Closing the Systems to Silicon Gap: MBSE-Enabled Digital Electronics Verification

Lisa Murphy, Siemens Digital Industries Software
Mark Malinoski, Siemens EDA

NDIA Systems and Missions Engineering Conference
December 2021

Approved for Public Release

SIEMENS

Toward Trustworthy Microelectronics

A long journey, as yet not completed

NDIA’s first Trusted Microelectronics Workshop held in 2015

Siemens acquisition of Mentor Graphics in 2017 creates new opportunities

SIEMENS

We don’t have trustworthy electronics today

Hard to get electronics failure data for DoD, so look at autos

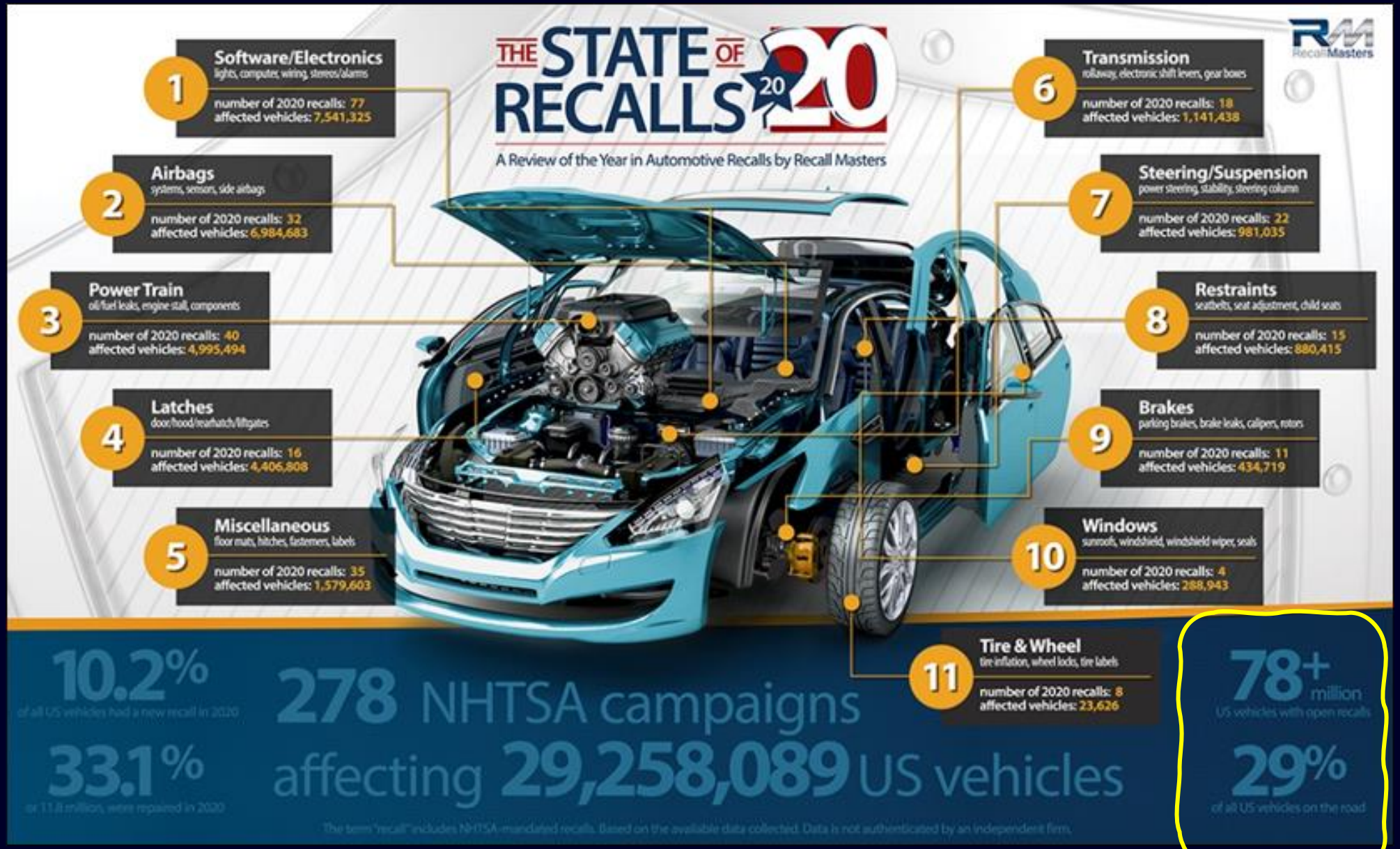
In 2020, there were **29 million** auto recalls per National Highway Traffic Safety Administration (about 2 vehicles recalled for each vehicle sold)

Almost 25% were faulty software or electronics, up from about 6% in 2016; **increasing frequency in integrated electronics**

At $500 average direct cost of about $36 BILLION

Many of you are aware of critical applications experiencing this problem in the defense space

[For comparison, both auto and military are around 3-4% of GDP]


THE STATE OF RECALLS 2020
A Review of the Year in Automotive Recalls by Recall Masters
RecallMasters
1 Software/Electronics
lights, computer, wiring, stereos/alarms
number of 2020 recalls: 77
affected vehicles: 7,541,325
2 Airbags
systems, sensors, side airbags
number of 2020 recalls: 32
affected vehicles: 6,984,683
3 Power Train
oil/fuel leaks, engine stall, components
number of 2020 recalls: 40
affected vehicles: 4,995,494
4 Latches
door/hood/rearhatch/liftgates
number of 2020 recalls: 16
affected vehicles: 4,406,808
5 Miscellaneous
floor mats, hitches, fasteners, labels
number of 2020 recalls: 35
affected vehicles: 1,579,603
6 Transmission
rollaway, electronic shift levers, gear boxes
number of 2020 recalls: 18
affected vehicles: 1,141,438
7 Steering/Suspension
power steering, stability, steering column
number of 2020 recalls: 22
affected vehicles: 981,035
8 Restraints
seatbelts, seat adjustment, child seats
number of 2020 recalls: 15
affected vehicles: 880,415
9 Brakes
parking brakes, brake leaks, calipers, rotors
number of 2020 recalls: 11
affected vehicles: 434,719
10 Windows
sunroofs, windshield, windshield wiper, seals
number of 2020 recalls: 4
affected vehicles: 288,943
11 Tire & Wheel
tire inflation, wheel locks, tire labels
number of 2020 recalls: 8
affected vehicles: 23,626
10.2%
of all US vehicles had a new recall in 2020
278 NHTSA campaigns
33.1%
affecting 29,258,089 US vehicles
78+ million
US vehicles with open recalls
29%
of all US vehicles on the road

SIEMENS

Challenges to achieving high levels of assurance for microelectronics

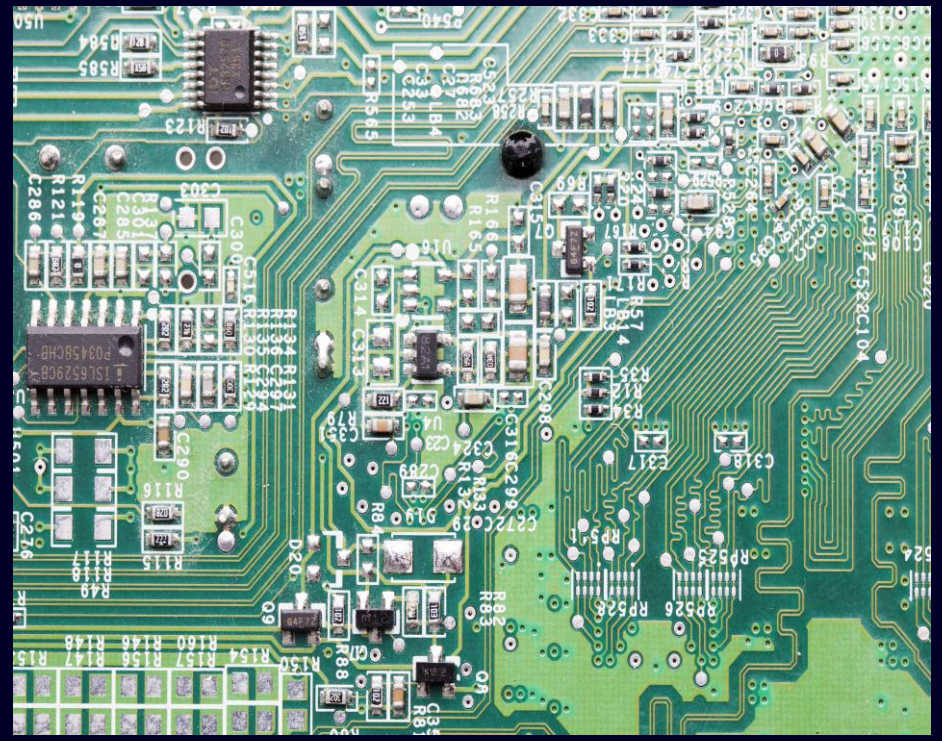
Electronics continue to evolve to produce higher performance in smaller and smaller packages

Not uncommon for a System on a Chip (called SoC or ASIC) to have 10 billion gates

The electronics industry has pioneered use of highly abstract models to drive automated verification (before any silicon is laid down)

But there's a gap that keeps that intense verification work from being sufficient to achieve high levels of assurance we desire and need – there is no direct linkage between requirements and design verification

So, what would help?



Microelectronics cannot (yet) be trusted

Reliance on sophisticated custom-build electronics in critical applications

Unintentional performance issues increasingly likely

Let’s shift focus to the left and close the loop with requirements

Not quite to the “easy button” stage but making progress

Let us share our journey starting with a little background

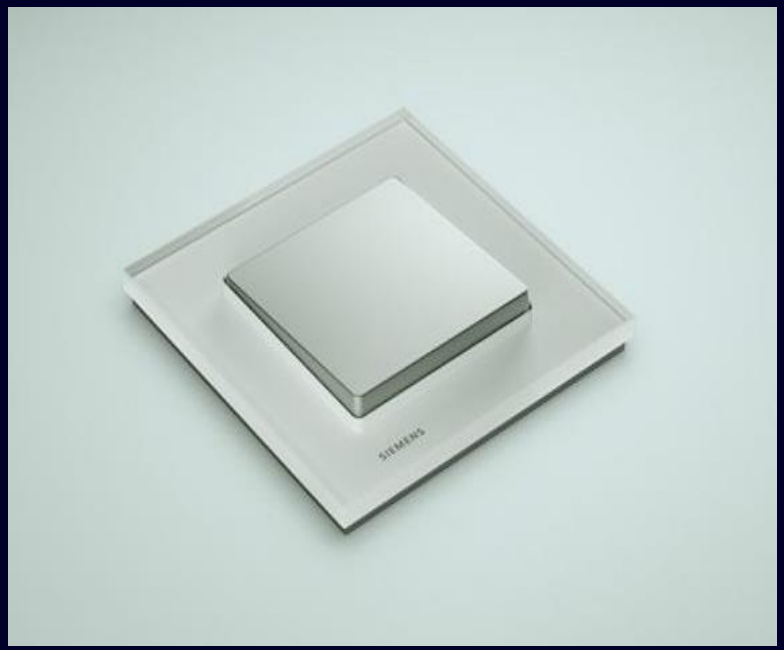
Siemens is now one of the top ten software companies in the world

We’ve been involved in product design and systems engineering for quite a while, including standards efforts

Today, initiatives are underway at Siemens to

- Deliver next-generation MBSE that is SysML V2 compliant*
- Connect electronics verification to systems engineering via MBSE
- Enable a major step forward for trustworthy microelectronics

We call this “Closing the Systems to Silicon Gap”



* *Called Systems Modeling Workbench with Arcadia/Capella*

SE Vision: Connected Engineering of Systems Across the Lifecycle

REQUIRED BEHAVIORAL STRUCTURAL AS DESIGNED AS ORDERED AS BUILT AS DELIVERED AS SERVICED

Systems Engineering

- Begins at the conceptual design phase, continuing throughout the life cycle
- Defines and validates requirements to meet user needs
- Designs, analyzes and verifies a system to meet the requirements

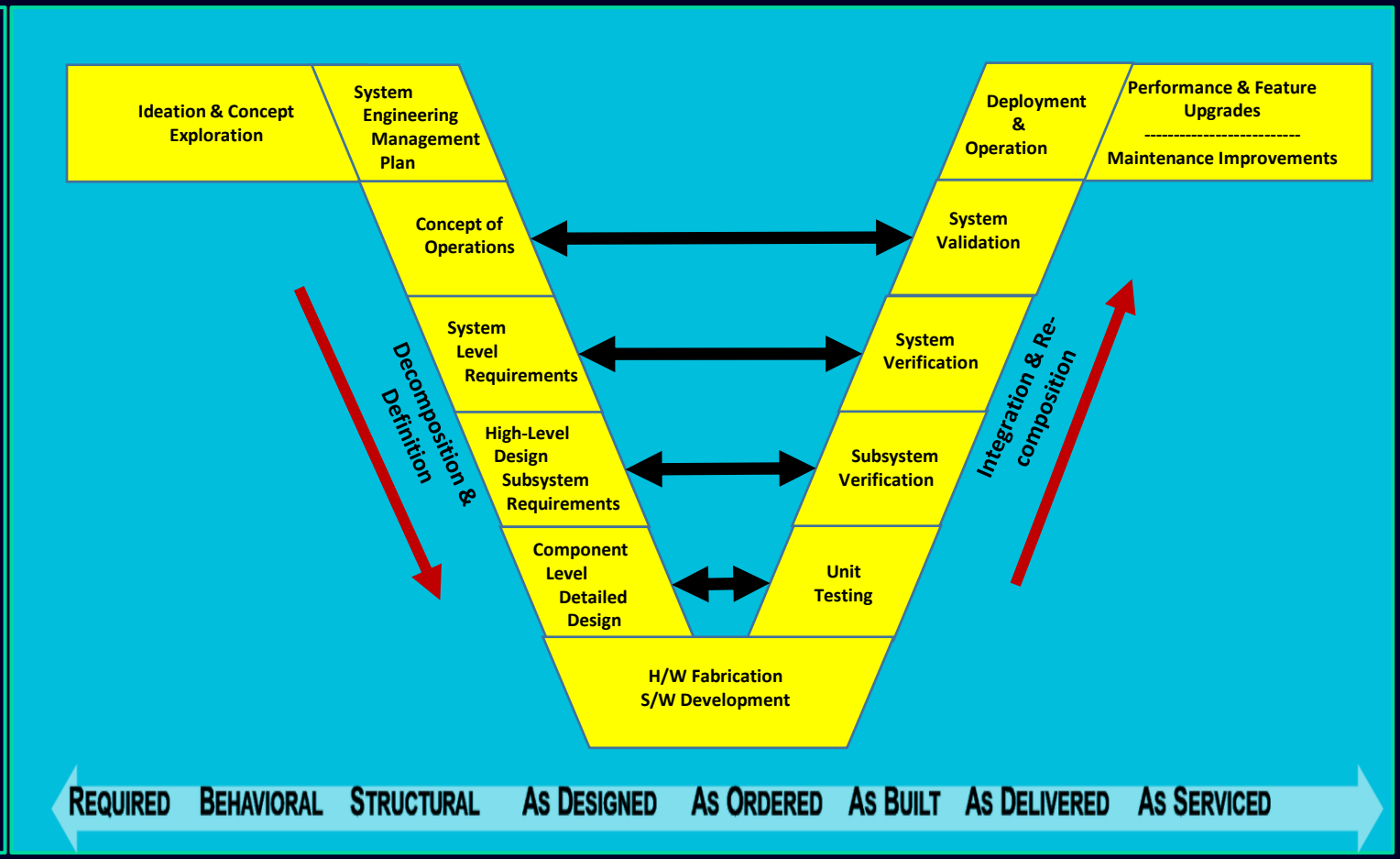
Before there was CAD/CAE, there was Systems Engineering. Many types of SE documents and diagrams were produced, maintained and shared manually.

If MBSE is to be CAD/CAE for SE, are we there yet?

SIEMENS

Engineering “V” – Emphasis on Continuous Verification Levels

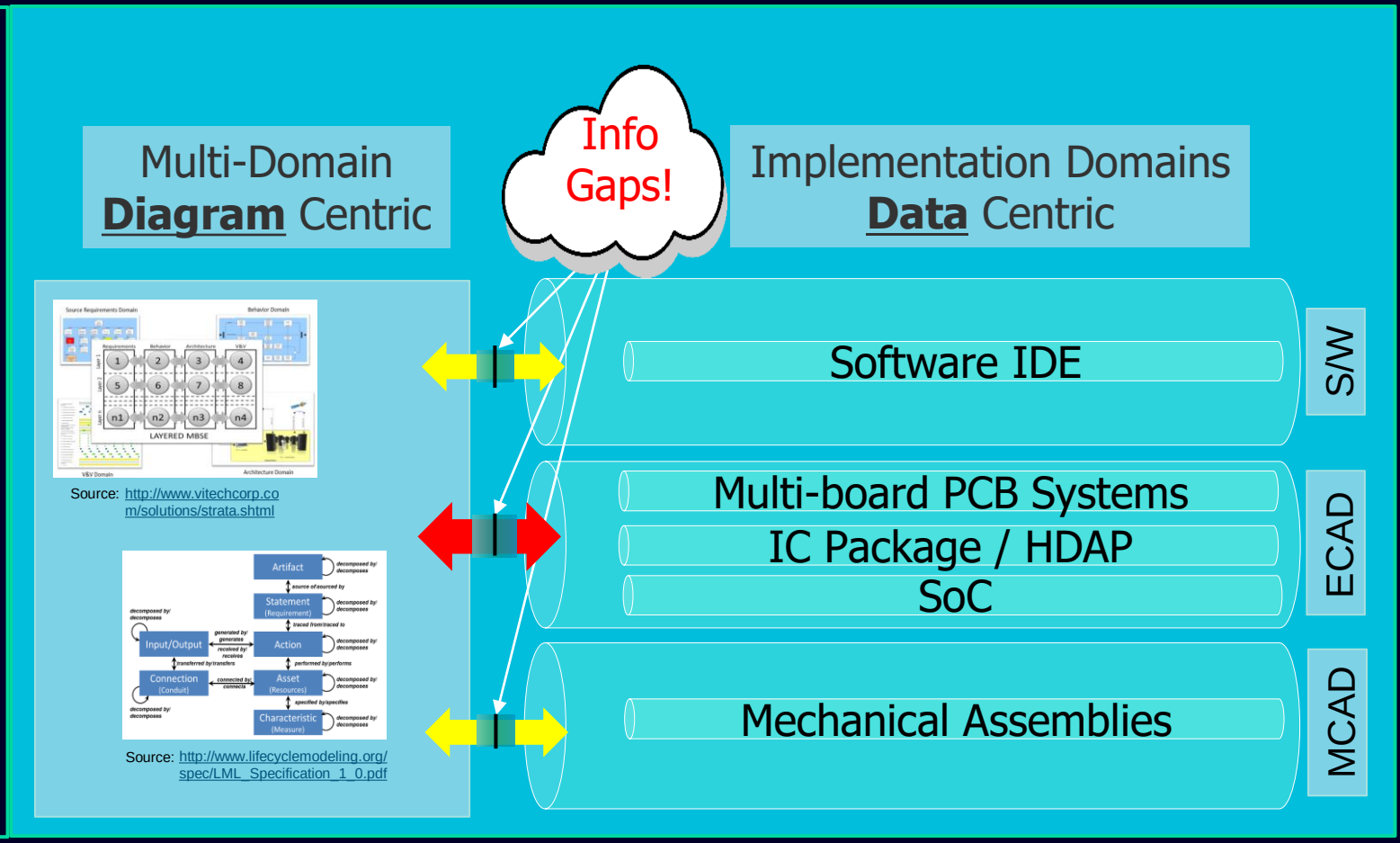
- Verification requires feedback loops in the life cycle timeline
- The engineering “V” diagram emphasizes verification feedback and detail layers
- Requirement verification plans MUST be continuously refined and then performed EARLY
- SE work-products must share architecture info to express requirements to be verified



SIEMENS

Current Electronics Status: MBSE-driven Architecture is NOT SHAREABLE

- Most SE diagrams are not intuitive, and Domain engineers are not fluent in them
- Most diagrams are not stored as data elements in enterprise level database repositories
- Gaps exist which restrict the flow of information and the ECAD gap is the most severe
- ECAD has sub-domain decomposition layers and the deepest verification challenge

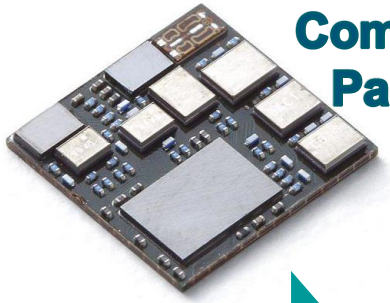


SIEMENS

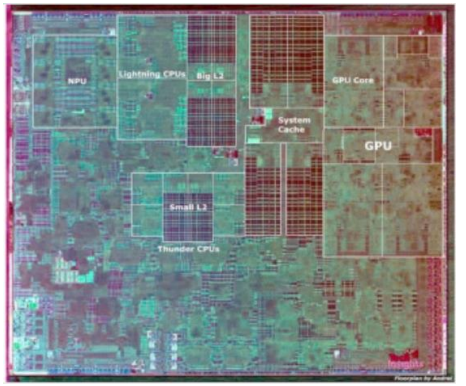
Electronics Requires Continuous Decomposition and Verification to Realize "System-to-Silicon" Verification

Multi-PCB System Enclosure

Printed Circuit Board



Component Package



SoC / ASIC

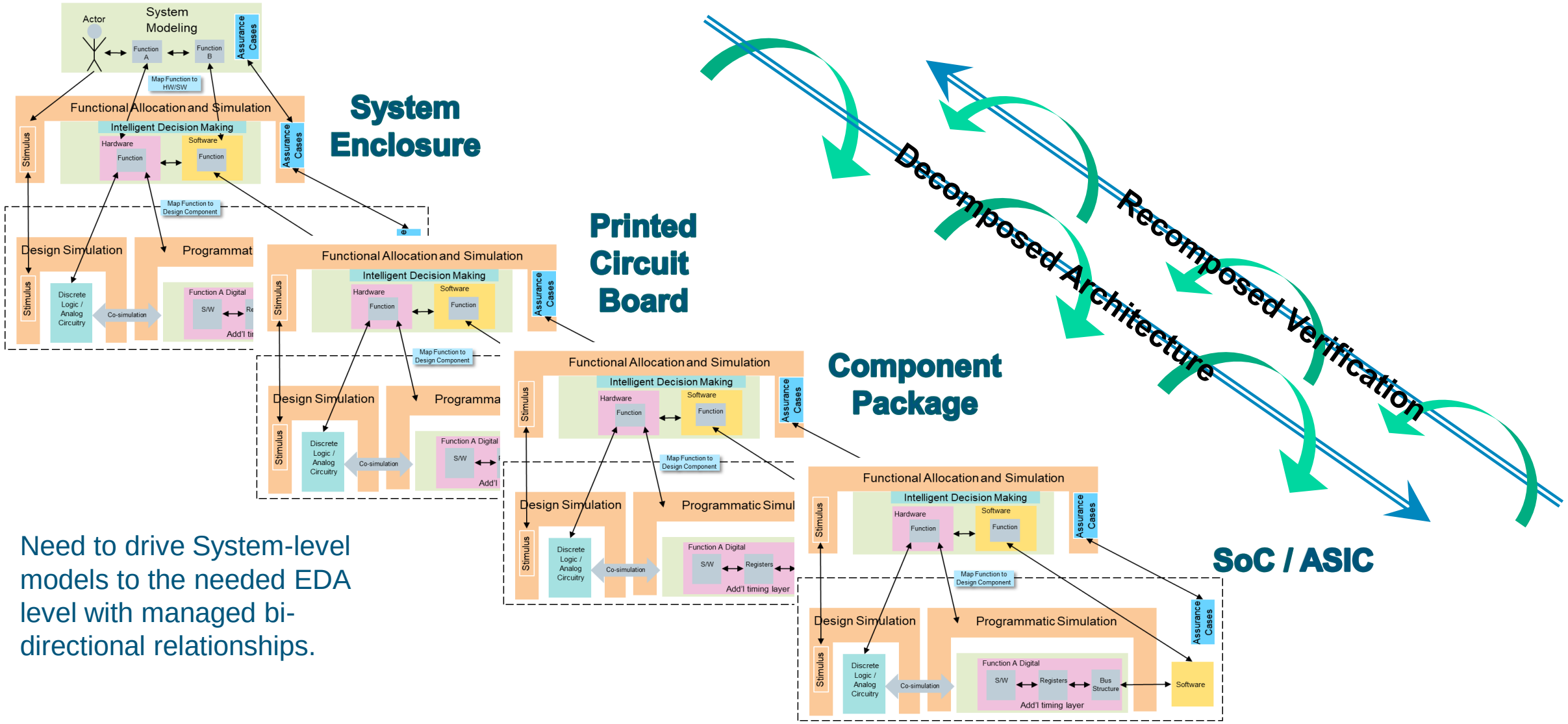
Decomposed Architecture

Recomposed Verification

The epicenter of the complexity explosion: SoCs executing embedded software

SIEMENS

Future State: Commonality Across Workflows, System-to-Silicon

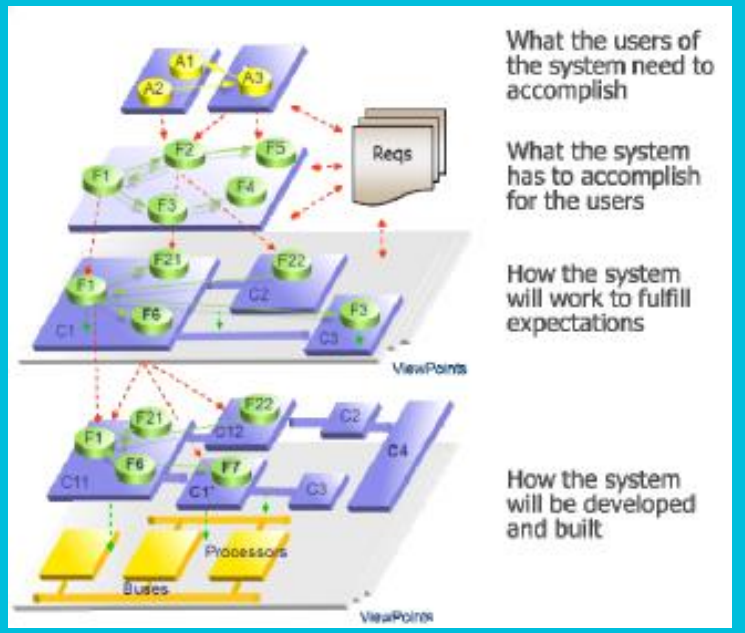


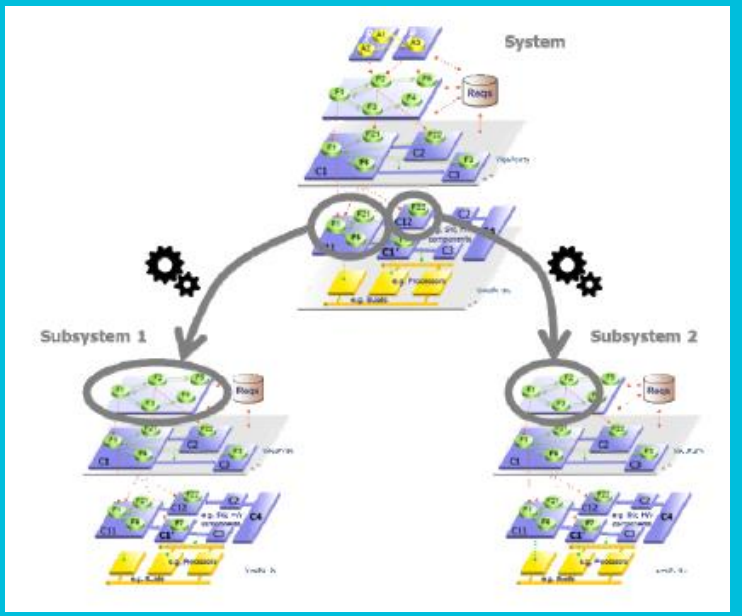
Need to drive System-level models to the needed EDA level with managed bi-directional relationships.

SIEMENS

ARCADIA/Capella Uniquely Addresses Continuous Decomposition

- Focused on Arcadia/Capella as the capability set for continuous decomposition
- Most modern method and tooling with most advanced refinement capabilities
- CAD/CAE style of underlying data model
- Guides the user to assure models are complete and consistent
- Advanced model management via SMW link to Teamcenter

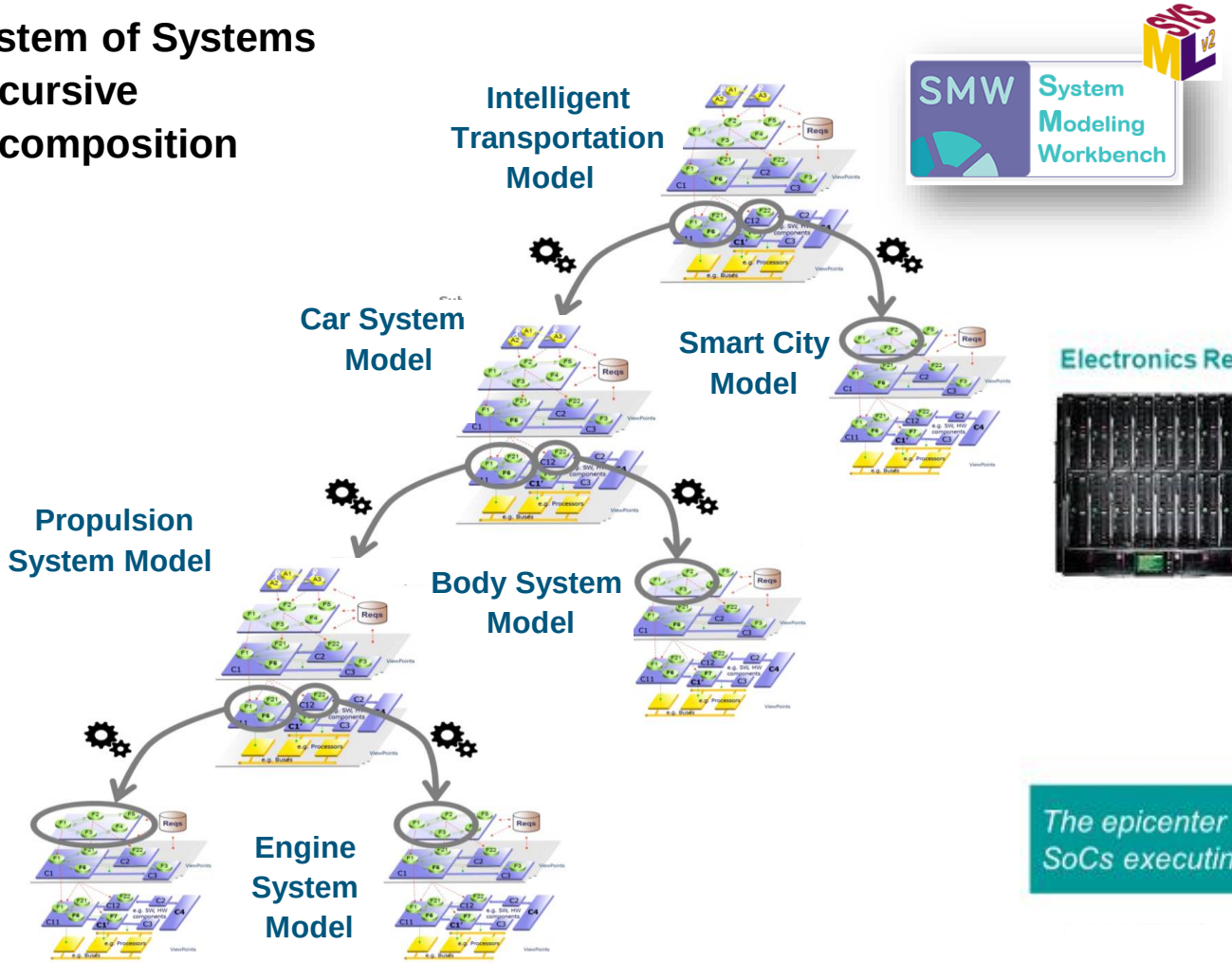




SIEMENS

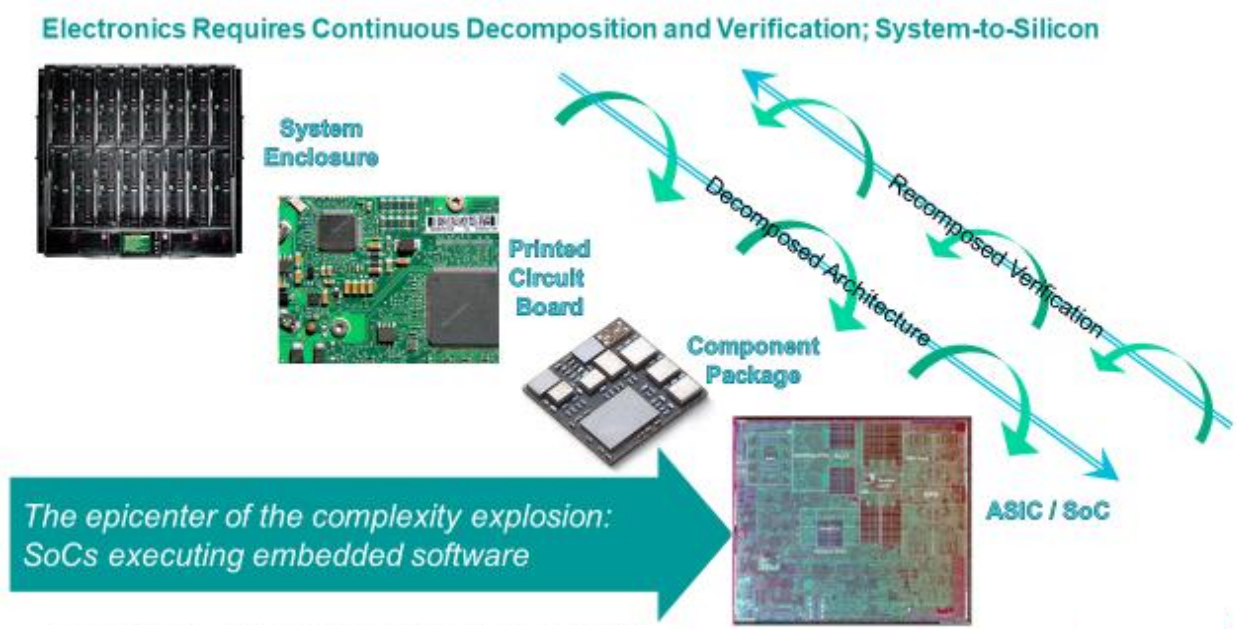
System-to-Silicon Engineering is Now Realizable

System of Systems Recursive Decomposition



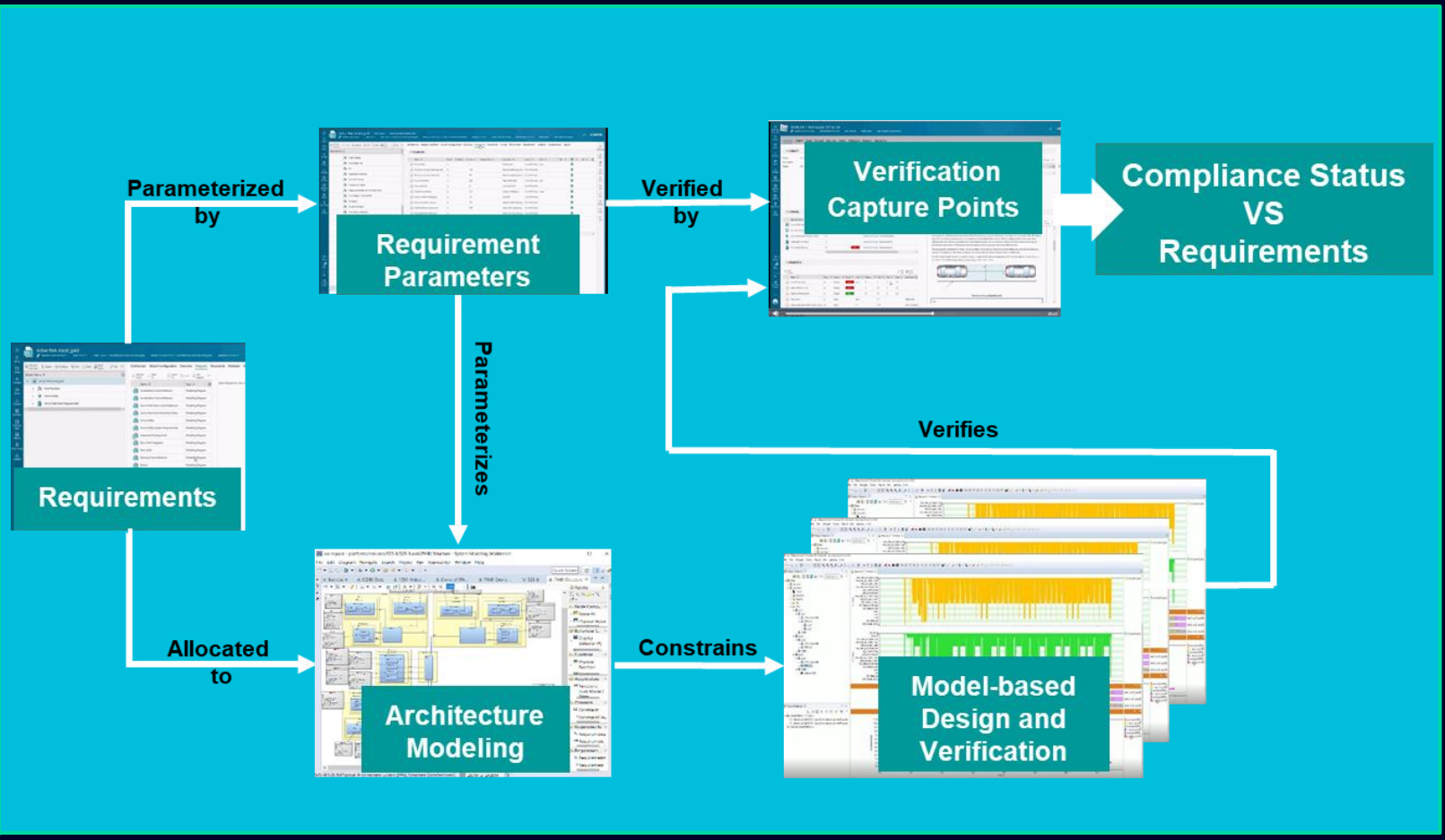
SMW System Modeling Workbench

The decomposition models and their relationships need to be tracked and managed, preferably in one Authoritative Source of Truth.



Proposed: A Solution Pattern for Electronics Verification in an MBSE Context

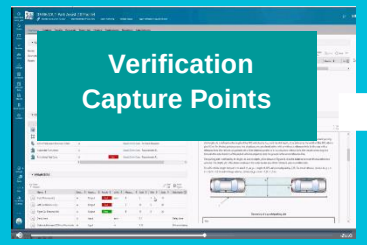
- Requirements are maintained, parameterized, allocated & verified in an ASoT manner
- Design simulation results are compared to parameter values and completes the VCP
- Verification conformance & compliance can be assessed based on total VCP status
- Design/implementation team owns requirement verifiability and refinement



SIEMENS

Verification Capture Points: “Do the Math”

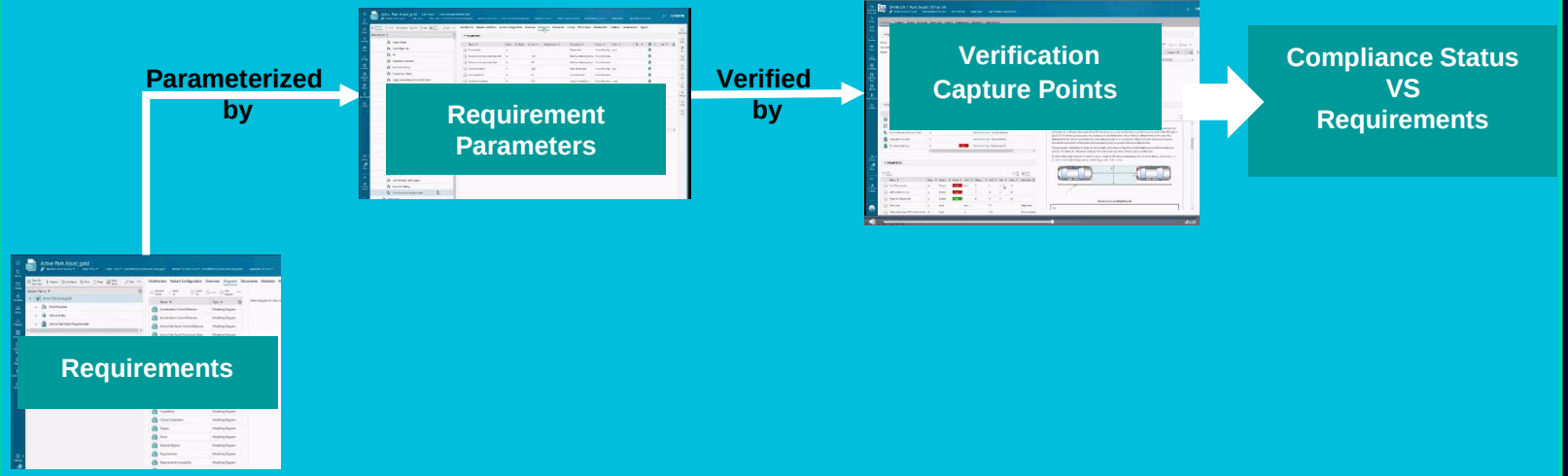
- We must digitalize verification with VCPs
- Implicit requirements currently outweigh explicit parameterized requirements
- Domain specific knowhow will determine what to verify and how to verify it
- Best known methods must be reviewable for escapes and organizational learning



Compliance Status VS Requirements

Requirements must be parameterized

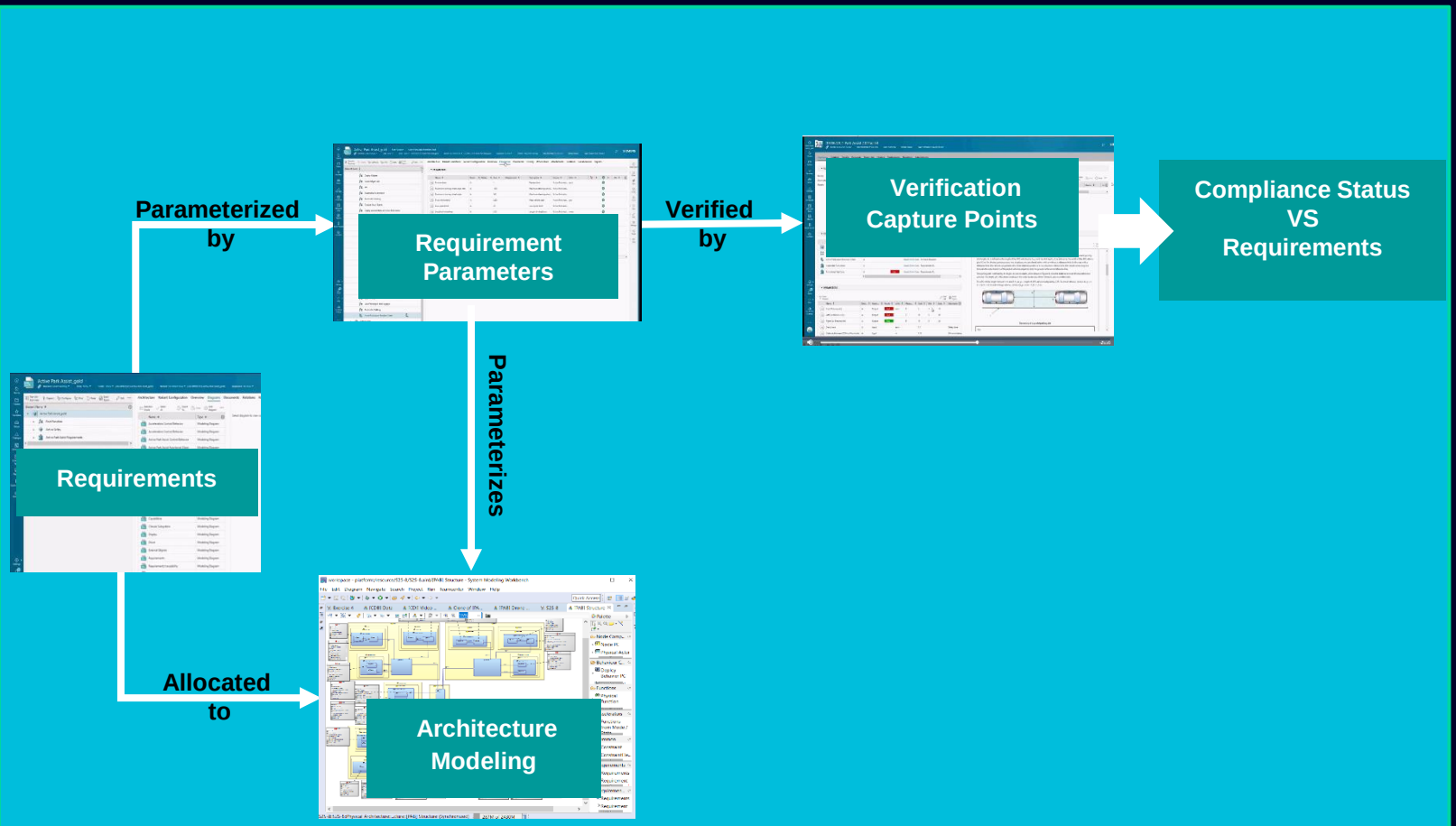
- A shall statement is not enough
- More progress is needed to parameterize and manage parameters
- The VCP math must be automatable
- Domain SMEs must own requirements decomposition



SIEMENS

Requirements Must Parameterize Architecture Models

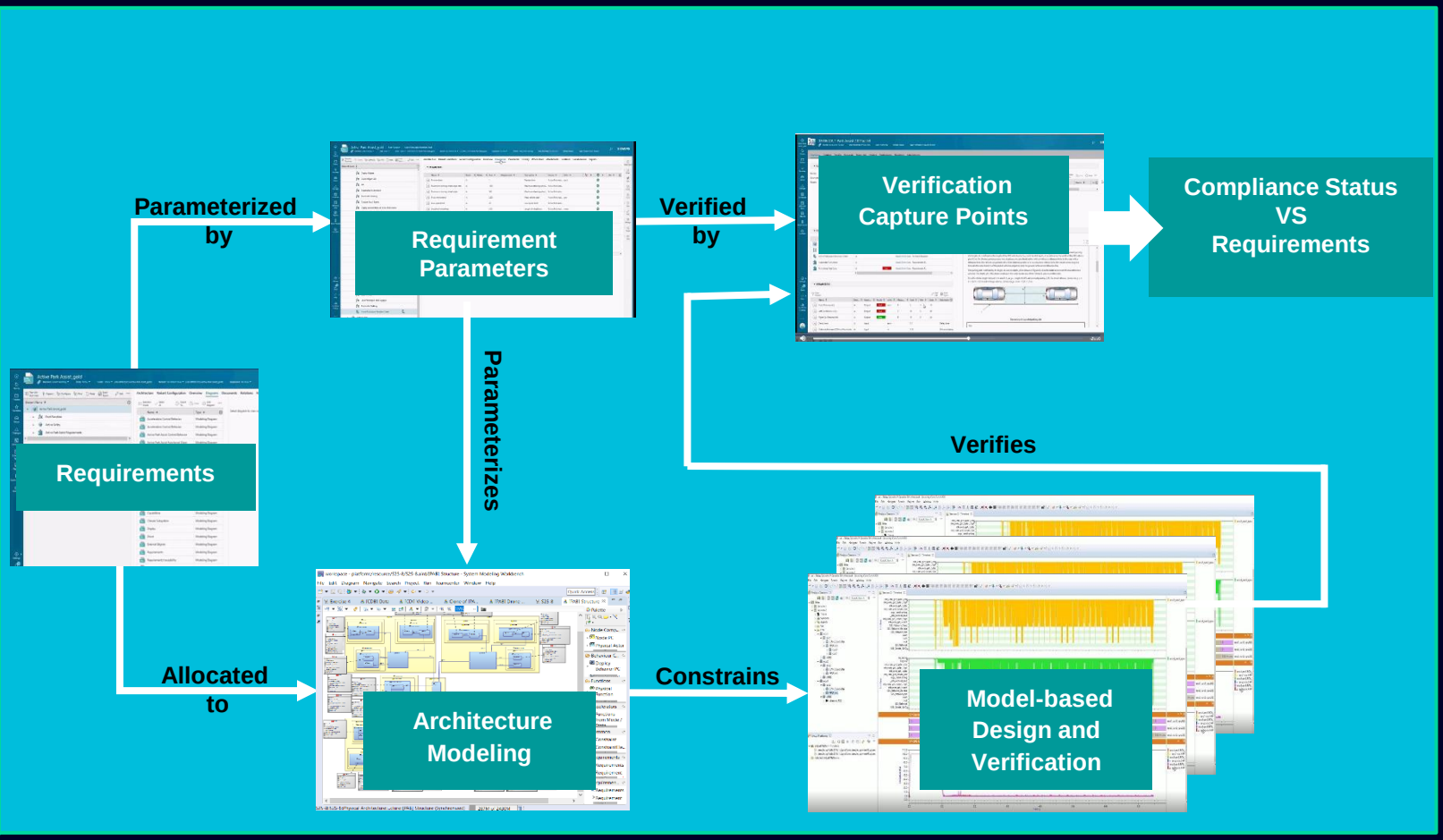
- Architecture must decompose from functions based on operational scenarios
- Requirement parameters must be allocated to architecture elements
- Enable the development and exploration of architecture options
- Domain SMEs must own architecture decomposition and refinement



SIEMENS

Closing the Info Gap

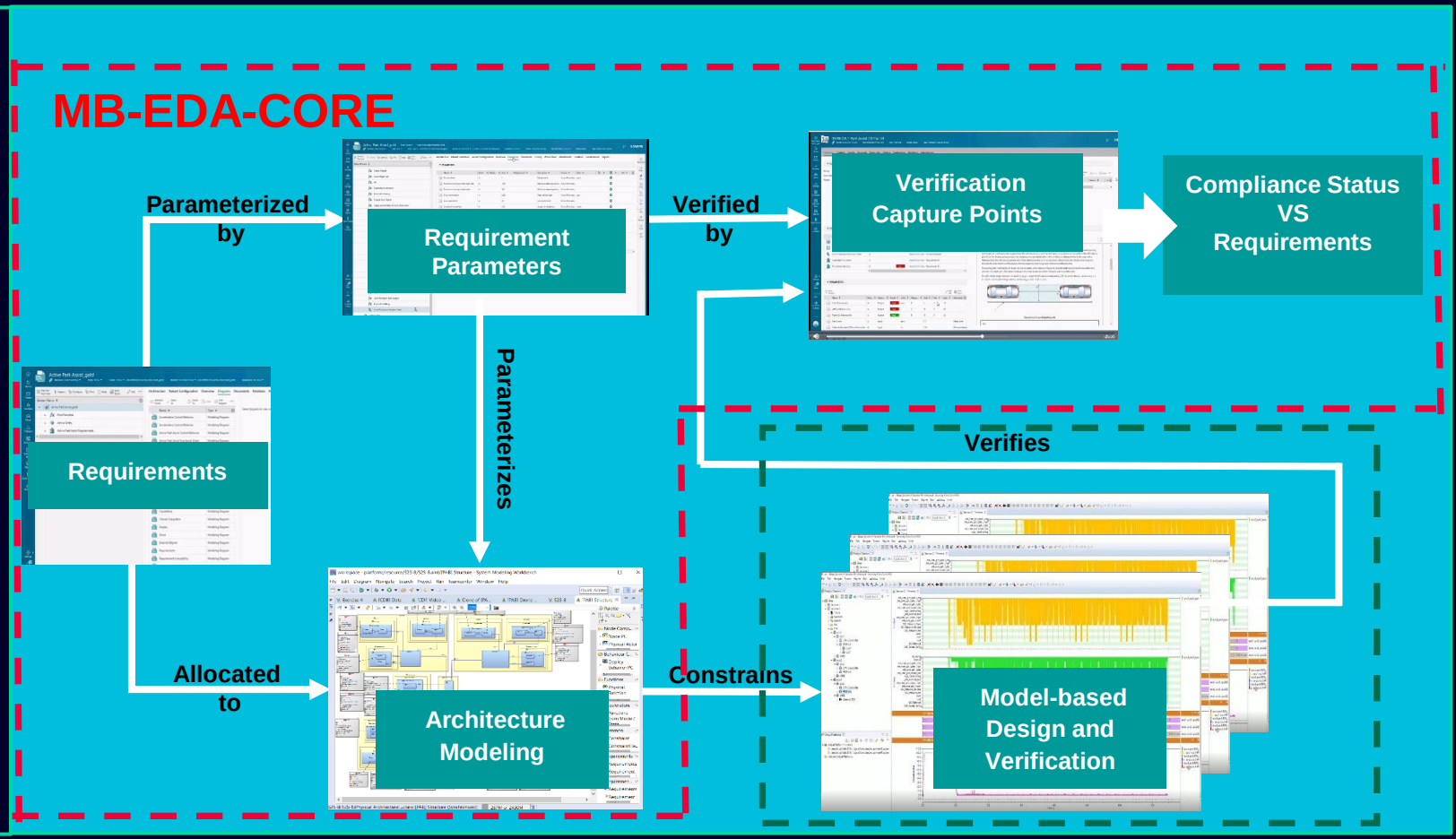
- One architecture can drive multiple sub-domains
- Enables simulation-based architecture optimization
- Architecture compliance to requirements is captured in the VCP
- Optimized architecture constrains and specifies design and implementation



SIEMENS

A Solution Pattern Implementation Consists of both Domain Independent (ASoT) and Domain/Sub-domain Dependent Workflow Components and Tools

- Enabling the ASoT can be domain independent and non-ECAD specific
- Domain specific tools can potentially be any design and verification toolset
- Domain specific tools will likely need automation to increase efficiency / reduce cycle time
- Bottom-up approach: Implement VCPs for what is simulated today



SIEMENS

Path to Standards Conformance:
ISO 24641 for Systems Engineering Methodology and Tools

Tooled Method to: Define, Analyze, Design & Verify System, SW, HW Architectures

Operational Analysis

System Analysis

Logical Architecture

Physical Architecture

Define Stakeholder Needs and Environment

Capture and consolidate operational needs from stakeholders
Define what the users of the system have to accomplish
Identify entities, actors, roles, activities, concepts

Formalize System Requirements

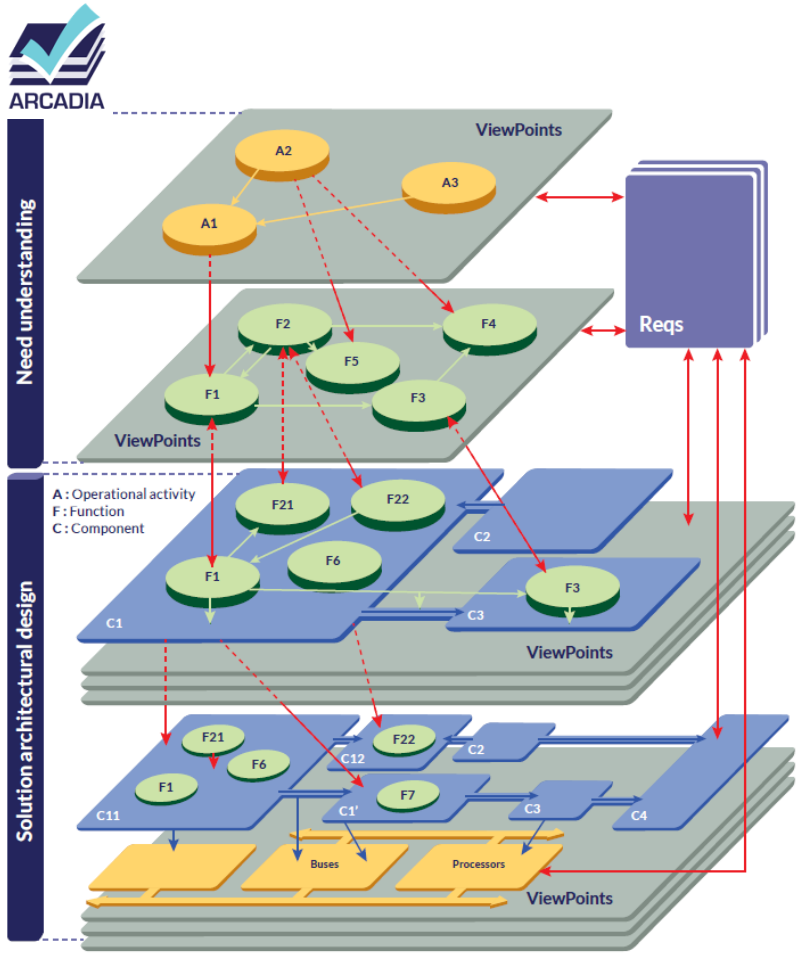
Identify the boundary of the system, consolidate requirements
Define what the system has to accomplish for the users
Model functional dataflows and dynamic behaviour

Develop System Logical Architecture

See the system as a white box: define how the system will work so as to fulfill expectations
Perform a first trade-off analysis

Develop System Physical Architecture

How the system will be developed and built
Software vs. hardware allocation, specification of interfaces, deployment configurations, trade-off analysis



Operational Analysis
What the users of the system need to accomplish

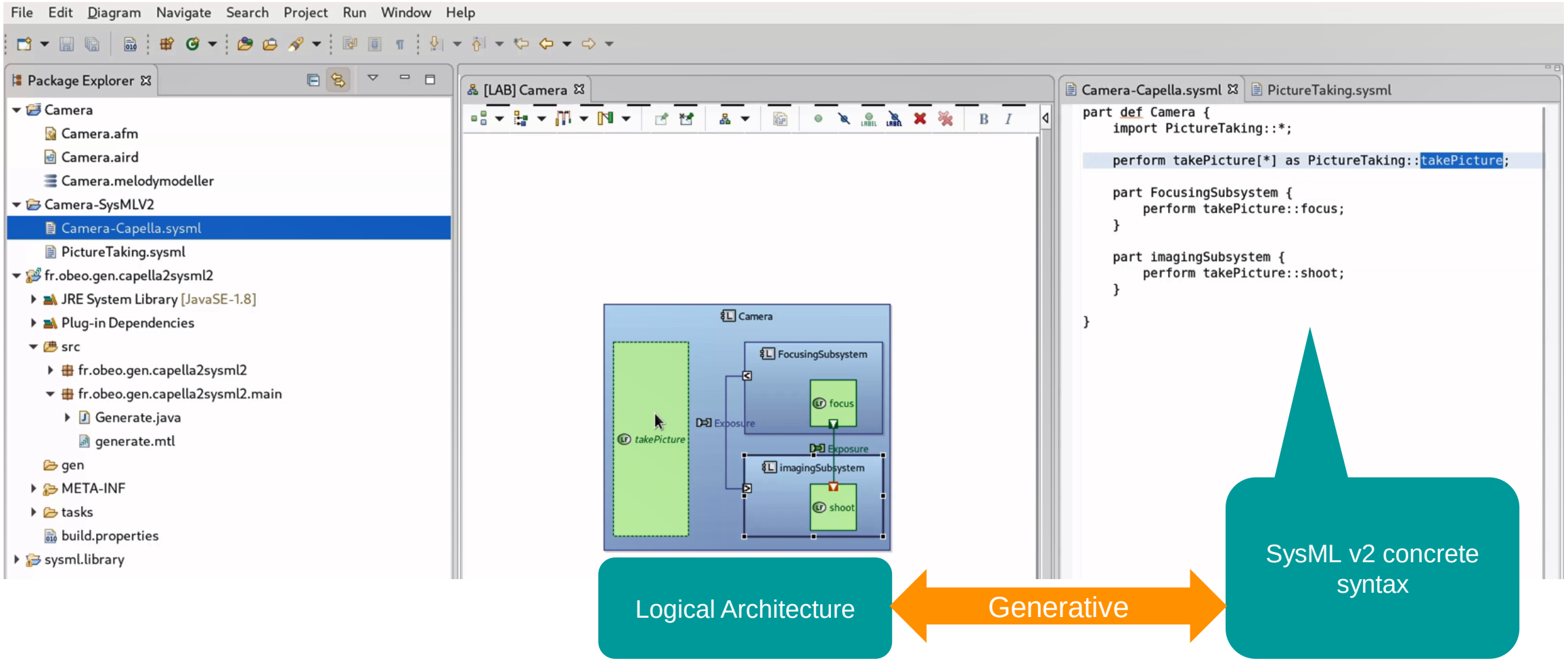
Functional & Non Functional Need
What the system has to accomplish for the users

Logical Architecture
How the system will work to fulfill expectations

Physical Architecture
How the system will be developed and built

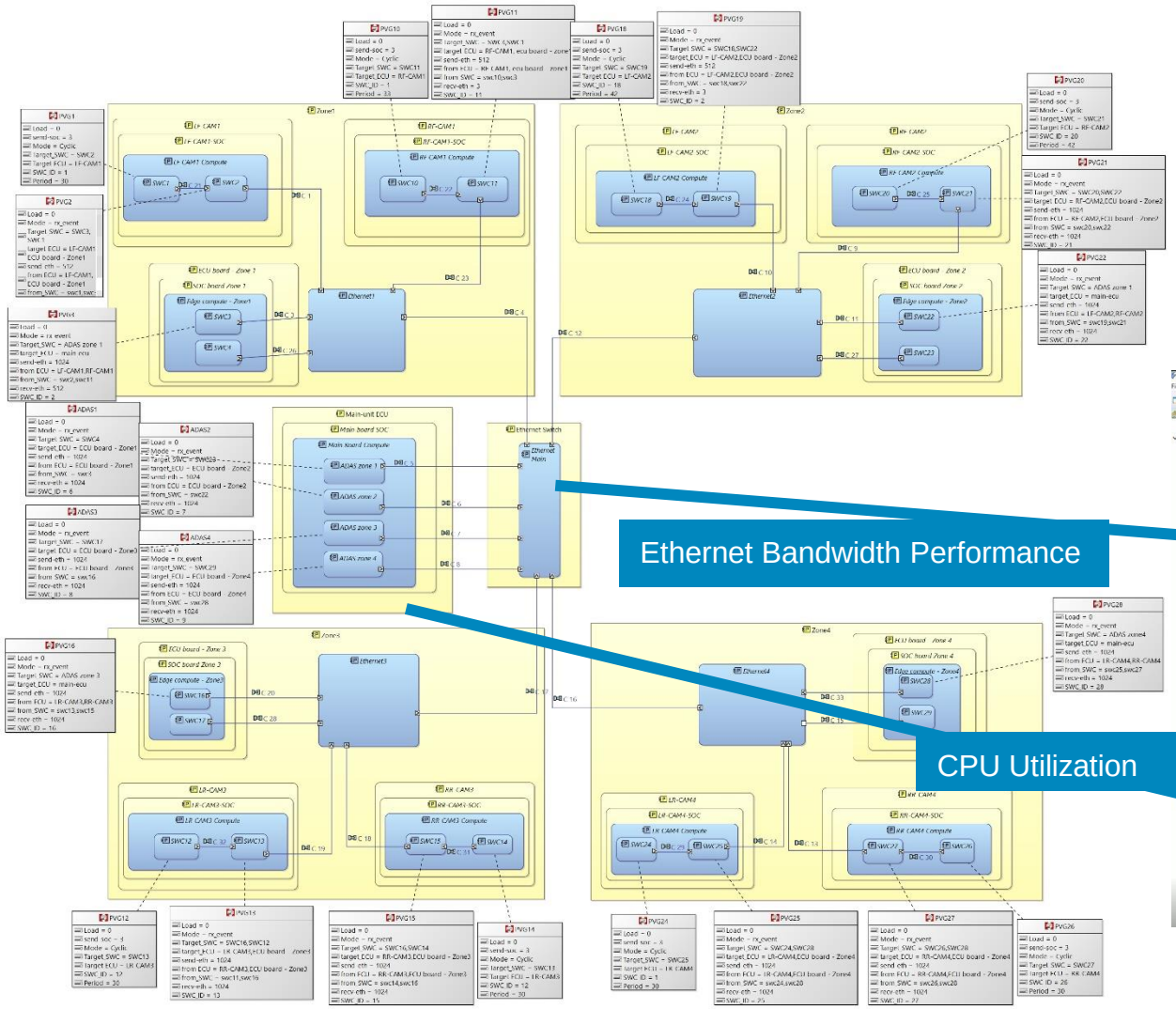
SIEMENS

Path to Standards Conformance:
Working toward Capella Generative SysML V2 Concrete Syntax



SIEMENS

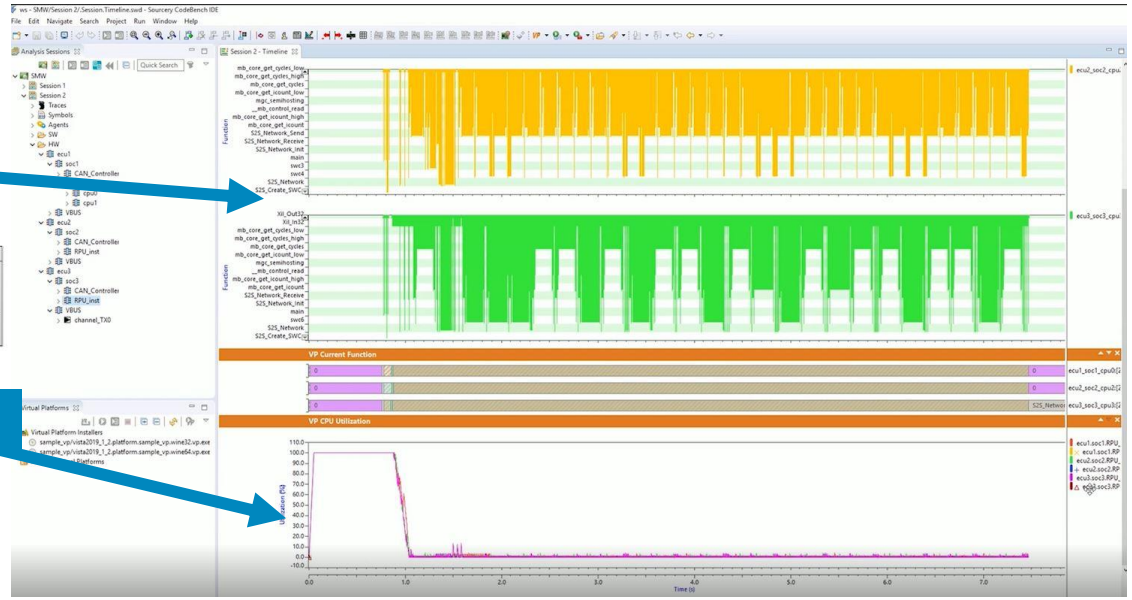
Architecture Exploration by Transaction Level Simulation: System-to-Silicon



Ethernet Bandwidth Performance

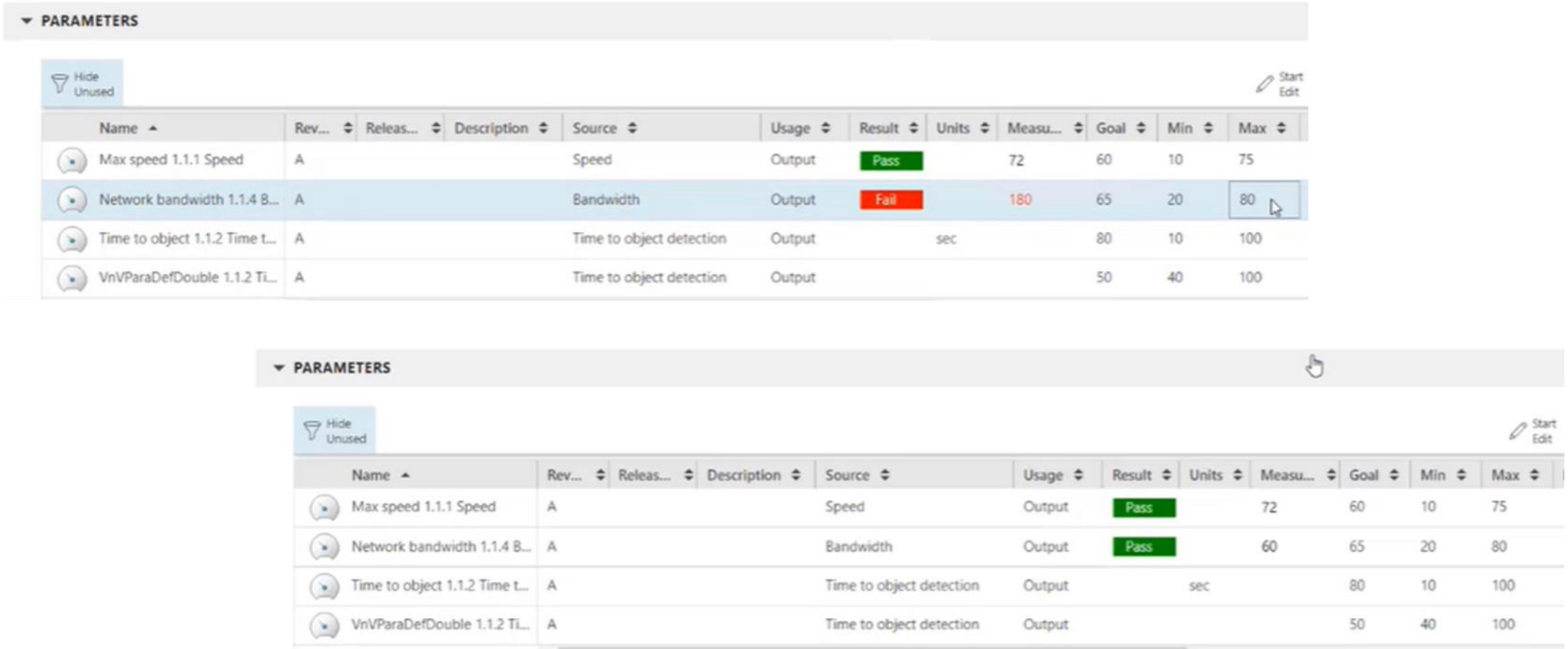
CPU Utilization

Dynamic Transaction Analysis



SIEMENS

Verification Capture Point Example



PARAMETERS

Hide Unused

Start Edit

Name	Rev...	Releas...	Description	Source	Usage	Result	Units	Measu...	Goal	Min	Max
Max speed 1.1.1 Speed	A			Speed	Output	Pass		72	60	10	75
Network bandwidth 1.1.4 B...	A			Bandwidth	Output	Fail		180	65	20	80
Time to object 1.1.2 Time t...	A			Time to object detection	Output		sec		80	10	100
VnVParaDefDouble 1.1.2 Ti...	A			Time to object detection	Output				50	40	100

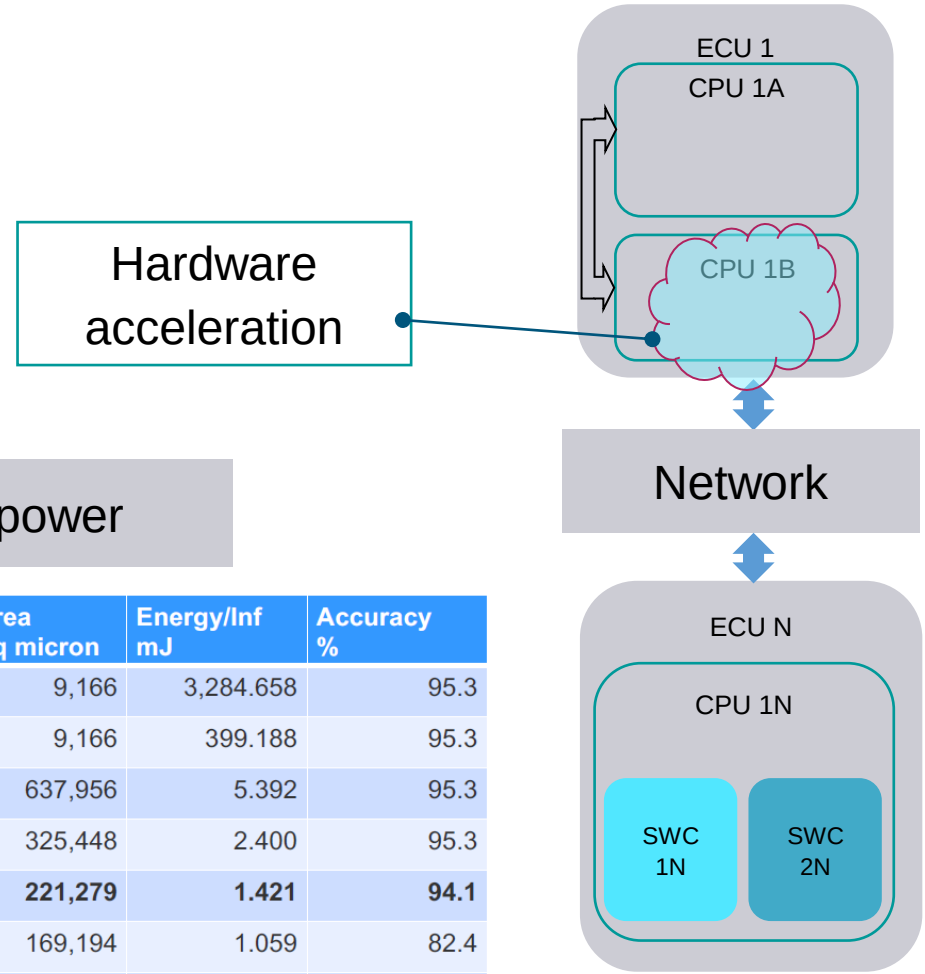
PARAMETERS

Hide Unused

Start Edit

Name	Rev...	Releas...	Description	Source	Usage	Result	Units	Measu...	Goal	Min	Max
Max speed 1.1.1 Speed	A			Speed	Output	Pass		72	60	10	75
Network bandwidth 1.1.4 B...	A			Bandwidth	Output	Pass		60	65	20	80
Time to object 1.1.2 Time t...	A			Time to object detection	Output		sec		80	10	100
VnVParaDefDouble 1.1.2 Ti...	A			Time to object detection	Output				50	40	100

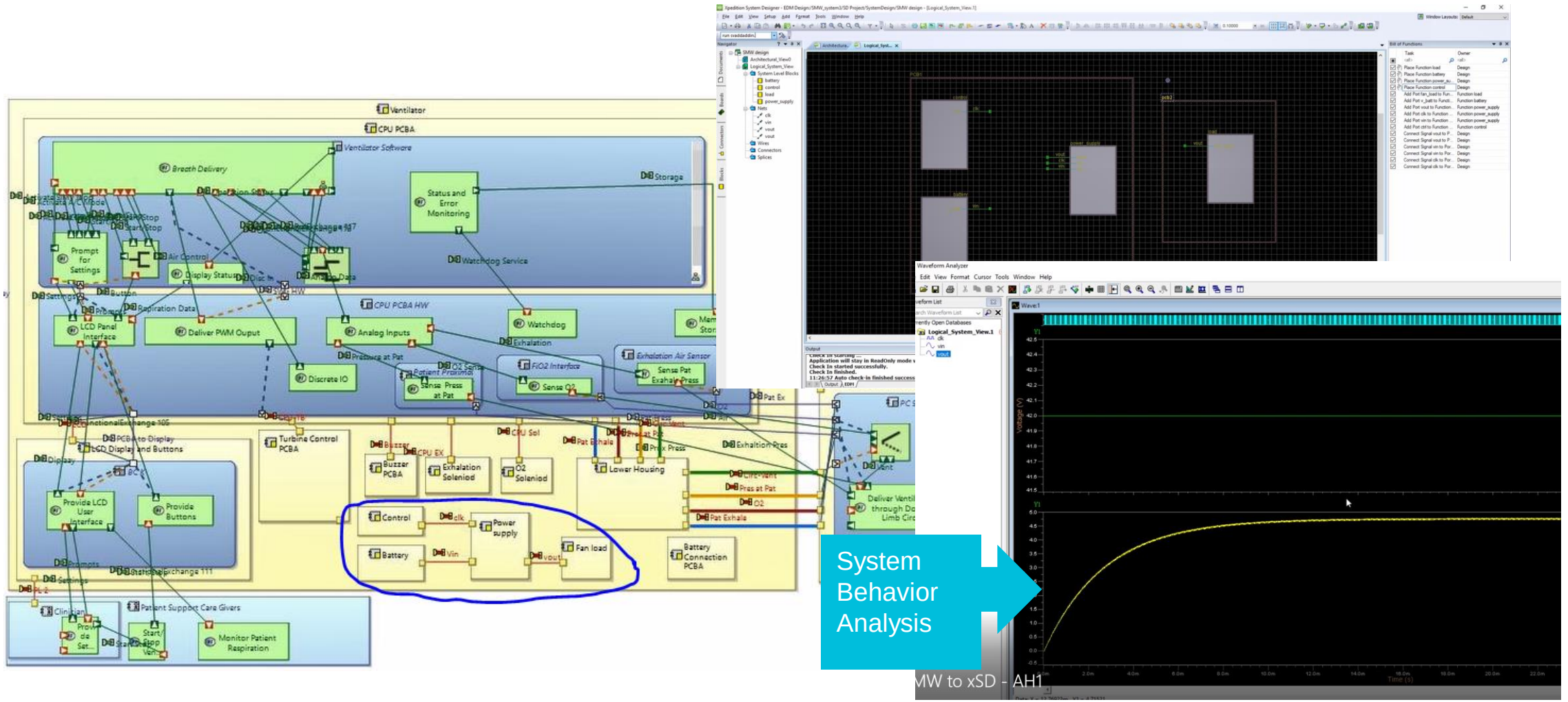
Architecture can be Refined using H/W Acceleration Synthesis



KPI analysis for speed/power

Configuration	Speed seconds	Power mW	Area Sq micron	Energy/Inf mJ	Accuracy %
Software Float	4,961.719	0.662	9,166	3,284.658	95.3
Software Fixed	616.031	0.648	9,166	399.188	95.3
Par1	2.003	2.692	637,956	5.392	95.3
Par2	1.001	2.398	325,448	2.400	95.3
Par3	**0.667**	**2.131**	**221,279**	**1.421**	**94.1**
Par4	0.536	1.975	169,194	1.059	82.4
Par5	0.416	1.776	137,994	0.739	44.8

Architecture Implementation: Interoperable PCB Flow

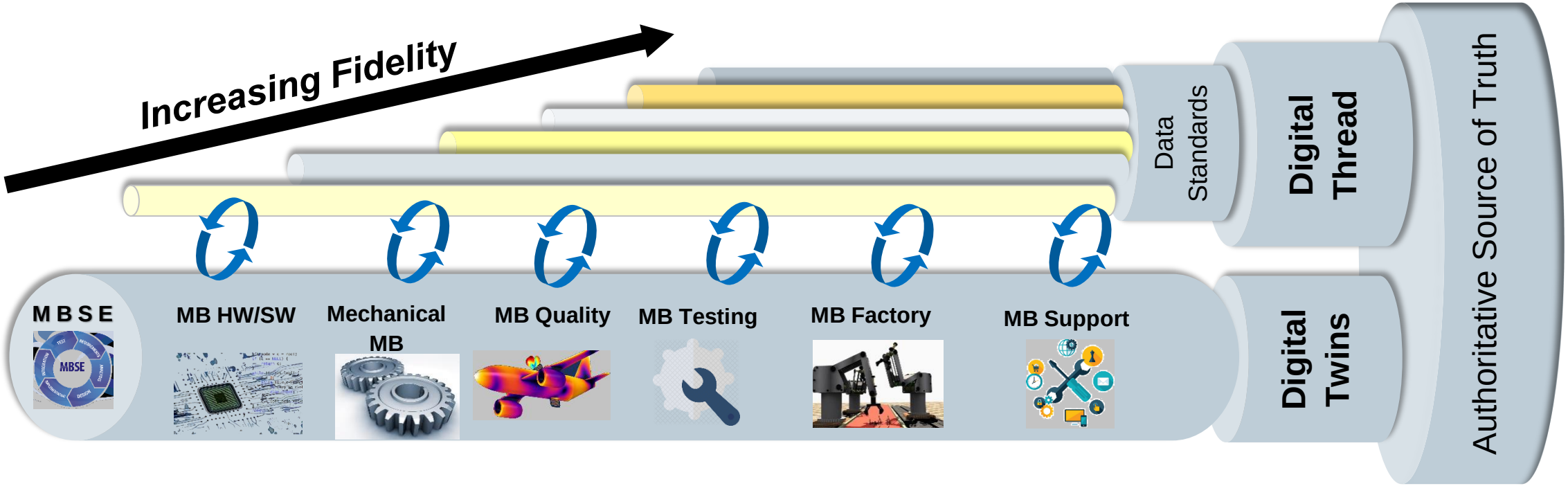


SIEMENS

Digital Transformation is Enabled by Digital Twinning and Threading

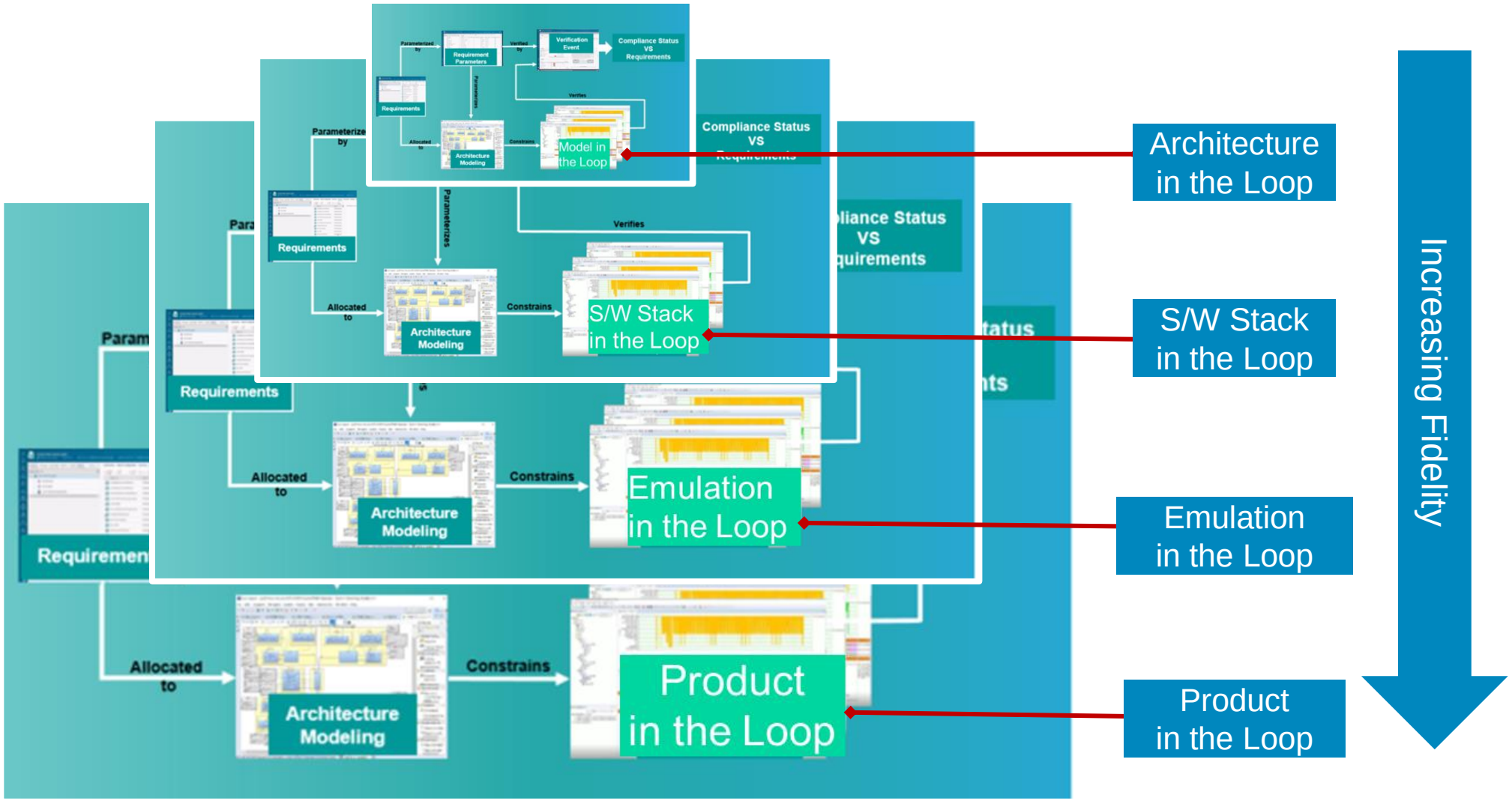
Digital Thread: The authoritative technical data providing decision makers the right data at the right time across the system life cycle

Digital Twin: An integrated digital simulation, enabled by digital threading



SIEMENS

Hybridizing the Digital Twin



SIEMENS

Closing the System to Silicon Gap for Trustworthy Electronics

Siemens is delivering MBSE-Enabled Digital Electronics Verification

We offer a solution pattern for electronics verification in an MBSE context

Initial pilot project results are encouraging; progress made in challenging areas

Additional projects being pursued to industrialize solution

SIEMENS

Contacts

Lisa Murphy
Technology Consultant
Siemens Digital Industries Software
Aerospace, Defense, Federal & Marine
Atlanta, Georgia
USA

Phone (770) 548-5225

E-mail lisa.murphy@siemens.com

Mark Malinoski
Technology Consultant
Siemens EDA
MBSE Solutions Director
Kirkland, Washington
USA

Phone (503) 685-1556

E-mail Malinoski@siemens.com

SIEMENS