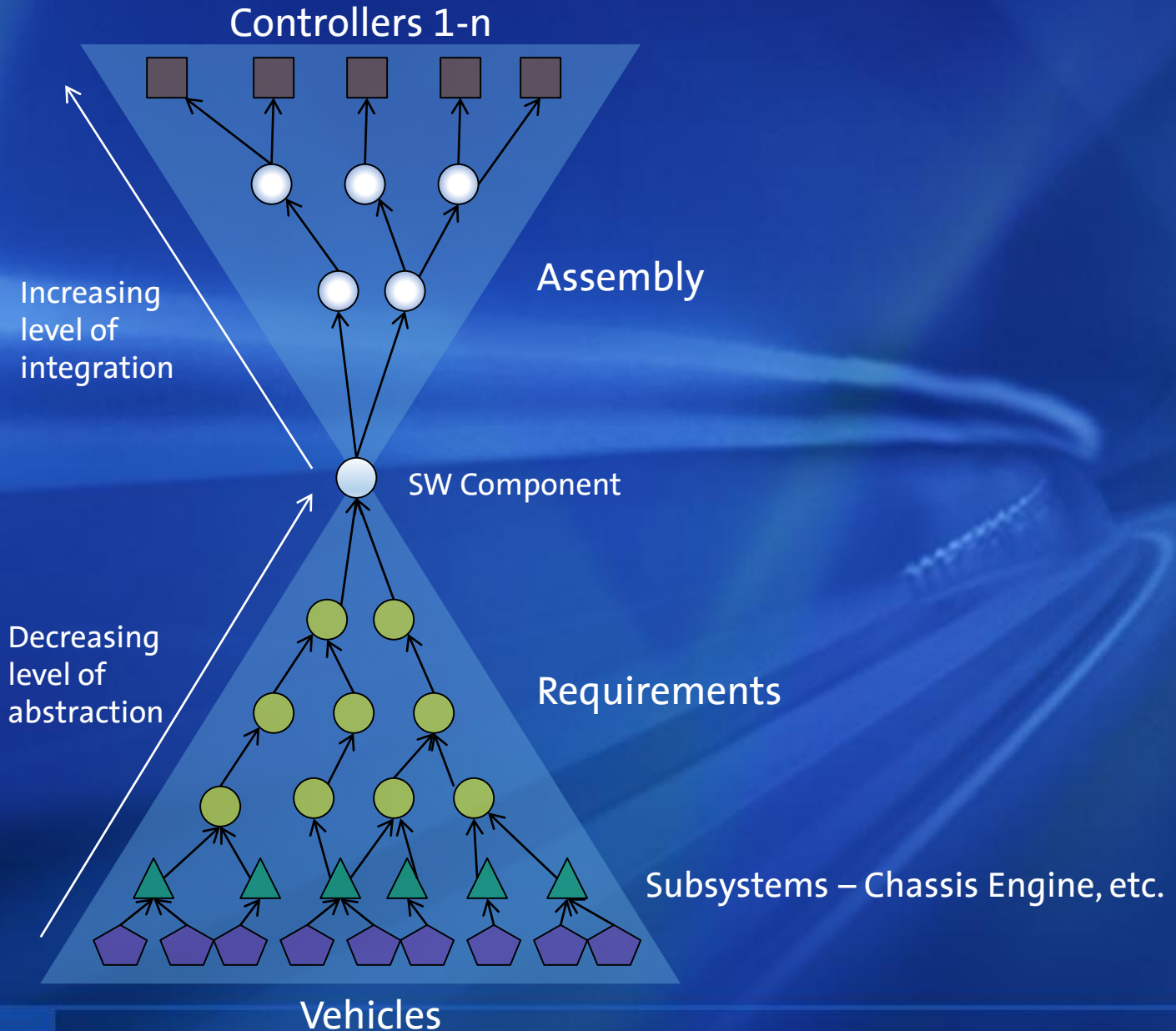
2016
Chevrolet
Volt

2017
Buick
Regal

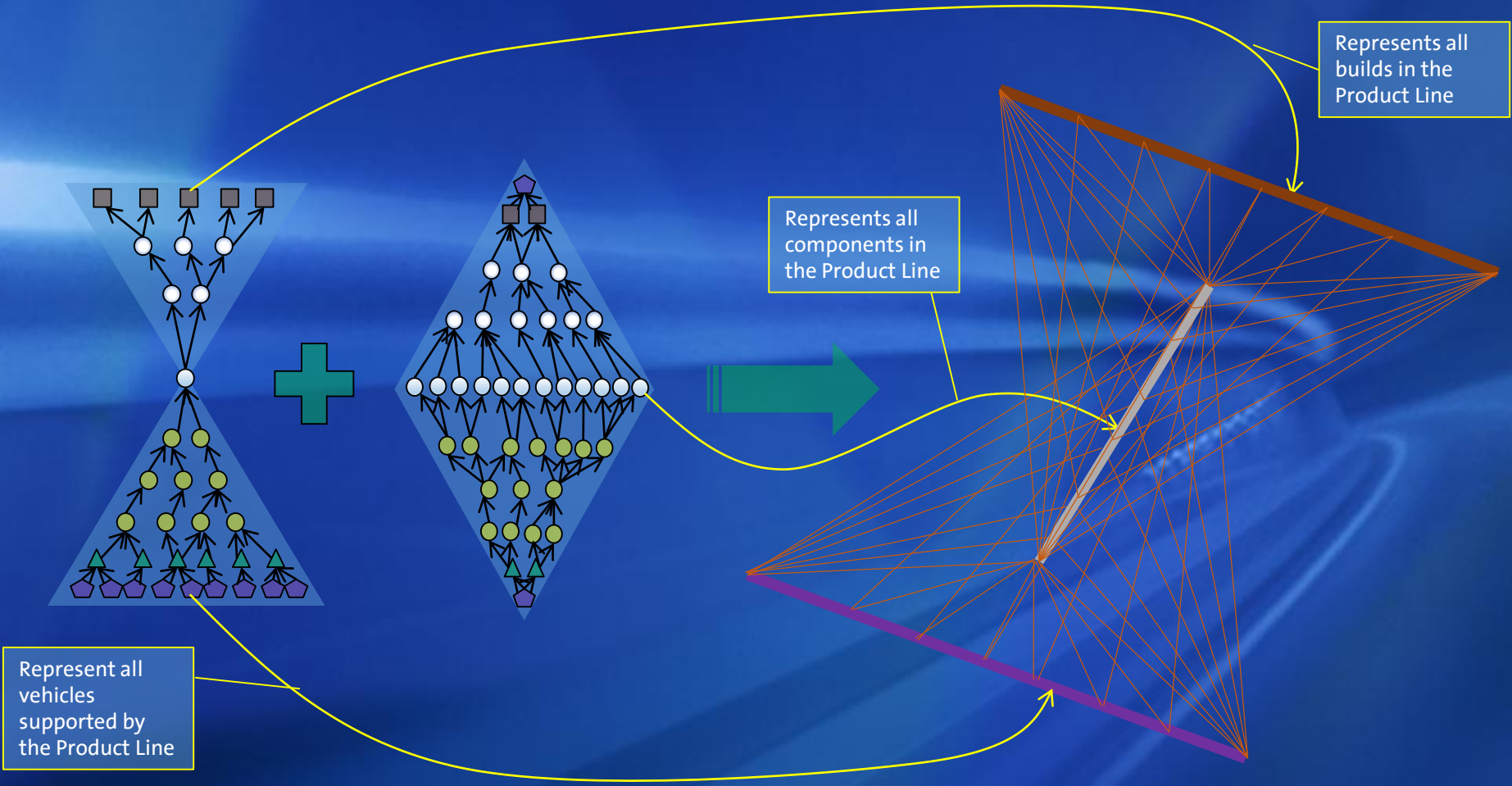
Software Product Line - Single Vehicle View



Software Product Line - Single Component View



Software Product Line - Components X Vehicles



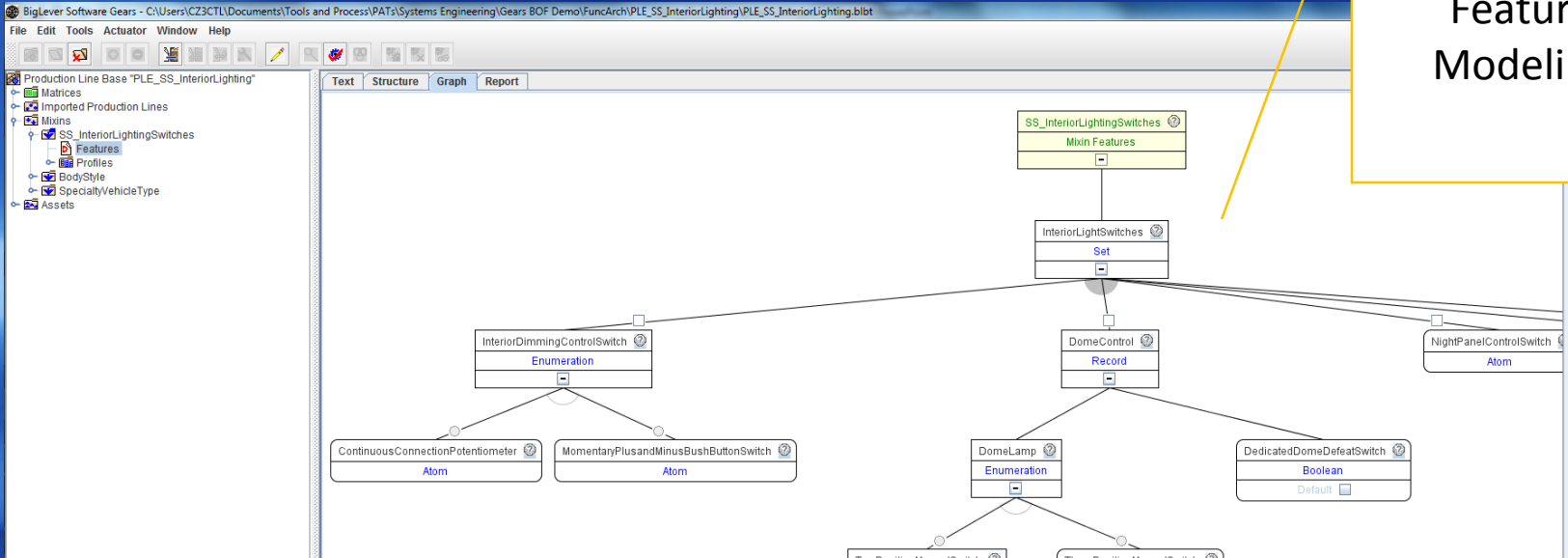
Example Product Line Requirements Challenges

- Traceability of requirements to vehicles deployments
 - Which requirements apply to a specific vehicle?
 - What tests need to be run?
 - Why do we have this requirement?
- Product line development
 - Which deployments need to be supported?
 - Which combination of features need to be tested?
- Can a design element be modified?
 - Why does this design element exist?
 - What is the impact of changing the design element?

Feature Modeling Example

Rational Doors; Big Lever Gears in Combination

Feature Modeling



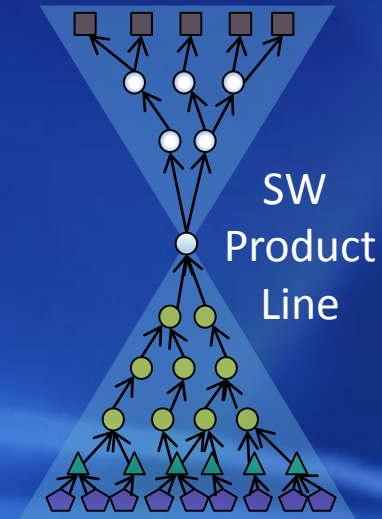
'Cruise Enable' current 7.0 in /SandBox/Doug Babcock/test/Cruise Control RME Example - Original/Functional Architecture/Domains/Propulsion System Coordination/Driver Interpretation/Cruise (Formal module) - DOORS

ID	VP	Cruise Enable	Gears Logic	Gears Variant	Gears Main Projection
CRUZ_ENB_L_17		1 Driver Foot Pedal Cruise Enable	When (TransmissionType == {Manual}) Select "ManualCruiseEnable"; When (TransmissionType == {Automatic}) Select "AutomaticCruiseEnable";		
CRUZ_ENB_L_15	v	1.1 Manual Trans Clutch Before Cruise Enable		ManualCruiseEnable	
CRUZ_ENB_L_16		xxxxManual transmission applications shall allow cruise enablement if the Top-of-Travel Clutch Switch Signal has transitioned OR Brake Pedal Apply discrete input and the GMLAN signal Brake Pedal Initial Travel Achieved transition from the "applied" state to the "not applied" state at least once during an ignition cycle. This requirement satisfies the			
CRUZ_ENB_L_1	v	1.2 Brake Before Cruise Enable		AutomaticCruiseEnable	
CRUZ_ENB_L_2		yyyCruise control shall require both the Brake Pedal Apply discrete input and the GMLAN signal Brake Pedal Initial Travel Achieved transition from the "applied" state to the "not applied" state during each ignition cycle before allowing cruise control engagement.			

Formal variation language and actuation

Outline

- Introduction
- Requirements Development for Automotive SW Product Lines
- GM R&D Experiences with Requirements Development for the SuperCruise Feature
- Summary



THE OPPORTUNITY

Crashes / Human Errors



Aging / Disabled



Congestion / Time



CADILLAC DRIVER ASSISTANCE / ACTIVE SAFETY

Package 1 – “Driver Awareness Package”

 Cadillac ATS
Cadillac XTS
Cadillac SRX




Safety Alert Seat

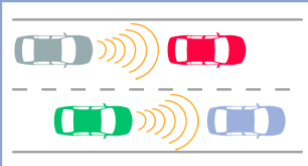
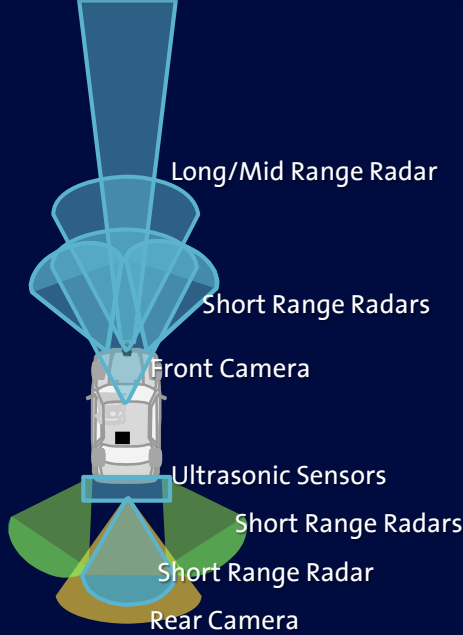
- Lane Departure Warning
- Forward Collision Alert
- Side Blind-Zone Alert
- Rear Cross-Traffic Alert
- Haptic Safety Alert Seat Feedback

Also includes:

- Rear Vision Camera
- Front & Rear Park Assist

Package 2 – “Driver Assist Package”

 Cadillac ATS
Cadillac XTS
Cadillac SRX



Package 1 plus:

- Full Speed-Range ACC (Stop w/Go Notifier)
- Auto Collision Preparation (includes Collision Imminent Braking)
- Low-Speed Front/Rear Automatic Braking (Emergency Braking to Avoid Contact)

DRIVING AUTOMATED (IN NON-AUTOMATED VEHICLES!)





NEXT STEP: SUPERCUISE



Requirements Development Challenges

VTS

Vehicle Technical Specification

- Not a focus, as vehicle integrates features from product line

SSTS

Subsystem Technical Specification

- Requirements / Specifications for multiple features
- Very large documents, requirements for individual feature dispersed
- Difficult to comprehend
 - individual features
 - how features relate to one another
 - Intent of requirements

CTS

Component Technical Specification

- e.g., controller or sensor specifications
- Relevant during later phases of the project

SuperCruise Requirements Development Strategy

Use Cases

Describe how system should handle various key driving scenarios

User Requirements

- High-level, capture key behavior aspects
- Implementation independent

Functional Requirements

- Detailed. all behavior described
- Comprehends interfaces with other features

Non functional Requirements

Capture intent of functional requirements

Feature Technical Specification (FTS)

SSTS & CTS

Example User Requirements

The Cruise Control (CC) feature shall assist the driver to maintain the vehicle at a constant speed, without the need for driver acceleration through the accelerator pedal.

U -1 CC shall work for speeds between $V_{Low\ Speed\ Inhibit}$ and $V_{High\ speed\ inhibit}$ miles per hour.

U -2 CC shall allow the driver to set the desired vehicle speed, when the vehicle current speed is between $V_{Low\ Speed\ Inhibit}$ and $V_{High\ speed\ inhibit}$ mph.

U -2.1 CC shall maintain the vehicle speed at the speed set by the driver.

U - 3 CC shall allow the driver to increase and decrease the current CC speed,

U- 3.1 CC shall allow driver to increment or decrement the current CC speed by a fixed value of TBD mph.

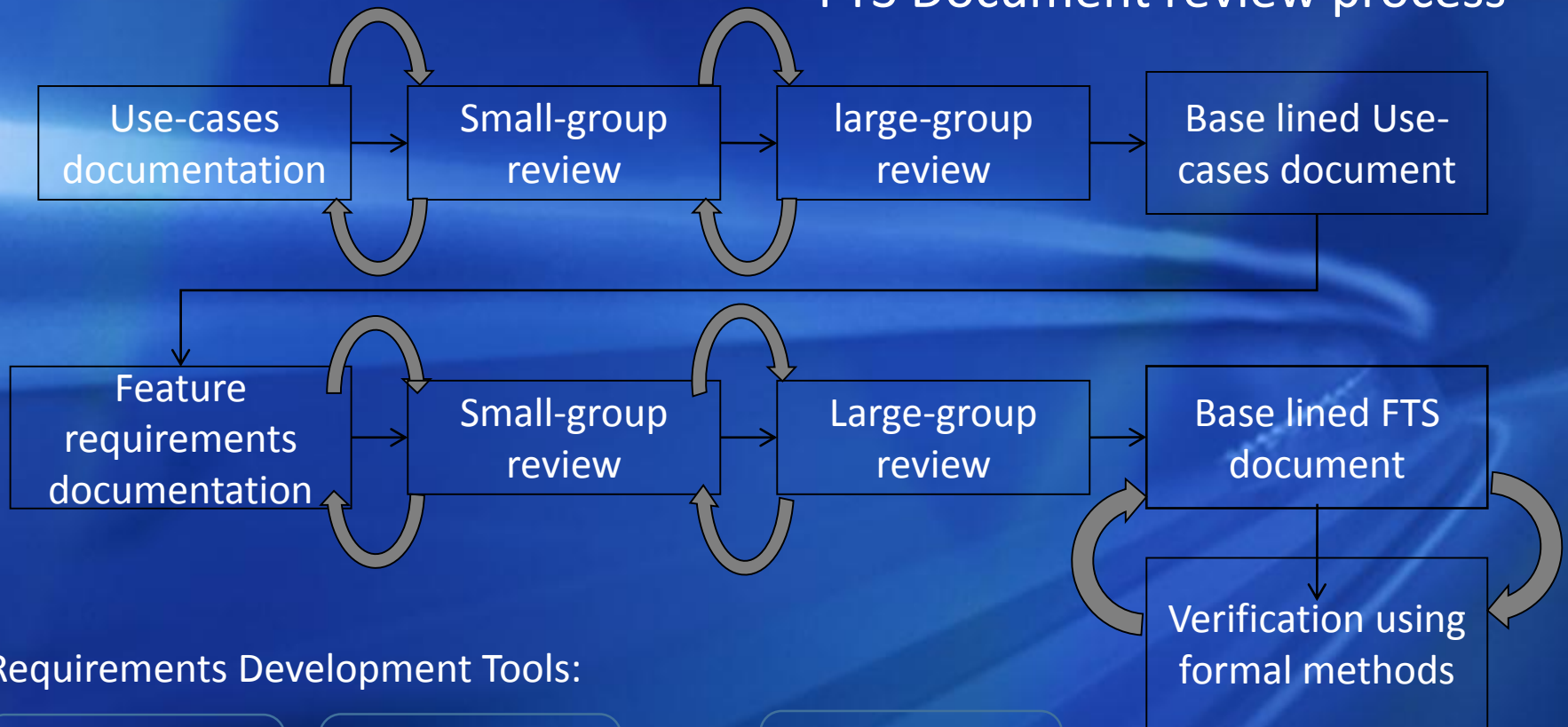
U – 3.2 CC shall allow driver to accelerate or decelerate from the current CC speed until a maximum limit of TBD mph is reached.

Example Functional Requirements

- F-1.0 CC shall transition between the following states:
 - **Control_Off** (default state)
 - **Disabled** (not ready to control).
 - **Performing_Diagnostics** (Waiting for diagnostics results)
 - **Standby_Disabled** (feature chosen but the enable criteria is not fulfilled)
 - **Standby_Enabled** (feature is chosen and the enable criteria is also fulfilled)
 - **Engaged** (regulating the speed of the vehicle at the driver set speed)
- F-2.0 CC must receive the following information
 - VehicleSpeed
 - BrakePedalStatus (indicating when pressed)
 - AcceleratorPedalStatus (indicating when pressed)
 - ClutchPedalStatus (indicating when pressed)
- F- 3.0 CC shall transition from **Control_off** to **Disabled** state, when System_Power_Mode is in the ON mode.
- F- 4.0 CC shall first perform diagnostic tests when the driver requests for CC.
 - F-4.1 CC shall inform the driver when CC functionality has some problem.
 - F- 4.2 The diagnostic tests failed message shall be sent to the Driver Display Console when CC is not functional.
- F-5.0 CC shall transition from **Disabled** to **StandBy_Disabled**, if CC passes diagnostic tests
 - F- 5.1 CC shall inform the driver when CC is ready to operate.
 - F-5.2 The CCOperatingIndicator shall light up when CC is operational (Which means that the diagnostic tests were passed).

SuperCruise Requirement Development Strategy (Cont.)

FTS Document review process



Requirements Development Tools:

REdit
Requirements
Authoring Tool

FRAMES
Formal Methods
Analysis

+

Virtual
Validation

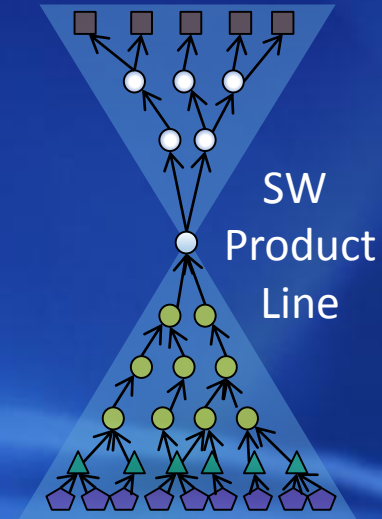
DOORS
Requirements
Management

HIL Bench
Validation

In-Vehicle
Validation

Outline

- Introduction
- Requirements Development for Automotive SW Product Lines
- GM R&D Experiences with Requirements Development for the SuperCruise Feature
- **Summary**



Summary

- Automotive product line challenges addressed by requirements & product line management
- Active safety and semi autonomous driving present new challenges
 - Complex interacting features
 - Highly depending on vehicle operating environment
 - To learn more
 - <http://spectrum.ieee.org/transportation/safety/the-crashproof-car>
- Challenges addressed by rigorous requirements development process
 - Implementation independent requirements vs. functional specification
 - Requirements management,
 - Design reviews and formal analysis
 - Validation activities: model-based, HIL bench, in-vehicle
- Next steps: System of Systems and feature interaction methods

Thank You!

