Formal Model-Based Design & Manufacture:

A Template for Managing Complexity in Large-Scale Cyber-Physical Systems

Paul Eremenko

fmr. Deputy Director/Acting Director
Tactical Technology Office

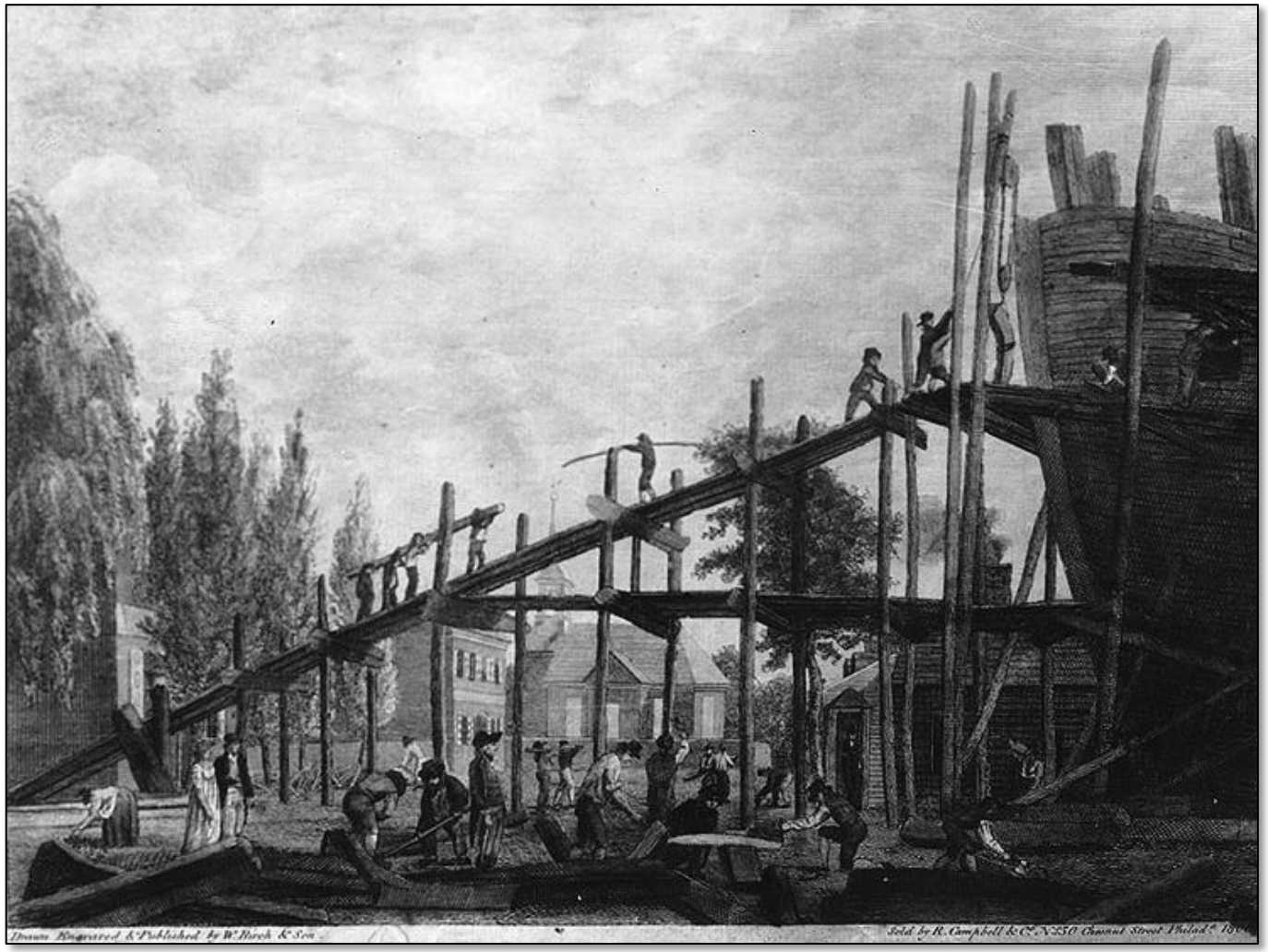
Briefing prepared for the
Conference on Systems Engineering Research

March 21, 2013

The six frigates (1794)

"… the sum of $688,888… to provide, equip and employ, four ships to carry forty guns each, and two ships to carry thirty-six guns each…."

--An Act to Provide a Naval Armament, March 27, 1794



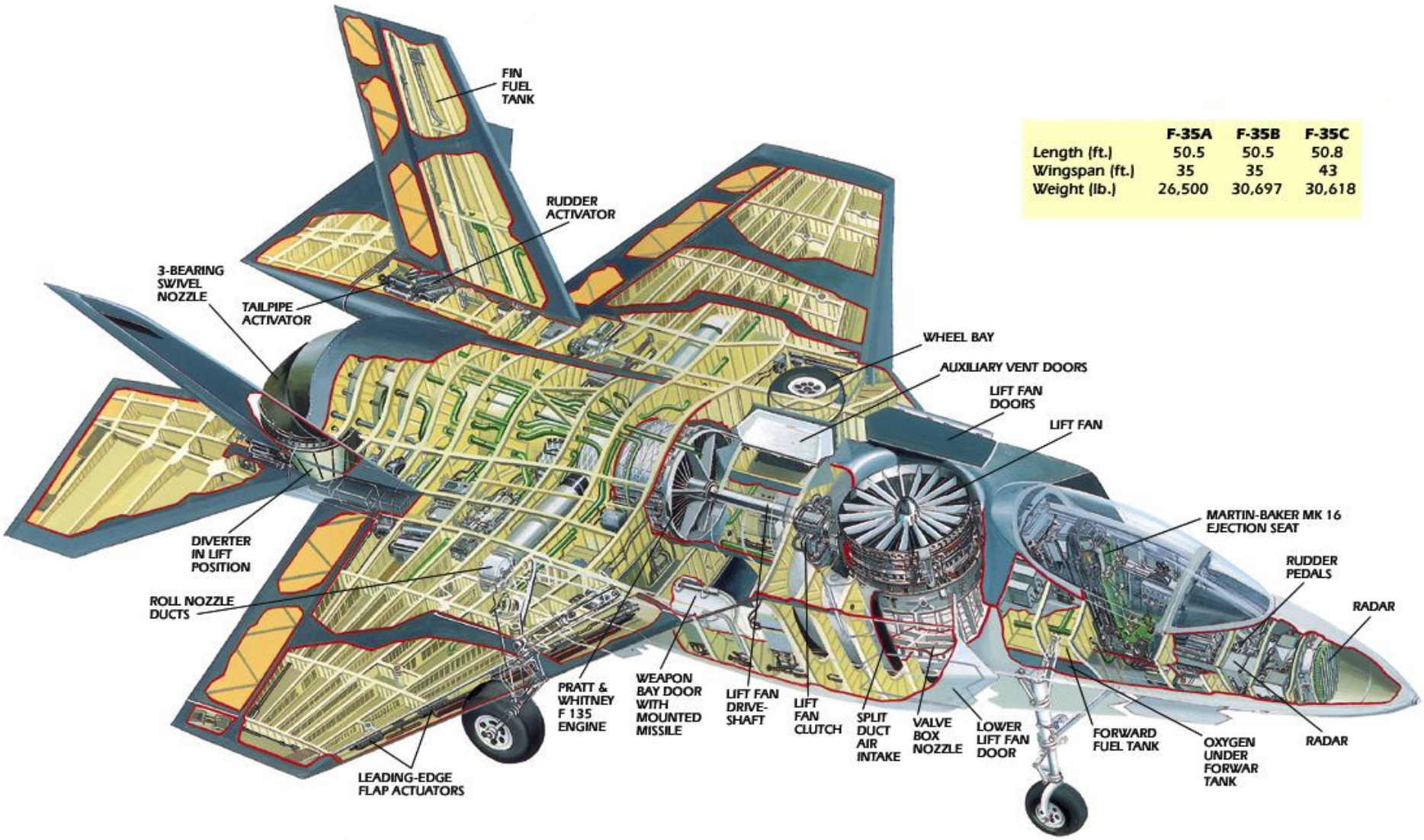
USS Philadelphia, Tripoli Harbor, February 16, 1804

B-52 Stratofortress (1946)

"It is desired that the requirements set forth be considered as a goal and that the proposal be for an interim airplane to approximate all requirements, except that emphasis must be placed on meeting the high speed requirement... It is the intent that design proposals should present the best possible over-all airplane..."
--Directive letter inviting design proposals for the B-52 bomber, February 13, 1946

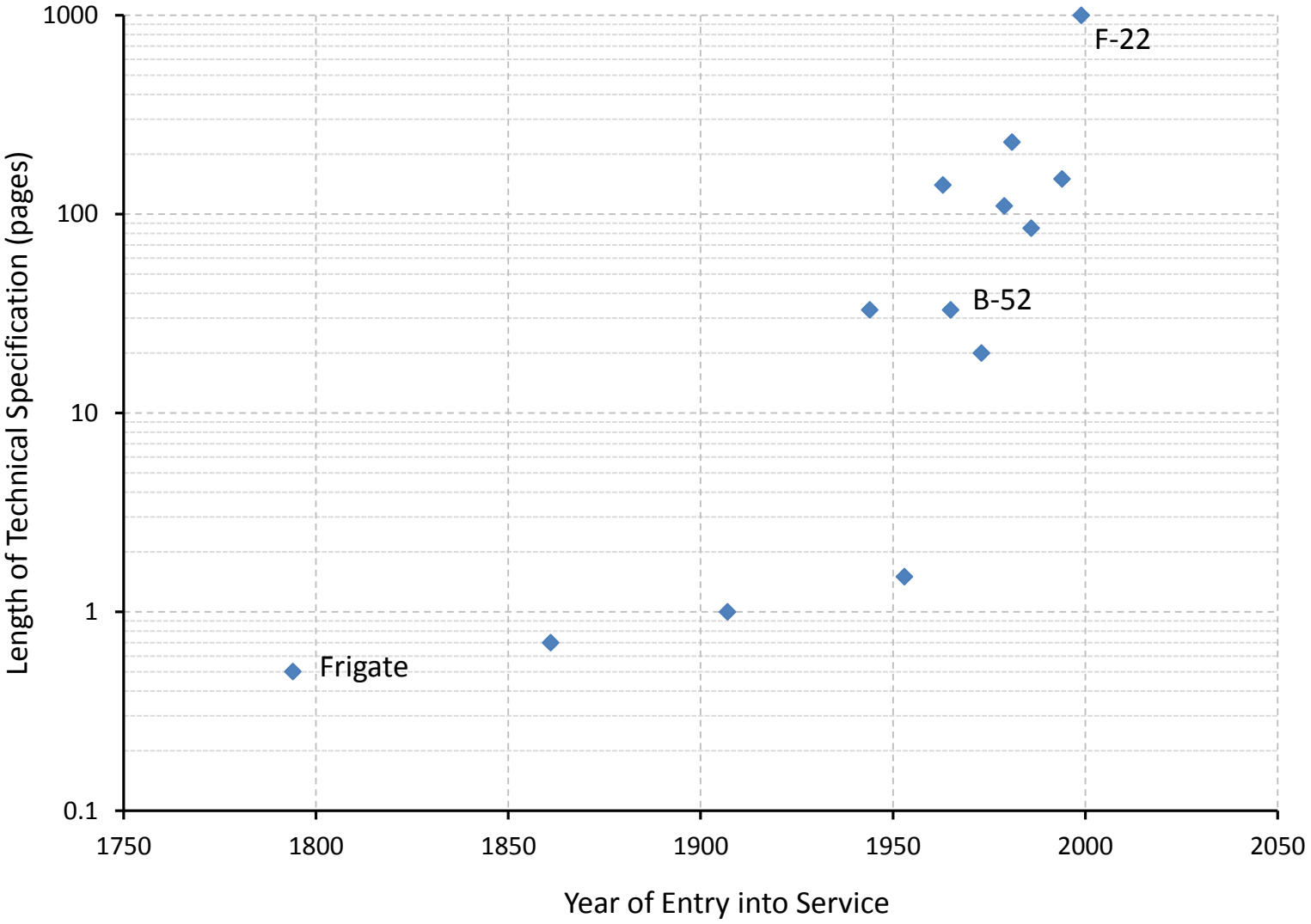
F-111 Aardvark (1961)

F-35 Joint Strike Fighter (2001)



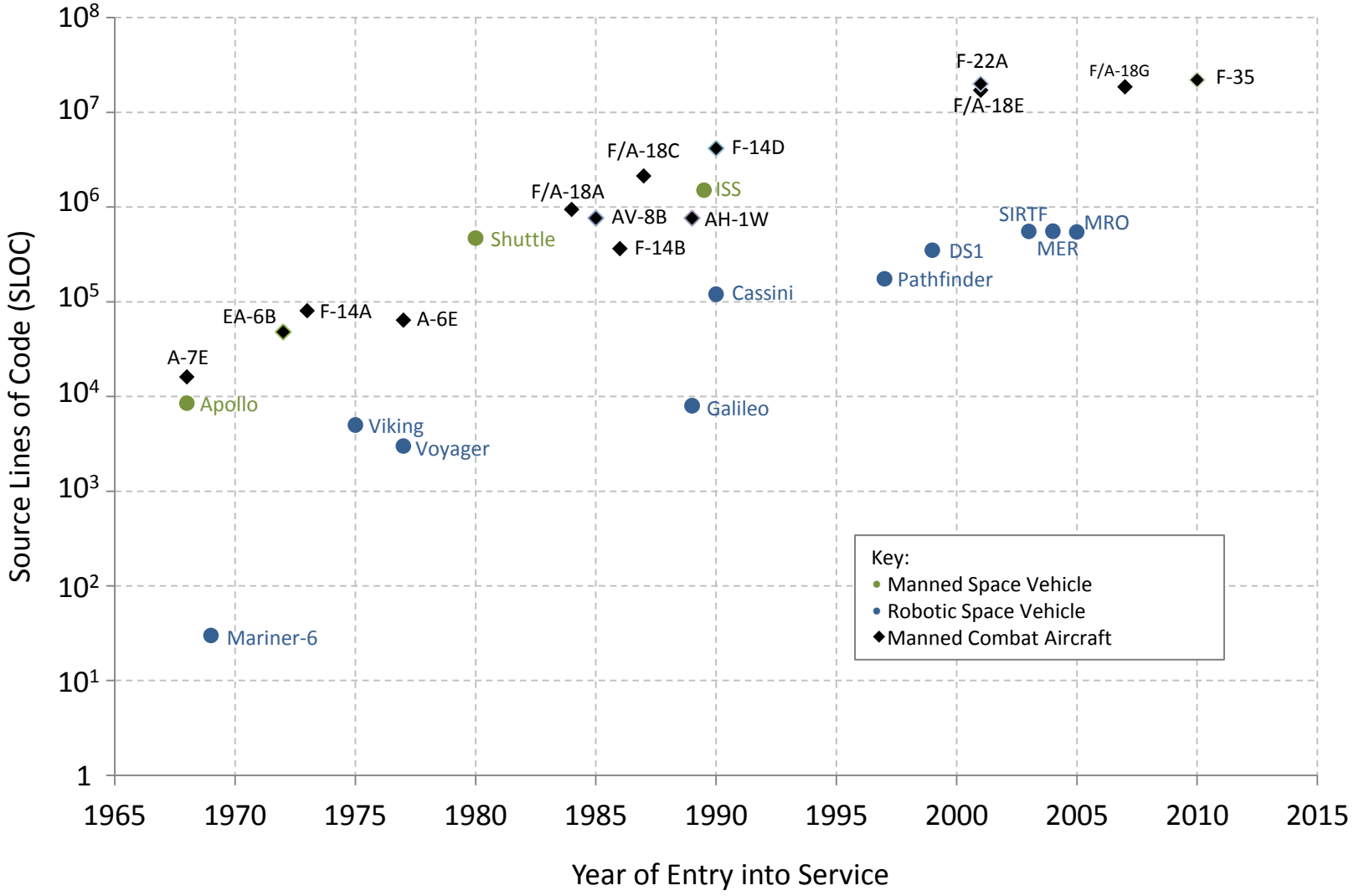
	F-35A	F-35B	F-35C
Length (ft.)	50.5	50.5	50.8
Wingspan (ft.)	35	35	43
Weight (lb.)	26,500	30,697	30,618

Kolmogorov complexity (sort of)



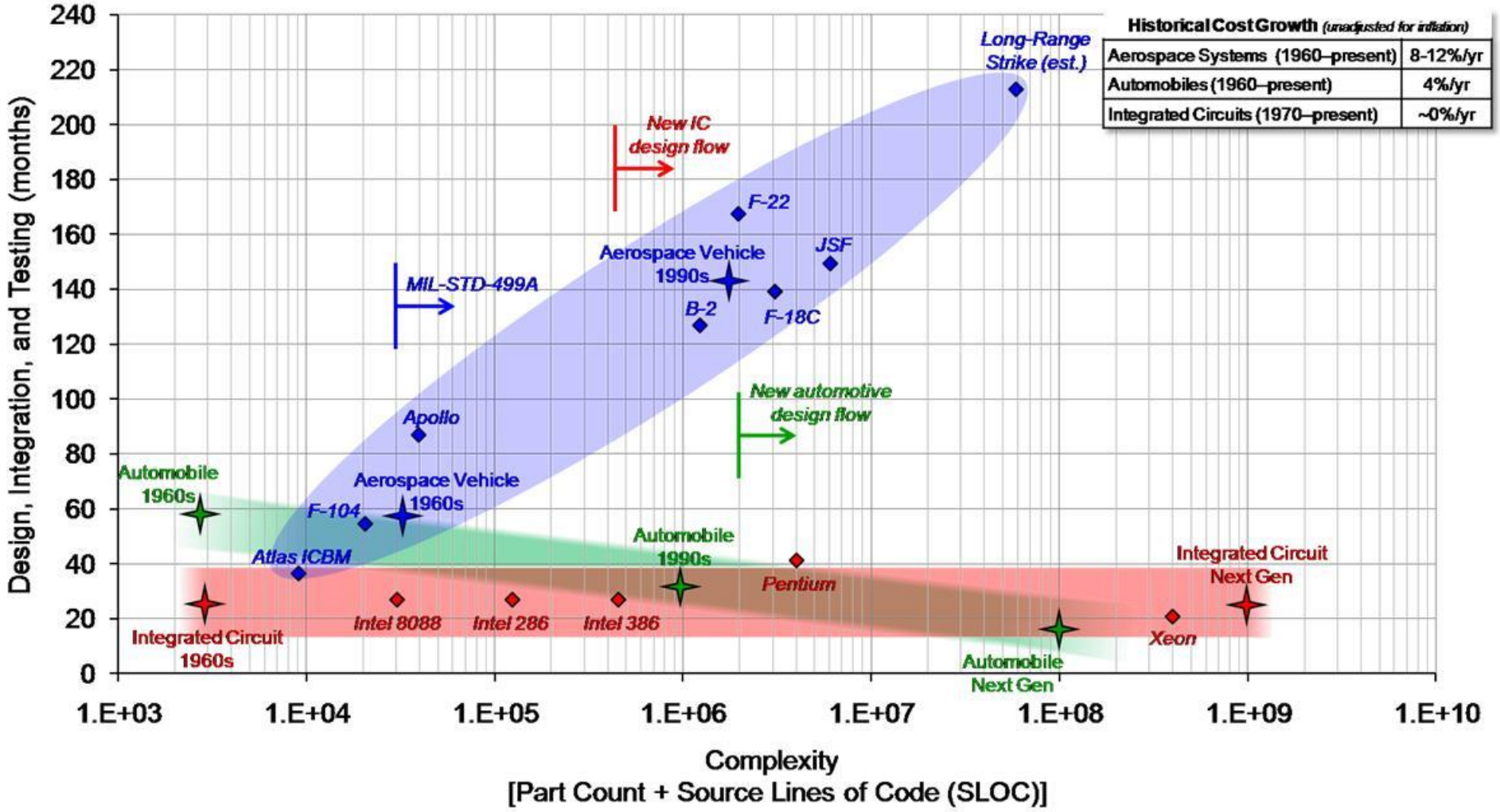
Data compiled by Mark Nowack, DARPA/TTO

Software complexity



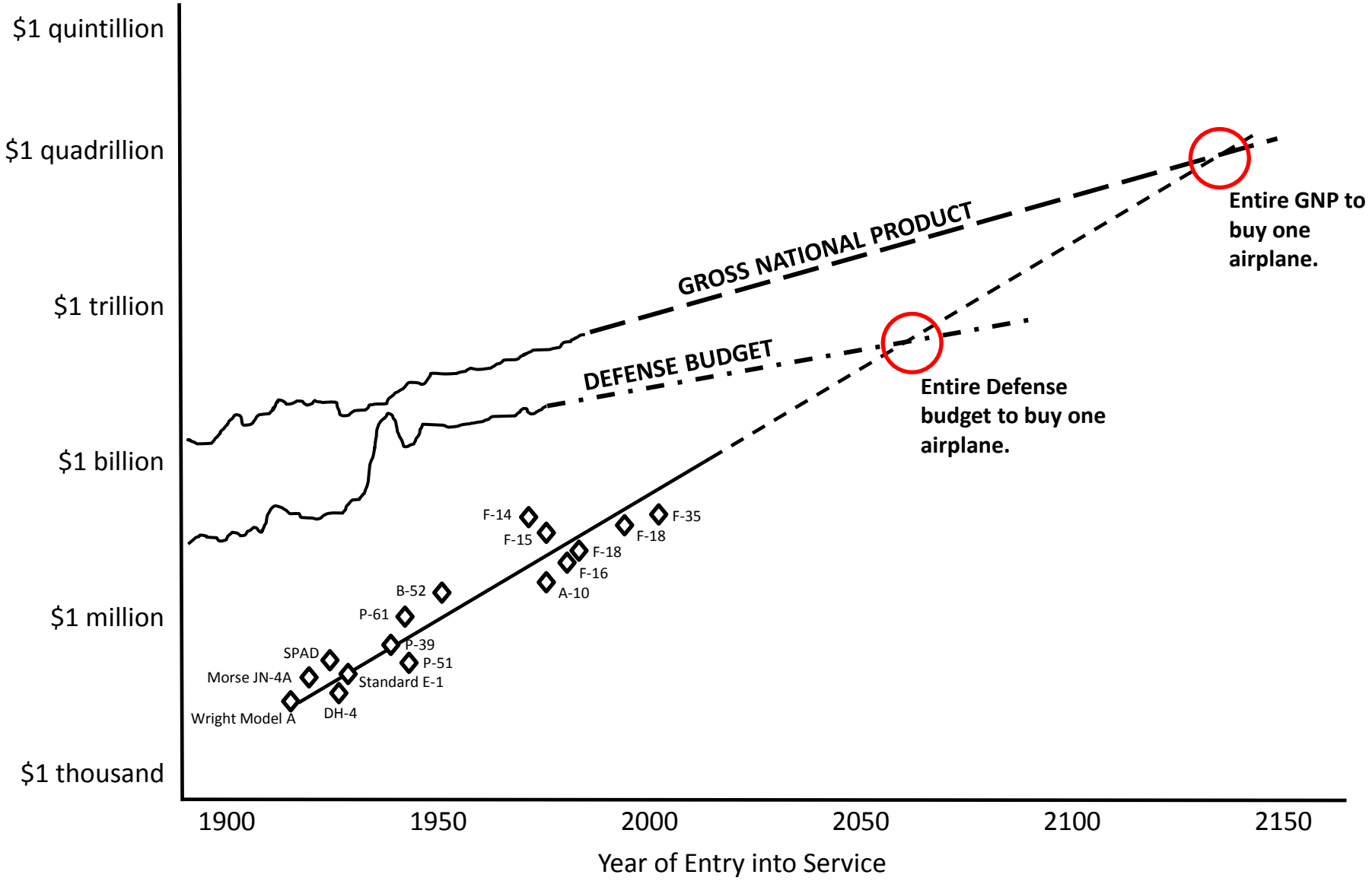
Dvorak, D. ed, NASA Study on Flight Software Complexity, Jet Propulsion Laboratory, California Institute of Technology, 5 March2009
Borden, D., Software Acquisition Process Improvement, NAVAIR, undated
Agle, D.C., Where Hunters Growl, Air & Space magazine, March 2011

Structural & software complexity



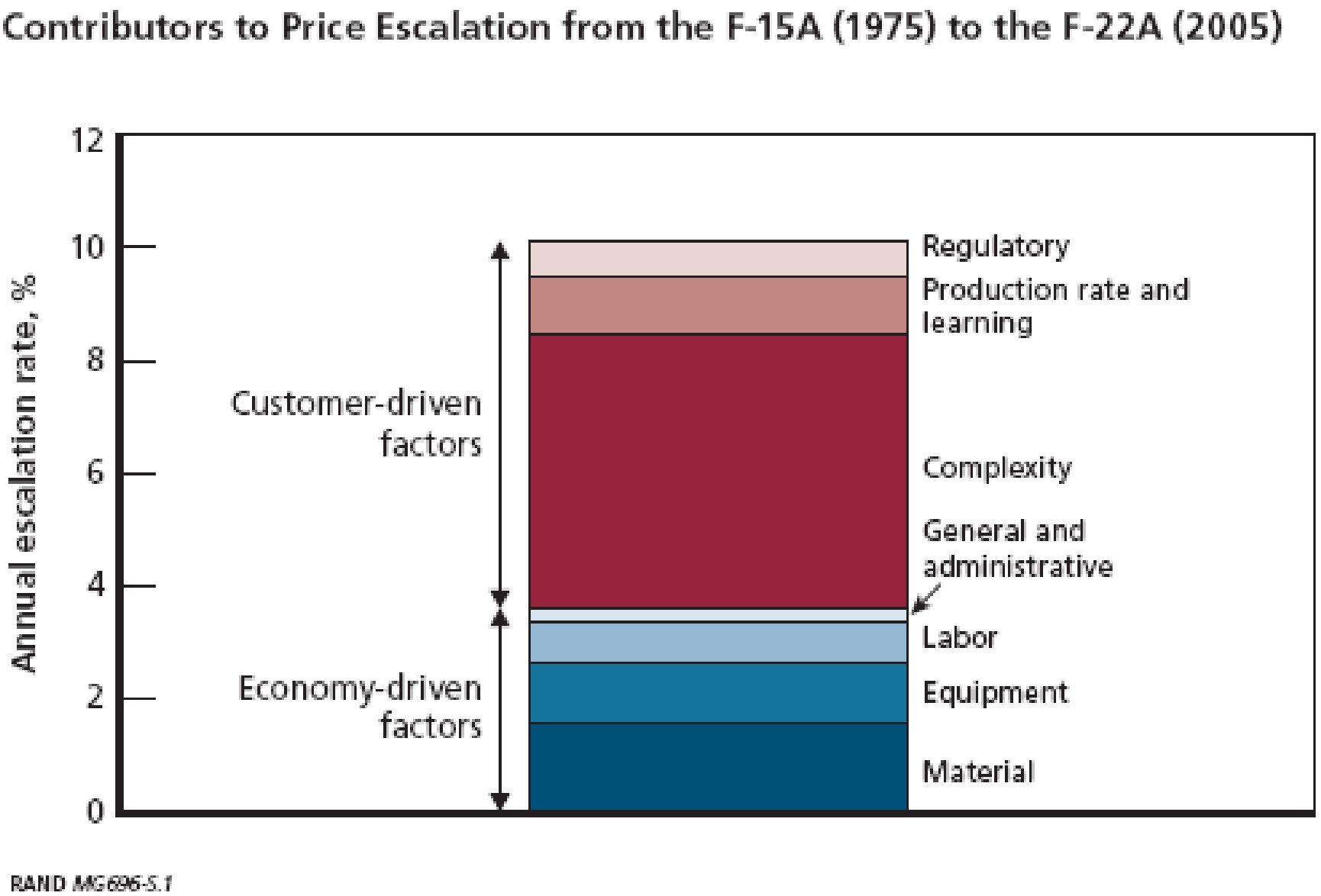
Data compiled by Mark Nowack, DARPA/TTO

Cost growth



Source: Norm Augustine, *Augustine's Laws*, 6th Edition, AIAA Press, 1997.

Evidence for a causal relationship with complexity



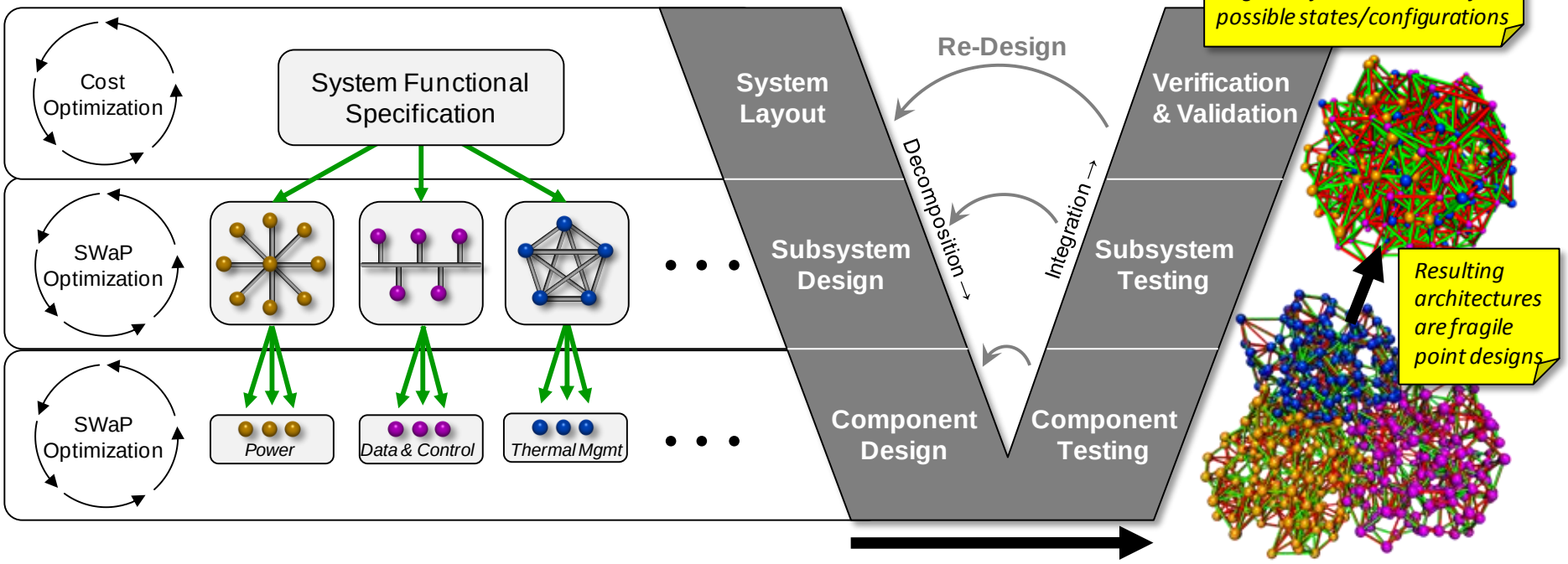
Modern systems engineering

MIL-STD-499A (1969) systems engineering process: as employed today

SWaP used as a proxy metric for cost, and dis-incentivizes abstraction in design

System decomposed based on arbitrary cleavage lines . . .

Conventional V&V techniques do not scale to highly complex or adaptable systems–with large or infinite numbers of possible states/configurations



Resulting architectures are fragile point designs

. . . and detailed design occurs within these functional stovepipes

Unmodeled and undesired interactions lead to emergent behaviors during integration

SWaP = Size, Weight, and Power
V&V = Verification & Validation

Desirable interactions (data, power, forces & torques)
Undesirable interactions (thermal, vibrations, EMI)

Tools have made it better…

Image courtesy of Dassault Systemes

Dassault Falcon 7X

Two-fold schedule compression for new business jets through faithful application of a digital master model with QA/QC feedback by tail number

Image courtesy of Lockheed Martin

Lockheed Martin F-35

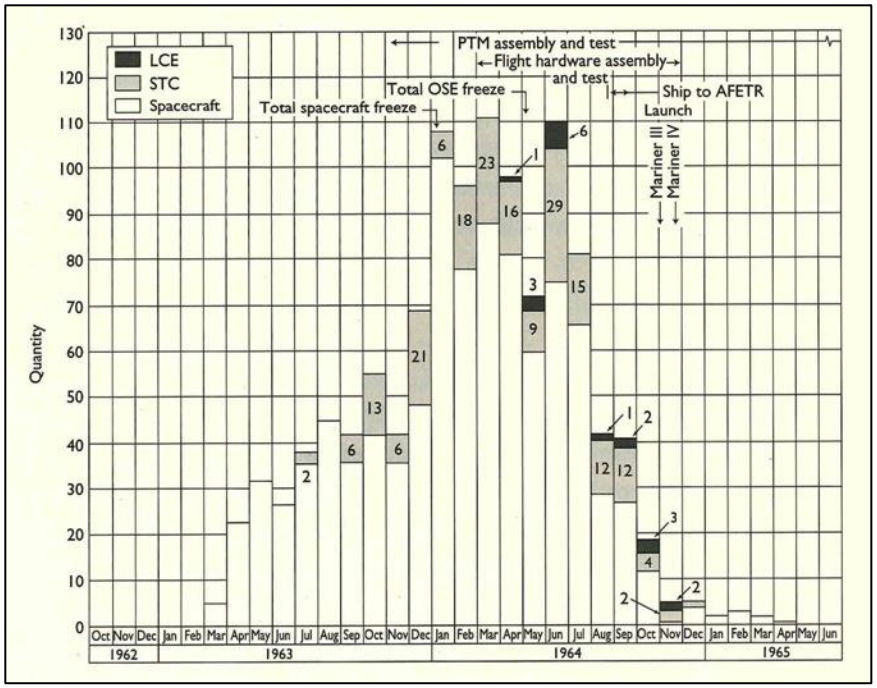
Shimming and 'drill and fill' approach significantly worsens production learning effects, leading to delays and cost growth*

** GAO-10-382: Joint Strike Fighter – Additional Costs and Delays Risk Not Meeting Warfighter Requirements on Time, Mar 2010*

… but the fundamental design flow hasn't changed!

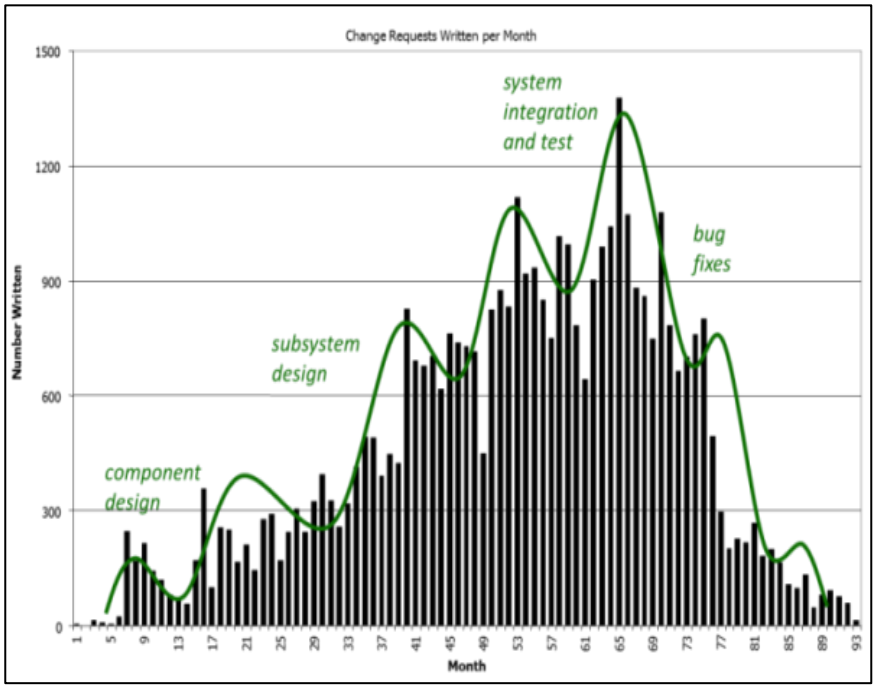
Engineering Change Requests (ECRs) per Month of Program Life

Mariner Spacecraft (1960s)



From Project Inception through Midcourse Maneuver, vol. 1 of *Mariner Mars 1964 Project Report: Mission and Spacecraft Development*, Technical Report No. 32-740, 1 March 1965, JPLA 8-28, p. 32, fig. 20.

Modern Cyber-Electromechanical System (2000s)

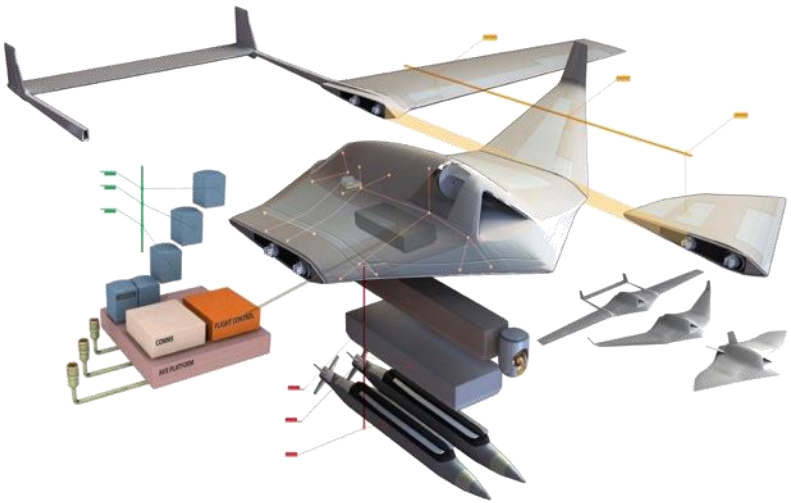


Giffin M., de Weck O., et al., *Change Propagation Analysis in Complex Technical Systems*, J. Mech. Design, 131 (8), Aug. 2009.

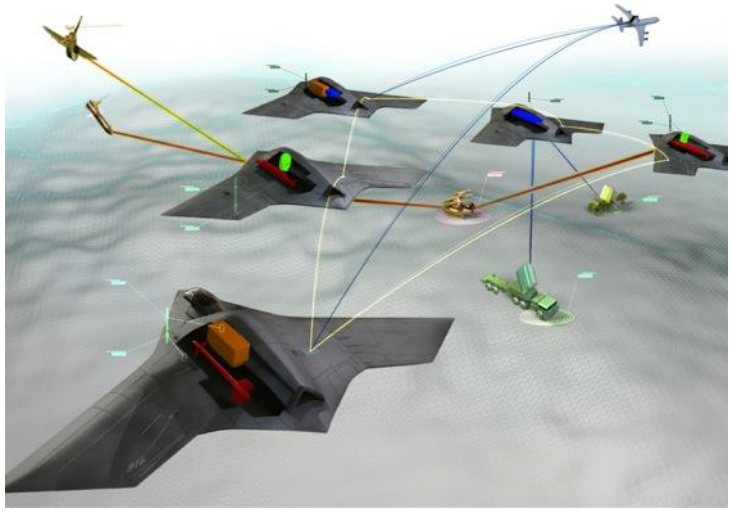
Adaptive Vehicle Make

Approaches for tackling complexity

Simplify



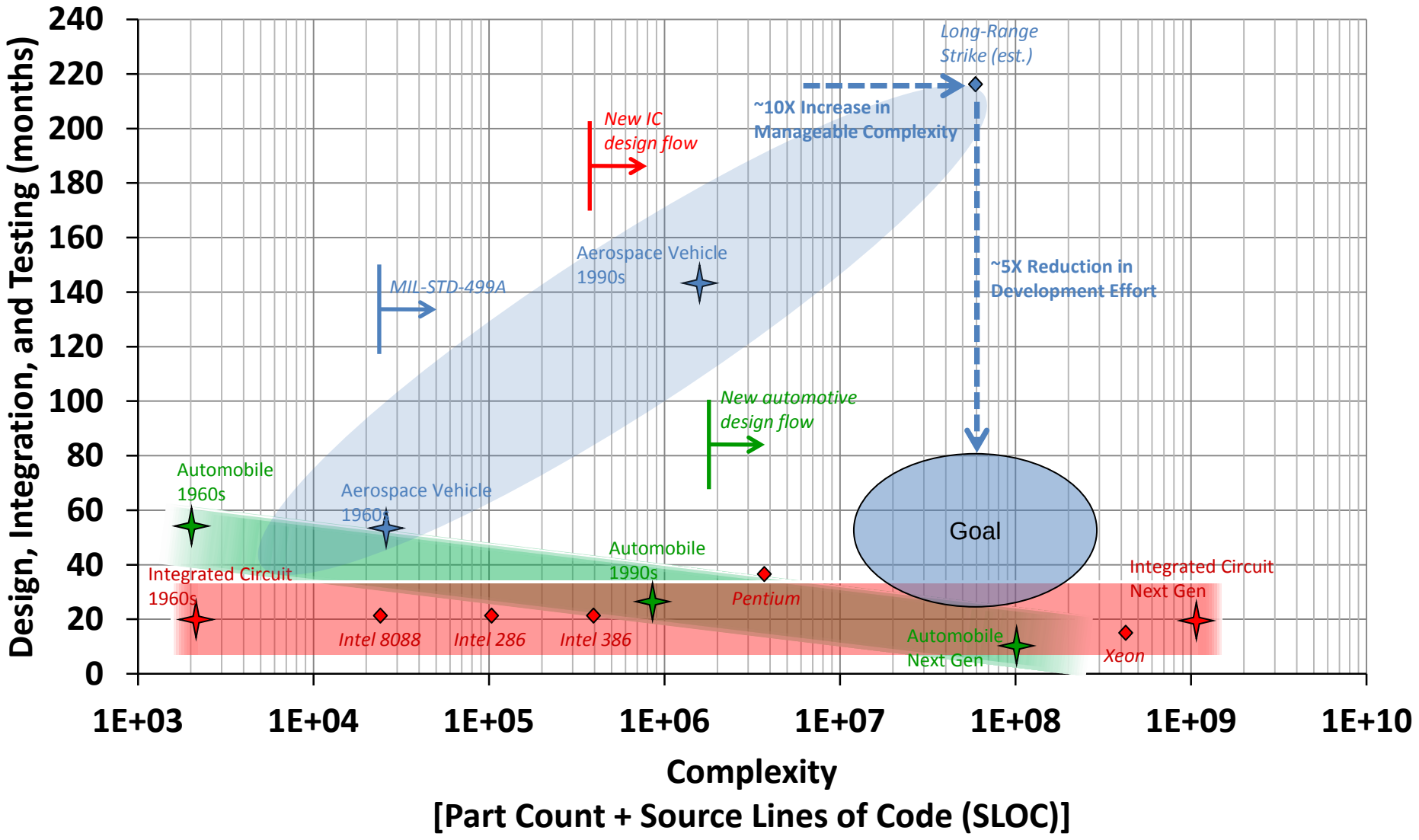
Modularize



Disaggregate

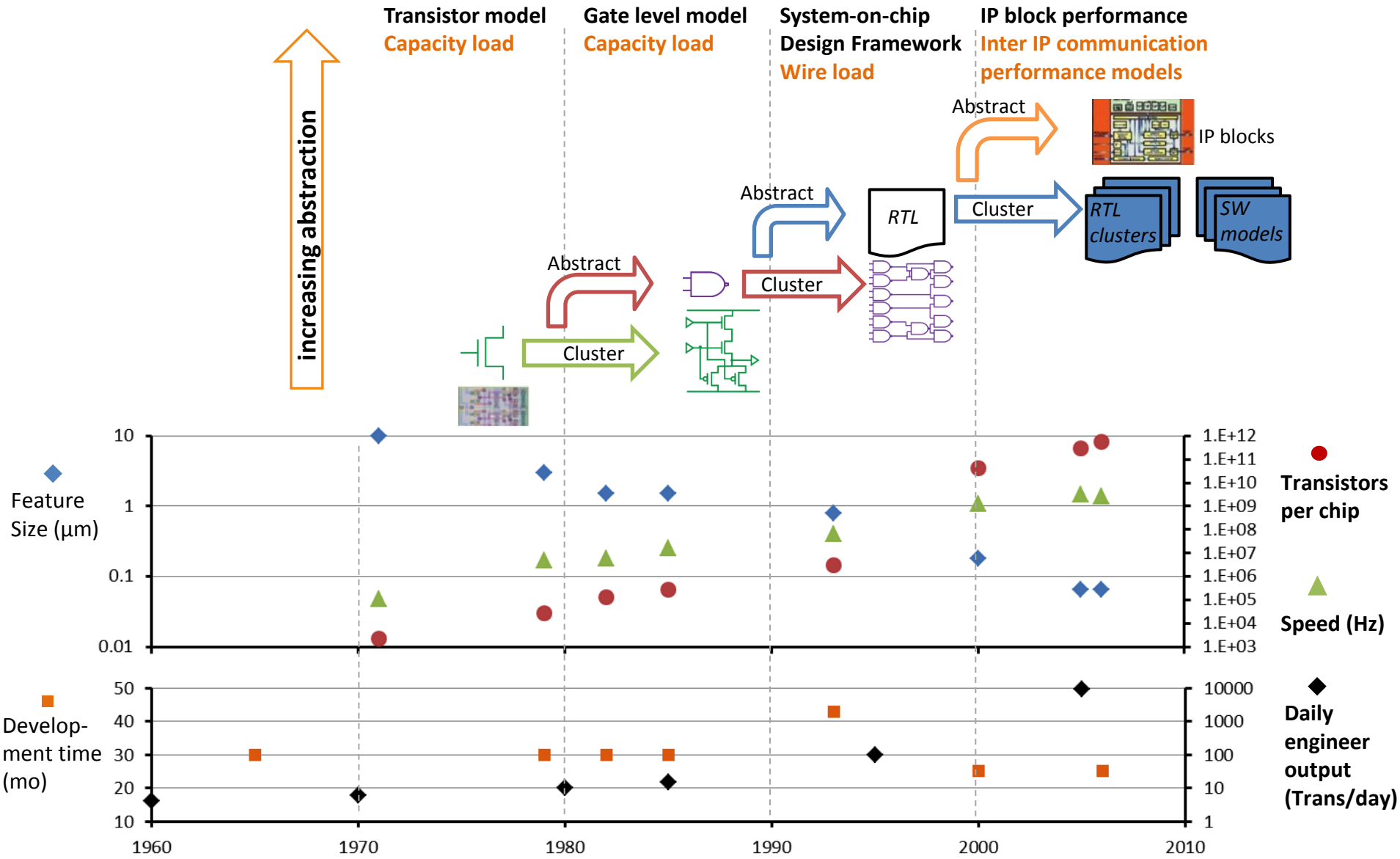
???

DARPA goals for AVM



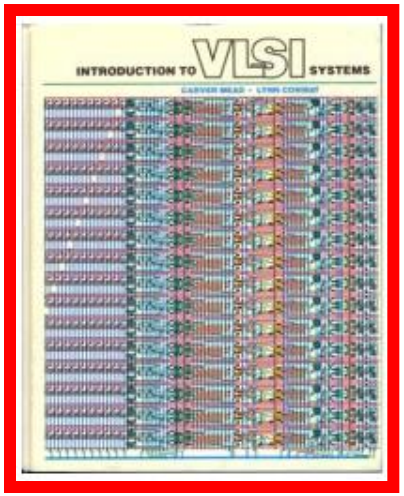
Data compiled by Mark Nowack, DARPA/TTO

Existence proof—VLSI design



Sources: Singh R., *Trends in VLSI Design: Methodologies and CAD Tools*, CEERI, Intel, *The Evolution of a Revolution*, and Sangiovanni-Vinventelli, A., *Managing Complexity in IC Design*, 2009

Existence proof—foundry-style manufacturing



The result:
Moved from hundreds of chip designers using vertically-integrated, captive semiconductor facilities to tens of thousands of designers using pure-play semiconductor foundries to create thousands of products.

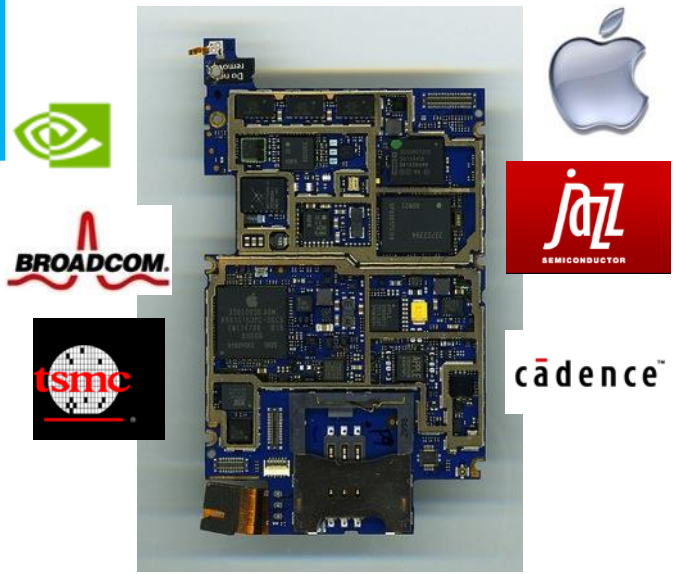
An approach to VLSI chip design that separates design from manufacturing (Mead & Conway, 1979).

Design implementation:
Use of simplified device & component models that trade some performance for automation of design.

Design rules that are independent of and scalable with process technologies.

Semiconductor manufacturing facility becomes the semiconductor foundry.

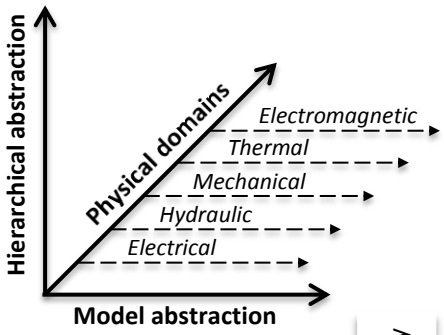
Semiconductor product implementation:
Chip prototypes are manufactured in silicon foundries using the *same tools, fabrication processes and materials* used for high-volume chip manufacturing… no seams.



Continues to enable, cost-effective custom VLSI products: Generating new markets & new companies including Apple, Silicon Graphics, Cadence, Jazz, TSMC, Broadcom, Nvidia and Qualcomm.

The META-iFAB Integrated Tool Chain

Rev. 10/18/2011



Constraints from Higher Levels of Abstraction

Design Trade Space Visualization

Dynamic Visualization

Structural & Entropy-Based Complexity Metrics Calculation

Domain-Specific Modeling Languages

Semantic Integration

Component Model Library

Design Space Construction(Static Models)

Qualitative/ Relational Models

Lumped Parameter (ODE) Models

Nonlinear Differential Equation (PDE) Models

Static Constraint Solver

Reachability Analysis

Controller/ FDIR Synthesis

CAD Geometry/ Grid Synthesis

Multi-Attribute Preference Surfaces

User Req'ment Synthesis

Context Model Library

Probabilistic Model Checker

Monte Carlo Dynamic Sim

FEA

CFD

BOM

PLM

Manufacturability Constraints

Requirements Verification

Probabilistic Certificate of Correctness

Design Update Feedback

Visualization

Metrics

Foundry Trade Space Construct.

Ass'y Selection

Machine Selection

Process Mapping

QA/QC

Foundry Design

Machine/Ass'y Mod Lib

Process Model Library

Instruction Sets

CNC Generator

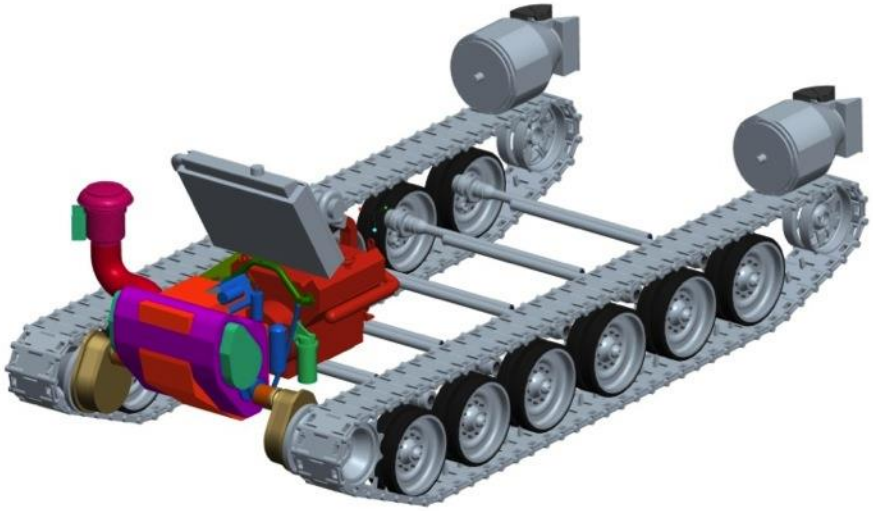
Source: Paul Eremenko, DARPA/TTO

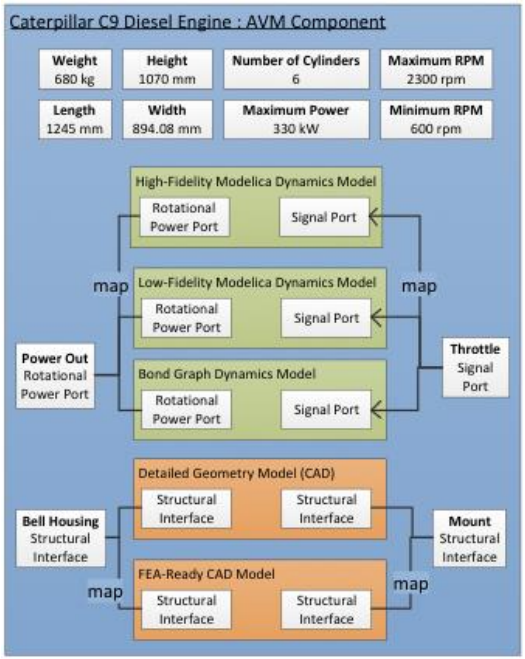
Formal Model-Based Design

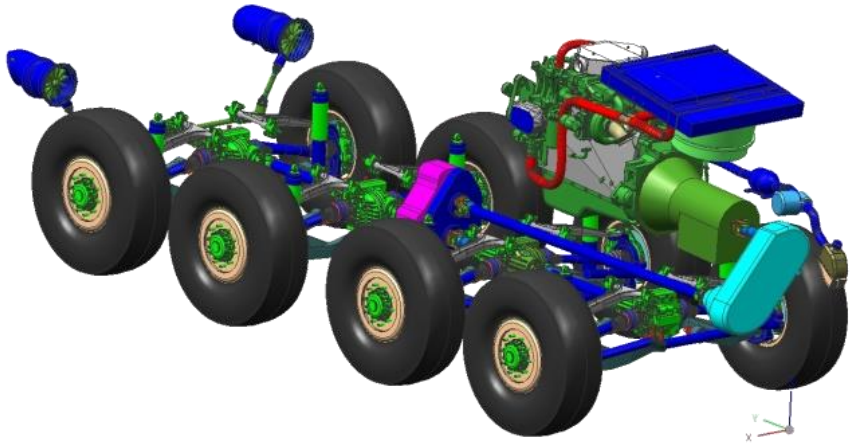
Component models

As of today:

- 131 component classes
- 469 component instances
- 43 parametric components
- 112 ITAR protected models
- 357 non-ITAR protected models



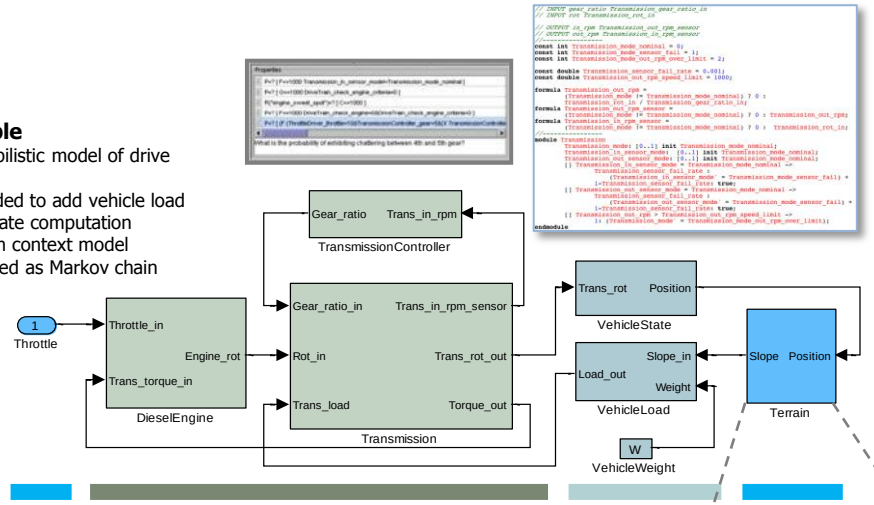




Source: Ricardo plc

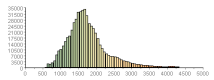
Context models

Example
- Probabilistic model of drive train
- Extended to add vehicle load and state computation
- Terrain context model specified as Markov chain



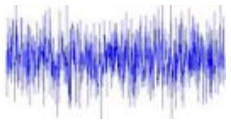
Probabilistic Context Model
- Generate discrete time Markov chain (DTMC) models of terrain from digital elevation data

DTED elevation data

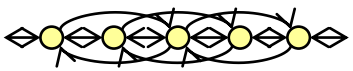


Specify terrain resolution for model and generate histogram (simple)

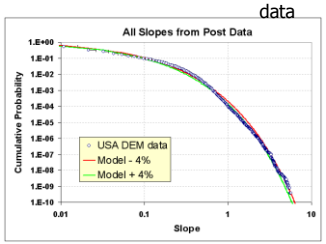
```
formula slope =
  s = 0 ? down :
  s = 1 ? level :
  s = 2 ? up : 1;
module terrain
  s : [0..2] init 1;
  [] s=0 -> 0.8 : (s'=0) + 0.2 : (s'=1) + 0.0 : (s'=2) ;
  [] s=1 -> 0.1 : (s'=0) + 0.8 : (s'=1) + 0.1 : (s'=2) ;
  [] s=2 -> 0.0 : (s'=0) + 0.2 : (s'=1) + 0.8 : (s'=2) ;
endmodule
```



Compute autocorrelation matrix for terrain data to incorporate relationship between adjacent locations (more realistic)



Markov chain representation of terrain for probabilistic model checking
Customized for required horizontal and vertical resolution



Context Descriptions	Available for Test Bench
Land Environment	
Surface Characteristics (for Depth of Interest)	
Concrete	X
Paved	X
Dirt	X
Sand	X
Wet	X
Mud	X
Snow	
Ice	
Discrete Obstacles (Forward and Reverse, and at Angles)	
Step Climb	X
Step Descend	X
Gap Crossing	X
V-Ditch	X
Half-Round	X
Curb	X
Features found in MOUT (Military Operations in Urban Terrain)	X
Jersey Barrier (Highway Divider)	X
Improvised Obstacles (e.g., passenger cars)	X
Terrains	
Terrains of varying roughness (Flat to 5" in rms)	X
Longitudinal Grades (Forward and Reverse)	X
Side-to-Side Slopes (Either side up-hill)	
Combined Grade and Slope (Fore-Aft and Side-to-Side)	
Curvature (Turns, Crown, Trough)	
Aquatic Environment	
Water Properties	
Density	X
Temperature	X
Viscosity	
Thermal Conductivity	
Specific Heat	
Water Body Features	
Depth	X
Calm	X
Surf	
Currents	
Sea-State	X
Contaminants	
Salt	X
Particulates (Sand, Volcanic Ash)	
Debris (Vegetation, Spills)	
Atmospheric Environment	
Air Properties	
Pressure	
Density	
Moisture	X
Temperature (Arctic, Cold, Normal, Hot)	X
Temperature (Locally Induced)	
Atmospheric Features	
Wind	X
Solar Radiation	X
Contaminants	
Corrosive Components (Salt spray, SO_2, NO_x)	
Particulates (Dust, Sand, Volcanic Ash, Rain, Snow, Ice Crystals)	
Electro Magnetic Interference (EMI)/ *Electro Magnetic Pulse (EMP)*	
Nuclear Biological Chemical (NBC)	

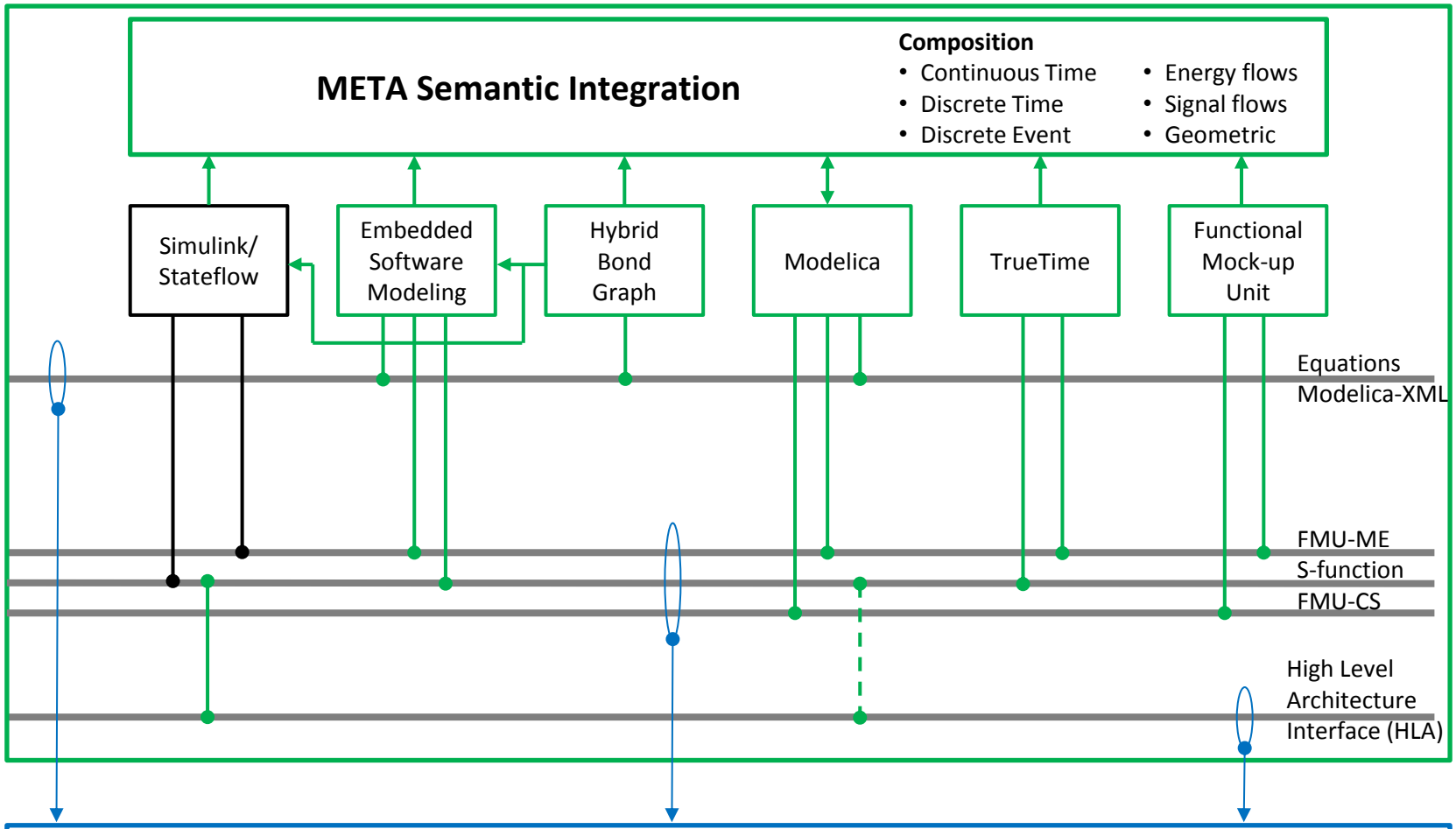
Modeled & Validated: 17/22
Delivered: 17/22

Modeled & Validated: 7/13
Delivered: 6/13

Modeled & Validated: 6/10
Delivered: 4/10

Source: BAE Systems Land & Armaments Division

Integration of formal semantics across domains



Formal Verification

- Qualitative reasoning
- Relational abstraction
- Model checking
- Bounded model checking

Stochastic Co-Simulation

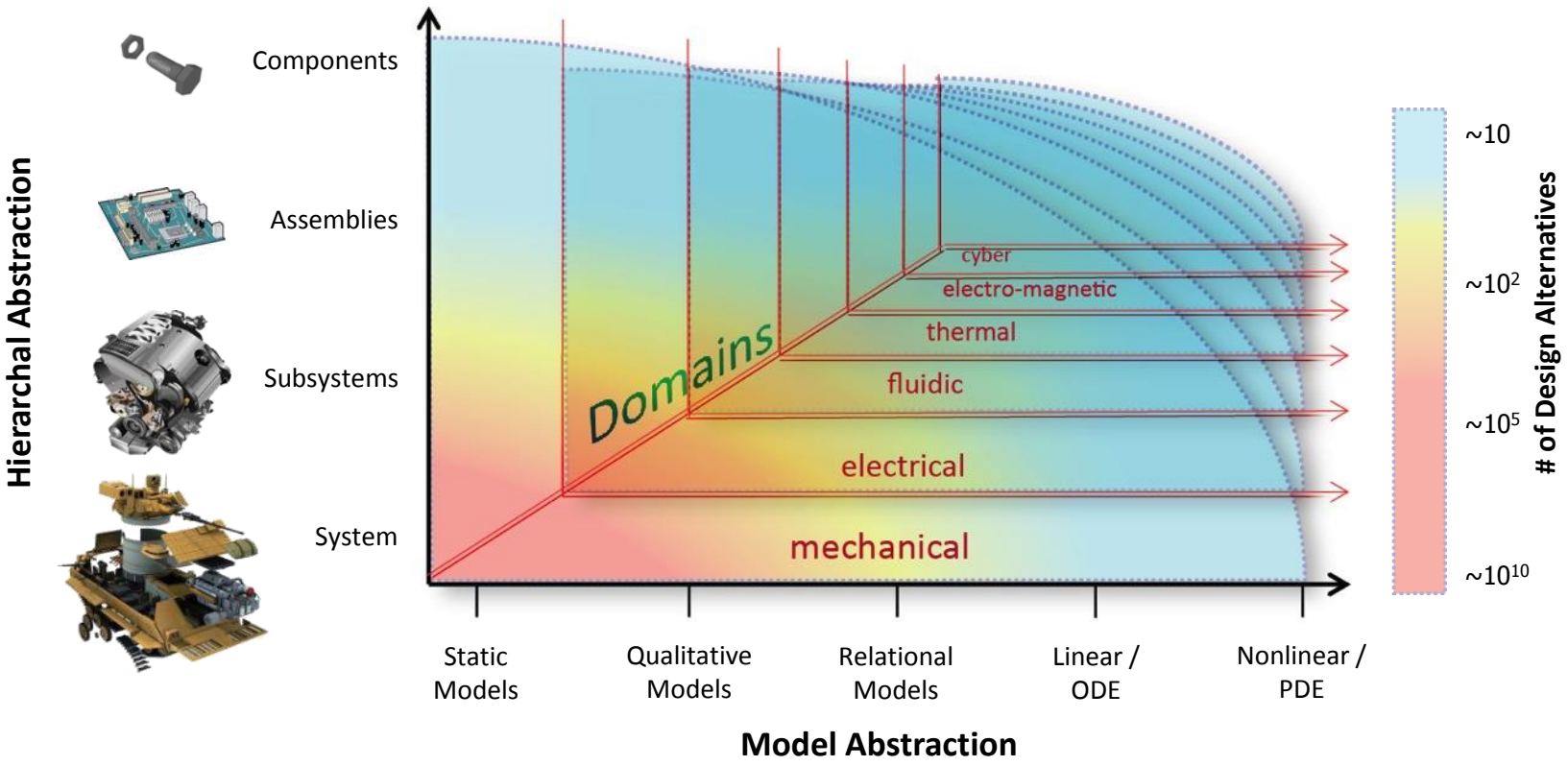
- Open Modelica
- Delta Theta
- Dymola

Distributed Simulation

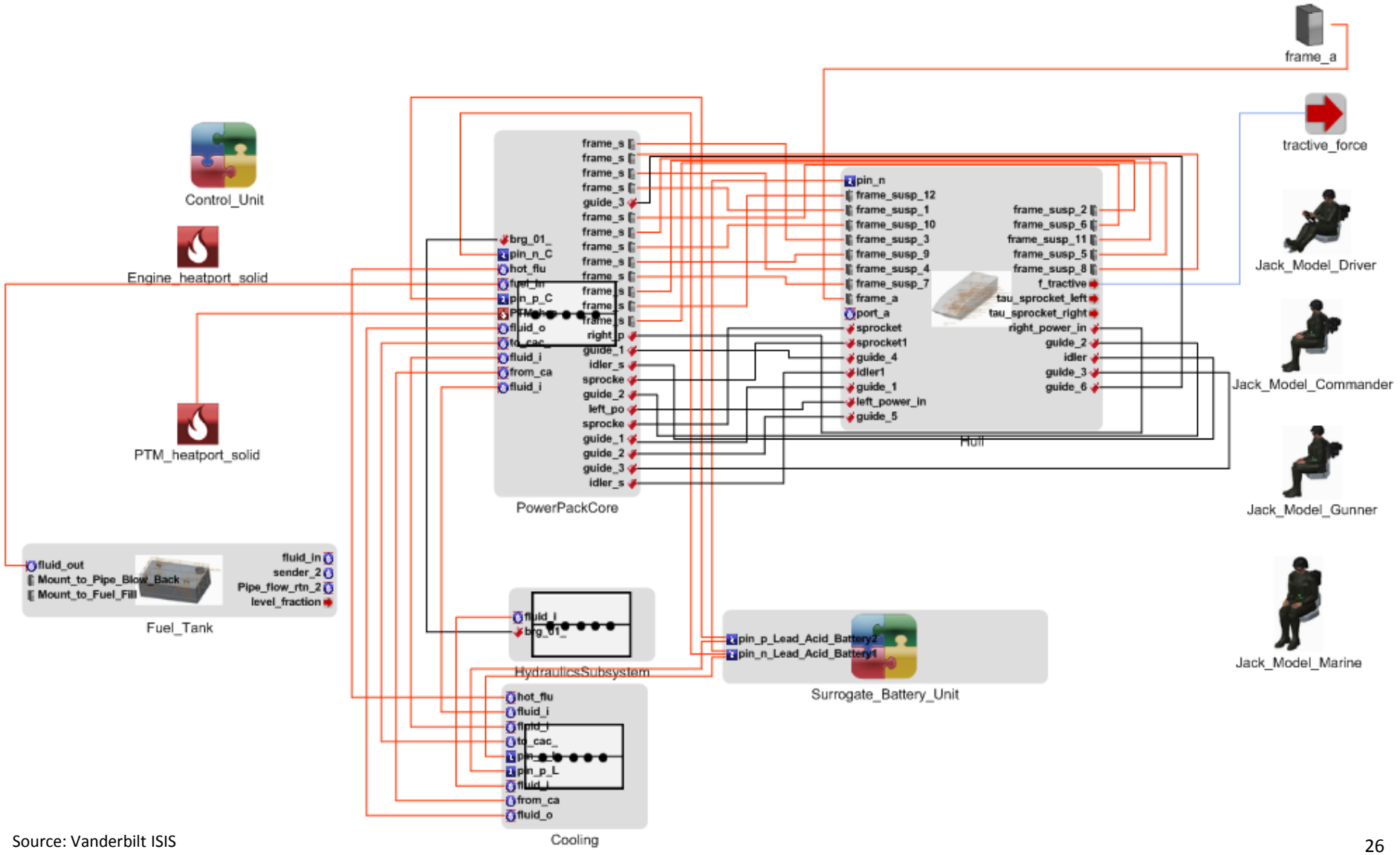
- NS3
- OMNET
- Delta-3D
- CPN

Source: Vanderbilt ISIS

Hierarchical and model abstraction

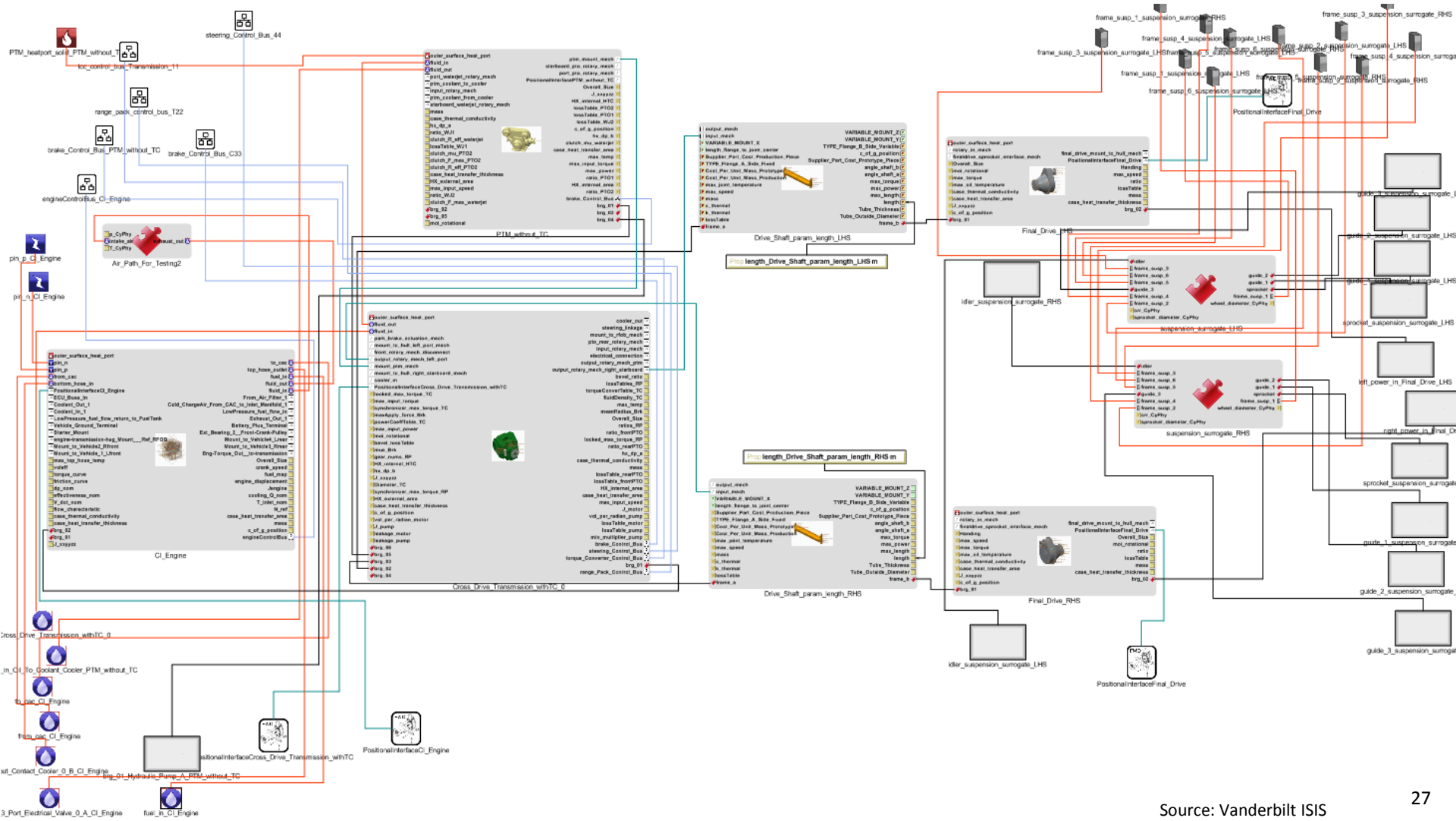


Hierarchical abstraction—assembly level



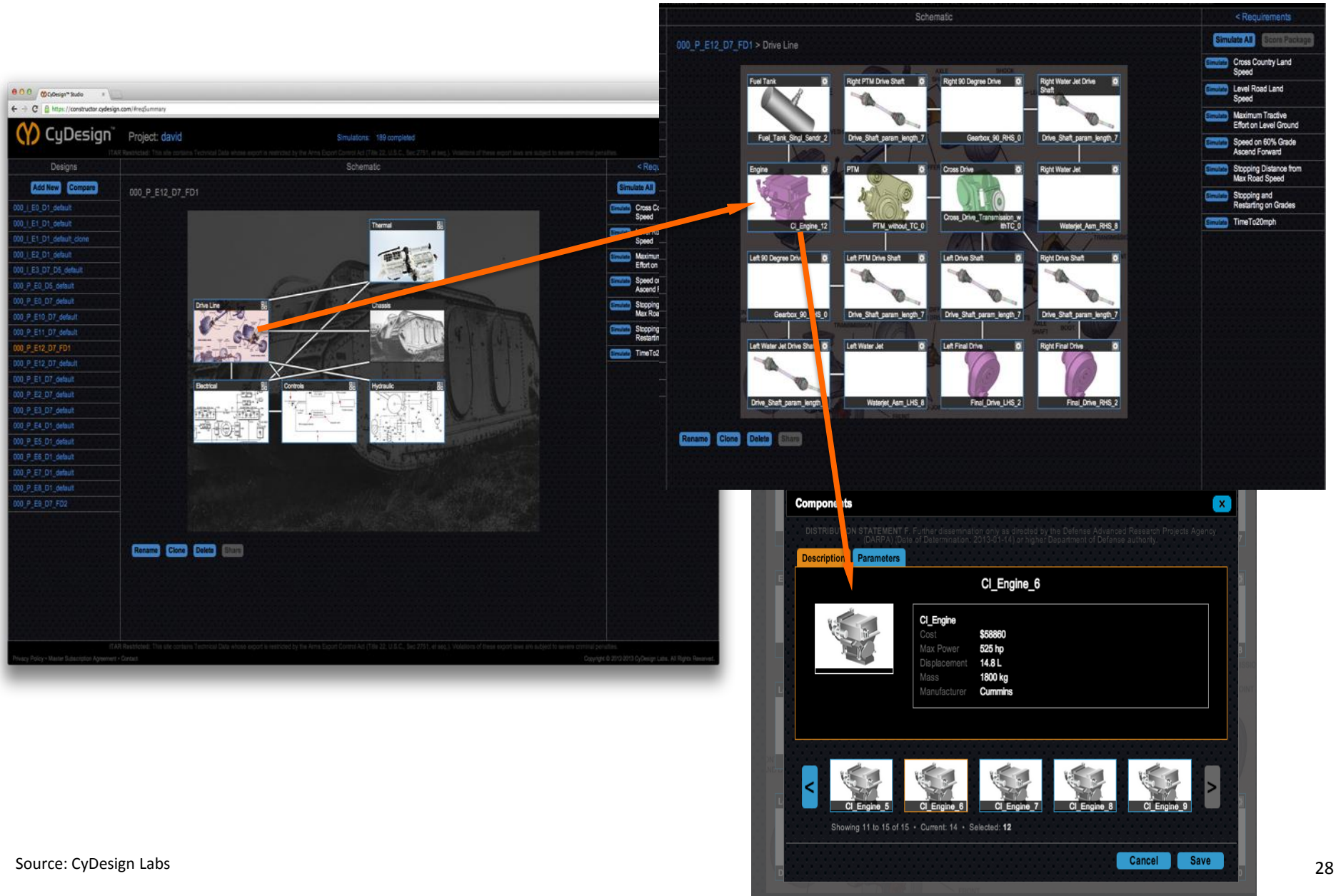
Source: Vanderbilt ISIS

Hierarchical abstraction—subassembly/component level



Source: Vanderbilt ISIS

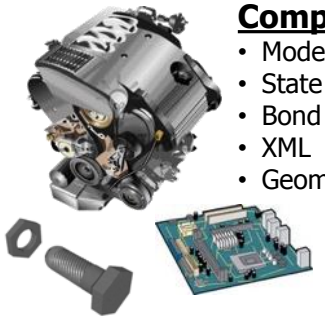
Cloud-hosted commercial tools instantiation



Source: CyDesign Labs

Model abstraction for verification

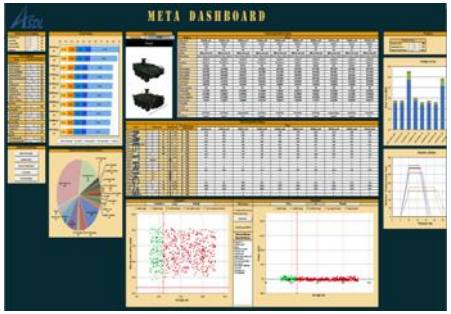
Component Models



- Modelica
- State Flow
- Bond Graphs
- XML
- Geometry

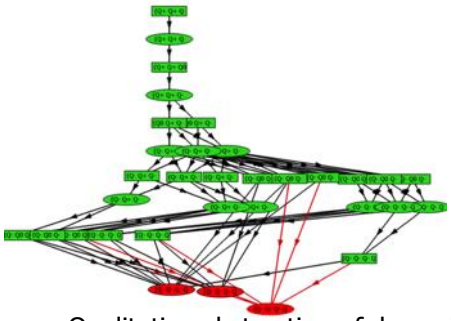
Semantic Integration

Static Trade Space Exploration



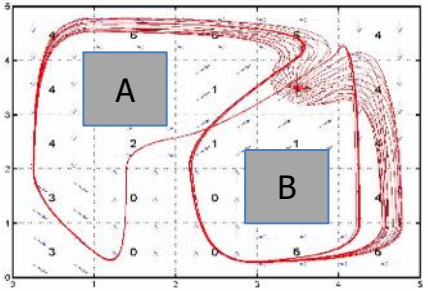
- Static constraint application
- Manufacturability constraints
- Structural complexity metrics
- Info entropy complexity metrics
- Identify Pareto-dominant designs
- 10^10 → 10^4 designs

Qualitative Reasoning



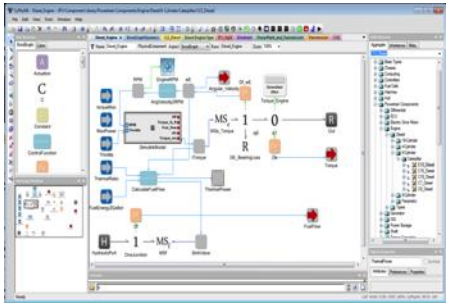
- Qualitative abstraction of dynamics
- Computationally inexpensive
- Quickly eliminate undesirable designs
- State space reachability analysis
- 10^4 → 10^3 designs

Relational Abstraction



- Relational abstraction of dynamics
- Discretization of continuous state space
- Enables formal model checking
- State-space reachability analysis
- 10^3 → 10^2 designs

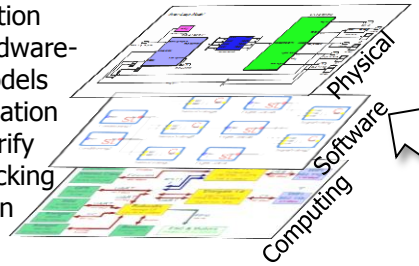
Linear Differential Equation Models



- Models are fully composable
- Simulation trace sampling to verify correctness probability
- Application of probabilistic model checking under investigation
- 10^2 → 10 designs

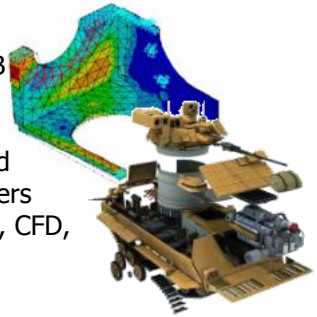
Embedded Software Synthesis

- Auto code generation
- Generation of hardware-specific timing models
- Monte Carlo simulation sampling to co-verify
- Hybrid model checking under investigation



CAD & Partial Differential Equation Models

- Generate composed CAD geometry for iFAB
- Generate structured & unstructured grids
- Provide constraints and input data to PDE solvers
- Couple to existing FEA, CFD, EMI, & blast codes
- 10 → 1 design



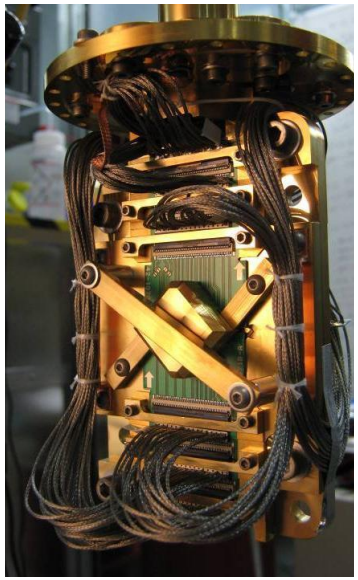
Sources: GATech; Xerox PARC; SRI; Vanderbilt ISIS

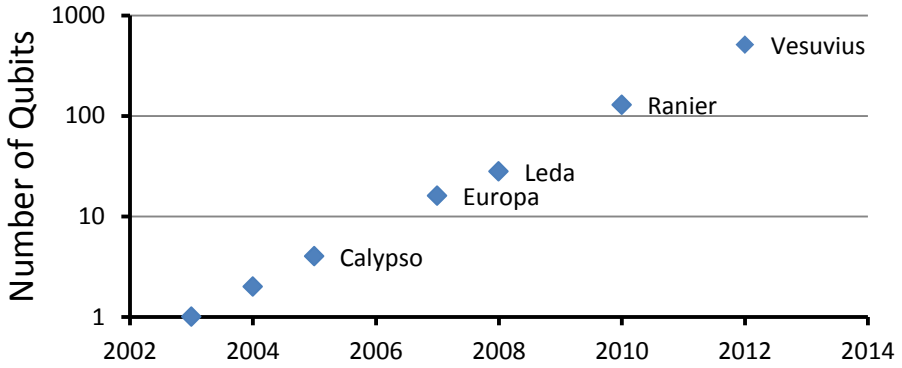
Verification on a adiabatic quantum computer

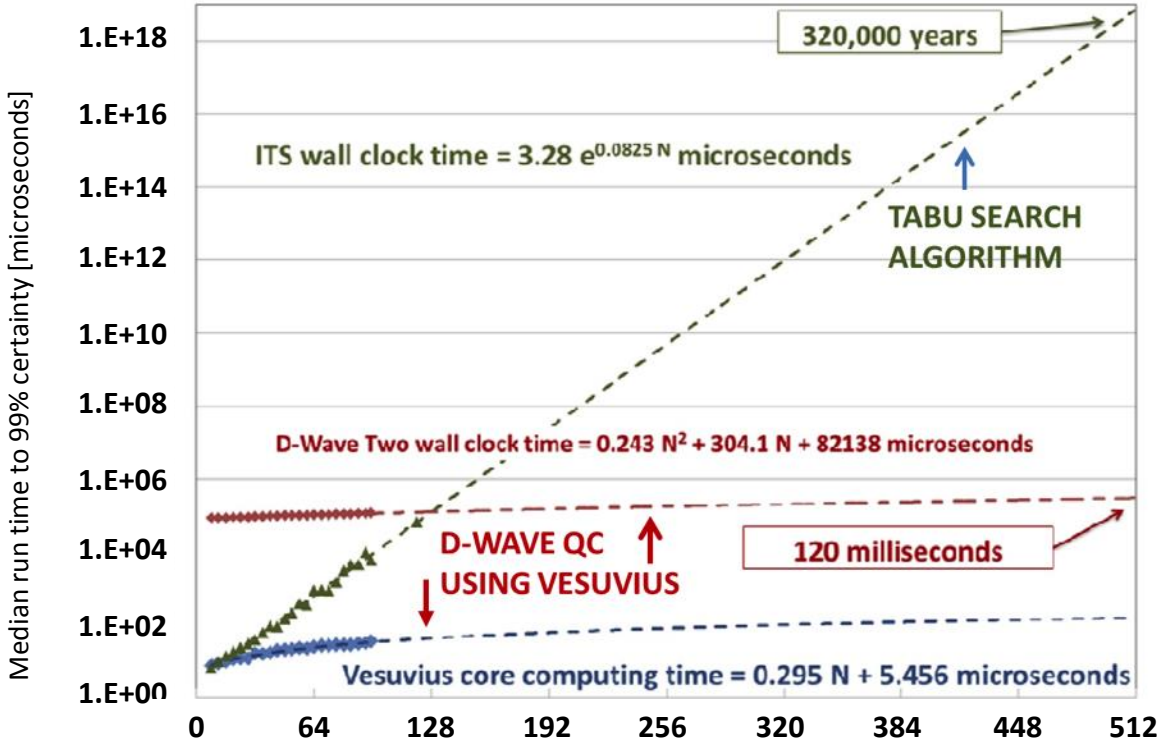
Vesuvius, 512 qubits

Leda, 28 qubits

Calypso, 4 qubits

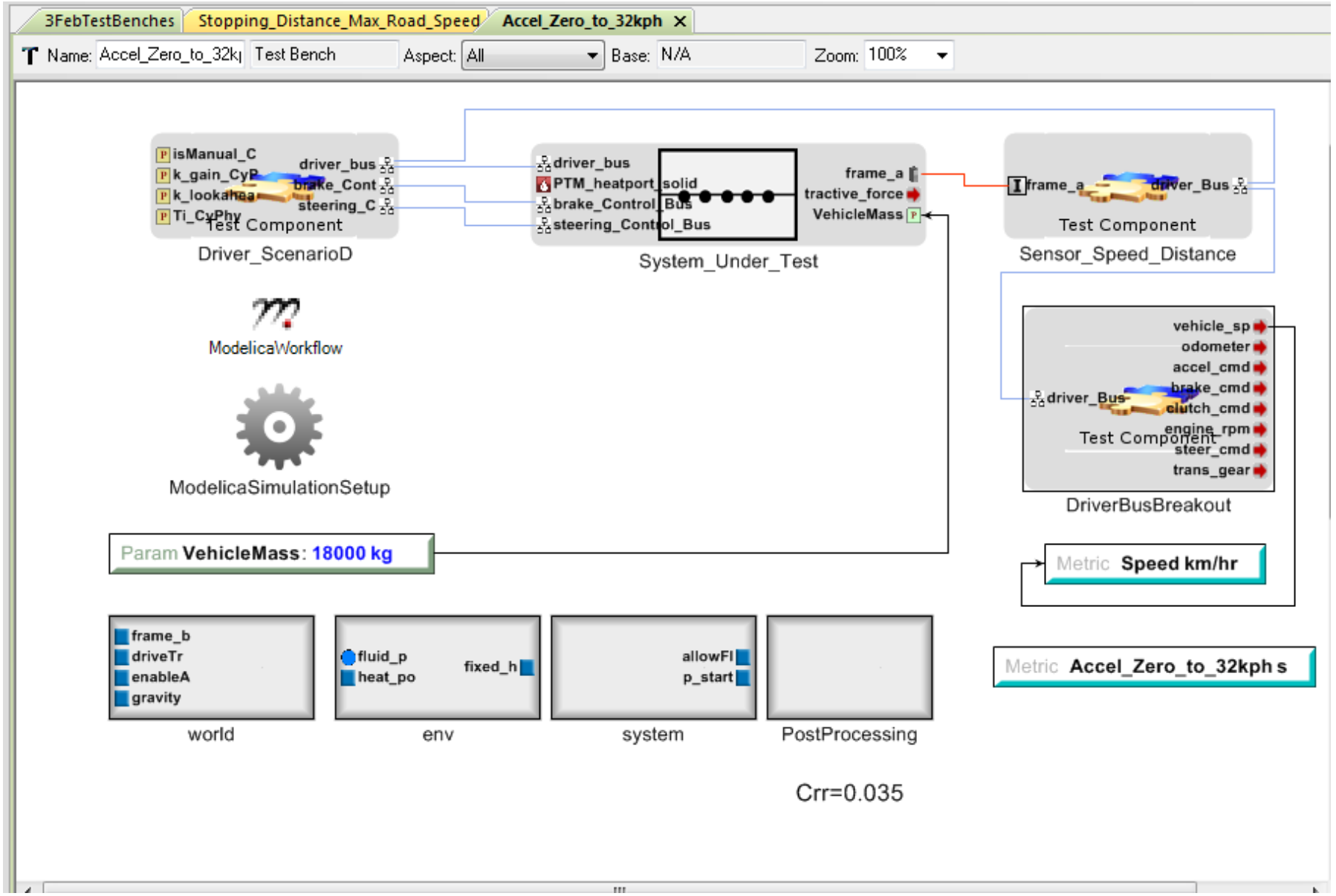






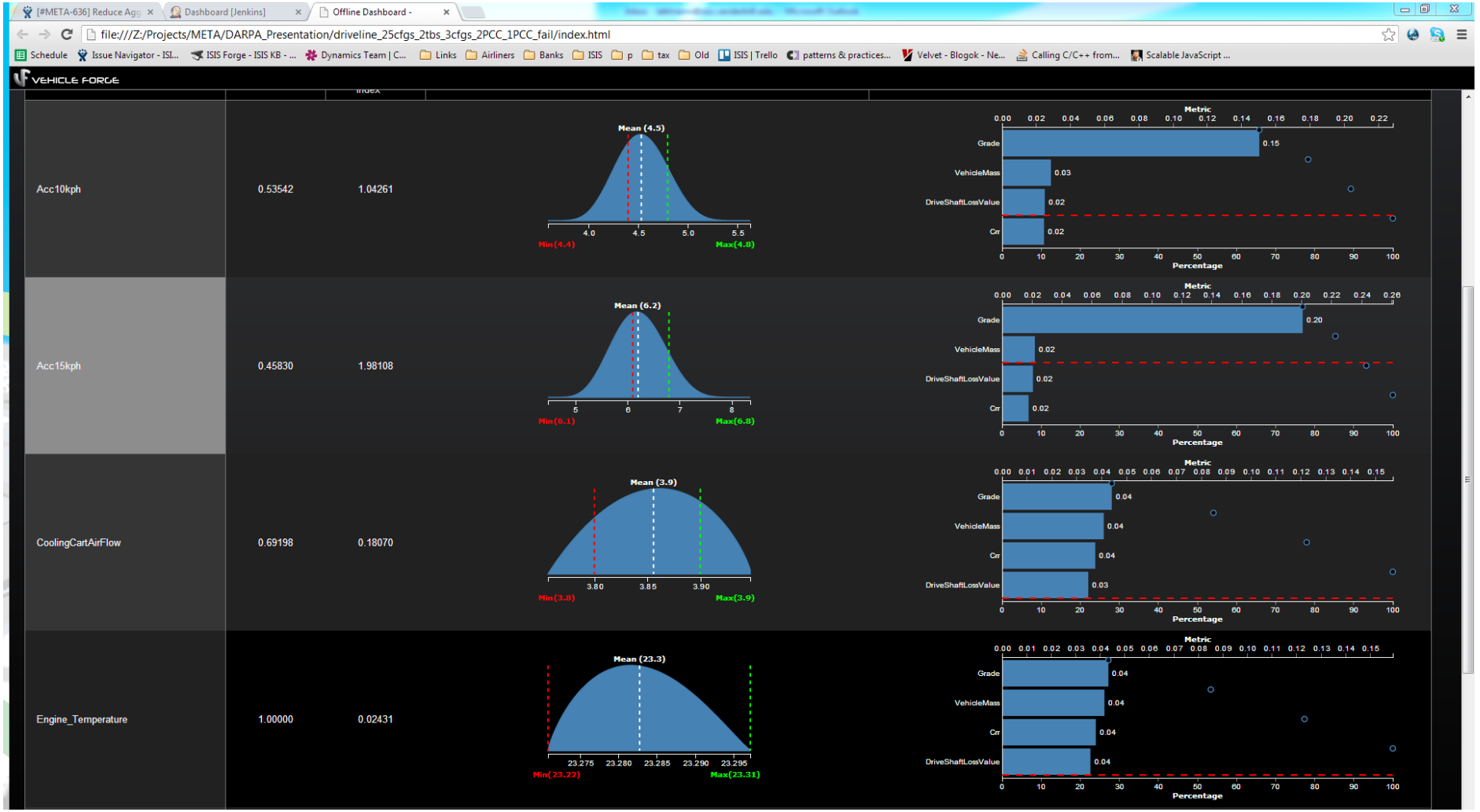
Source: USC/ISI

Probabilistic verification through simulation



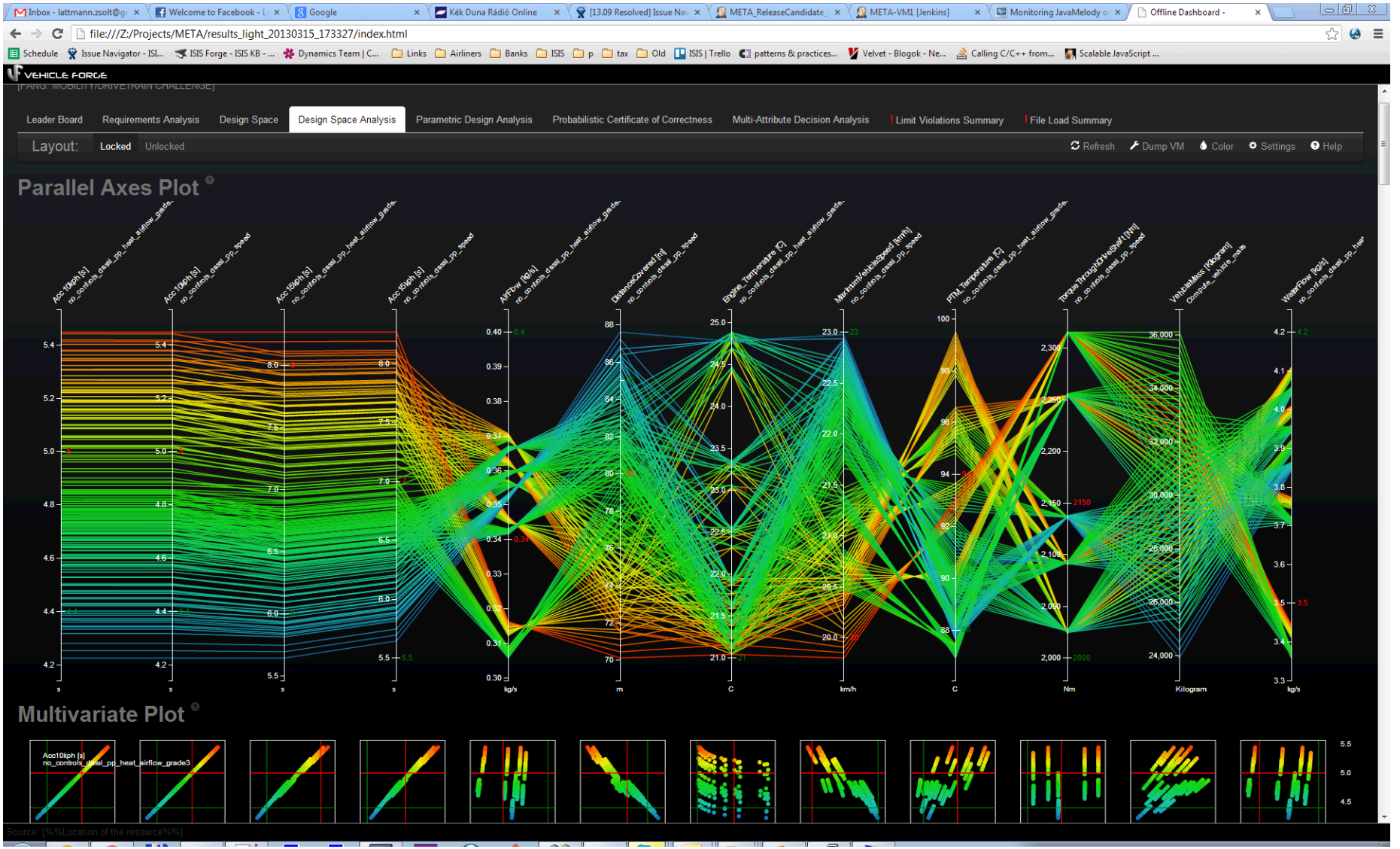
Source: Vanderbilt ISIS

Probabilistic certificates of correctness (PCCs)



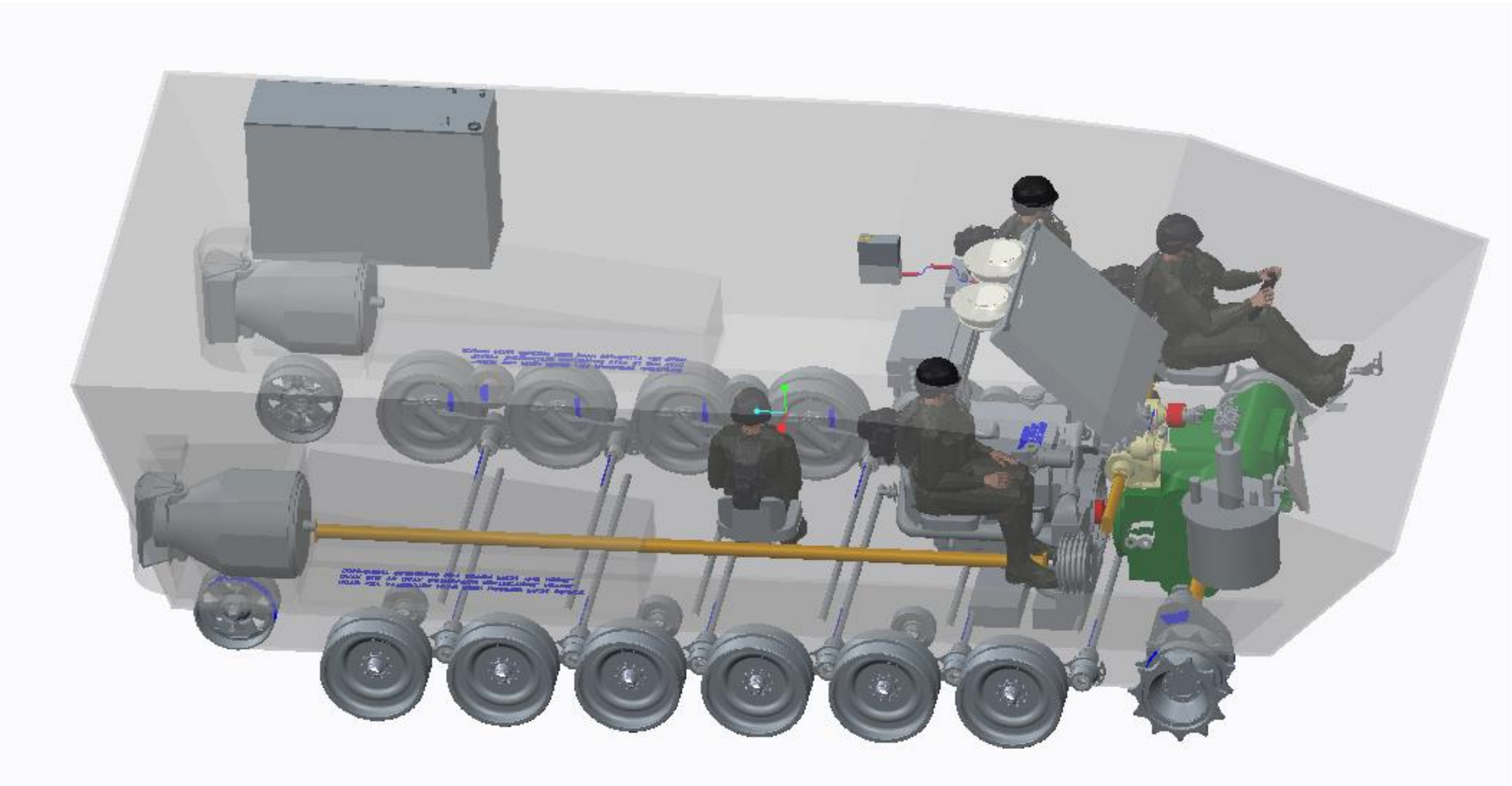
Source: Vanderbilt ISIS

Design space visualization



Source: Vanderbilt ISIS

Geometric composition for gridding/higher-order modeling



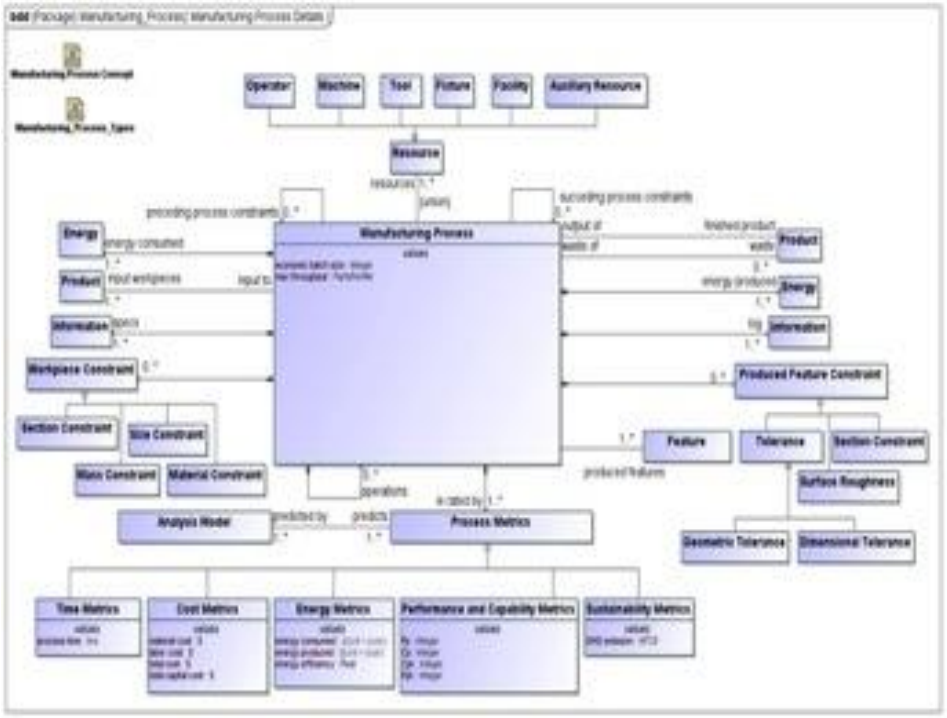
Source: Vanderbilt ISIS

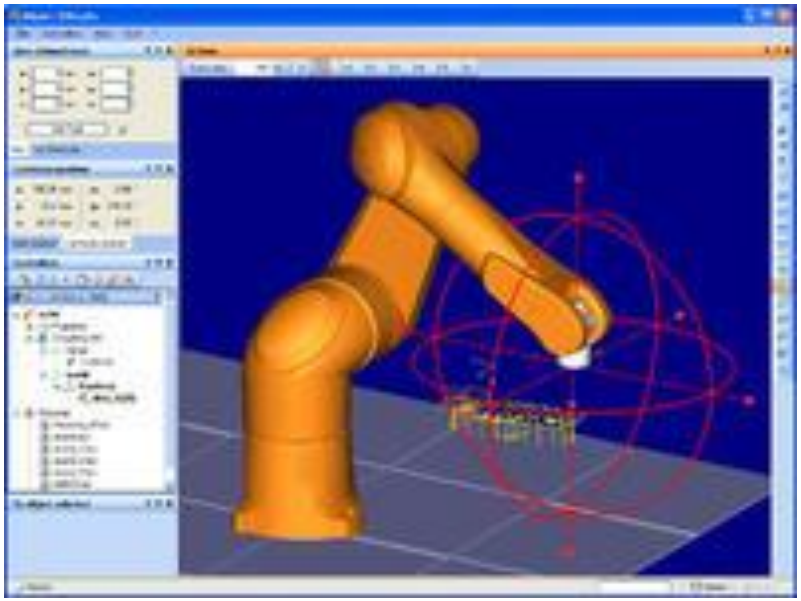
Model-Based Manufacturing

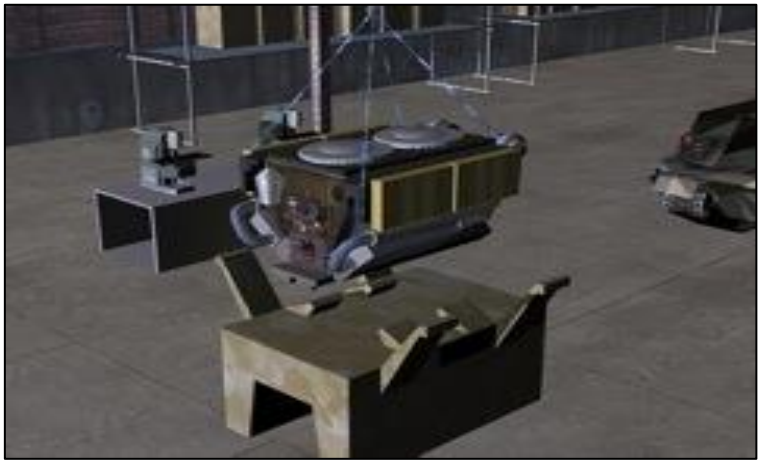
Manufacturing process models

As of today:

- 7 material shaping processes
- 19 general processes
- 231 machine instantiations
- 64 manual labor units
- 3,212 tools



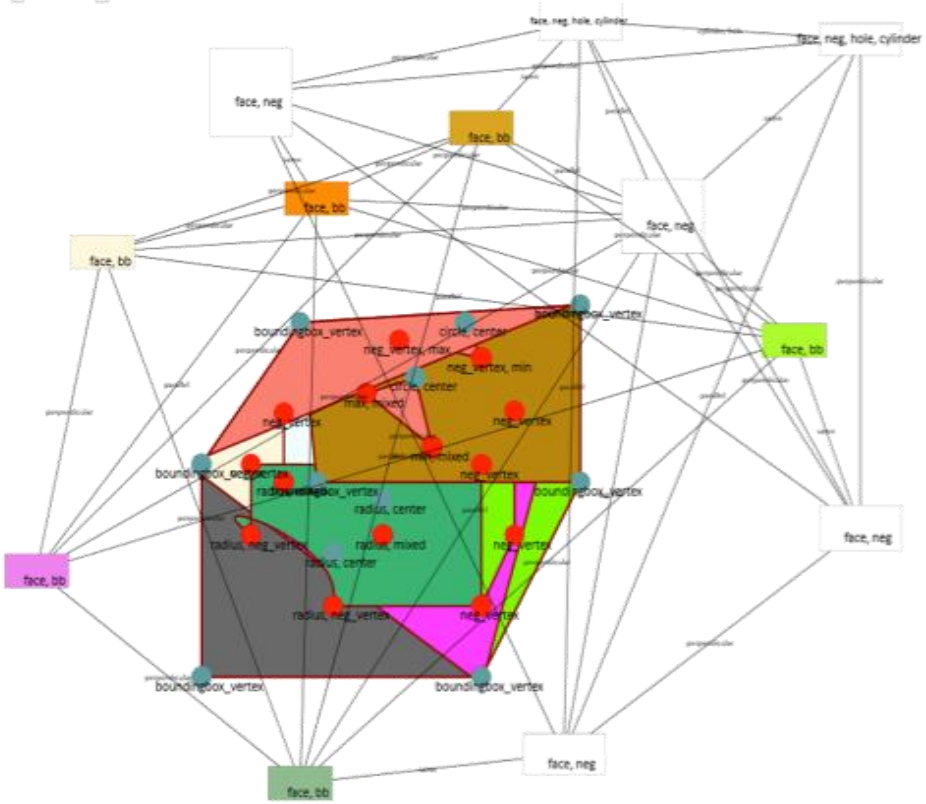




Sources: Penn State ARL; GM Research

Design decomposition

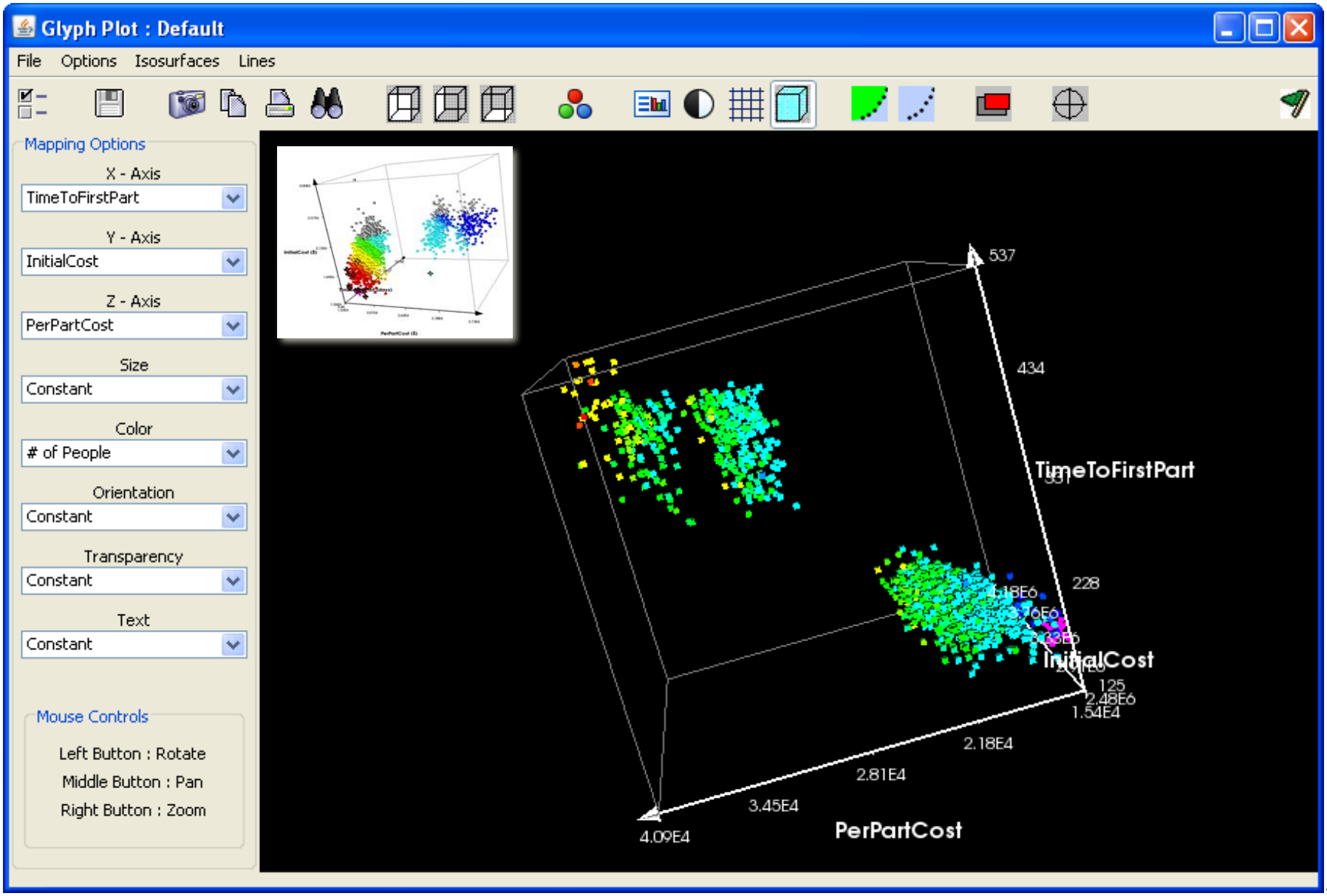
Topological Decomposition



"Reverse Composition"

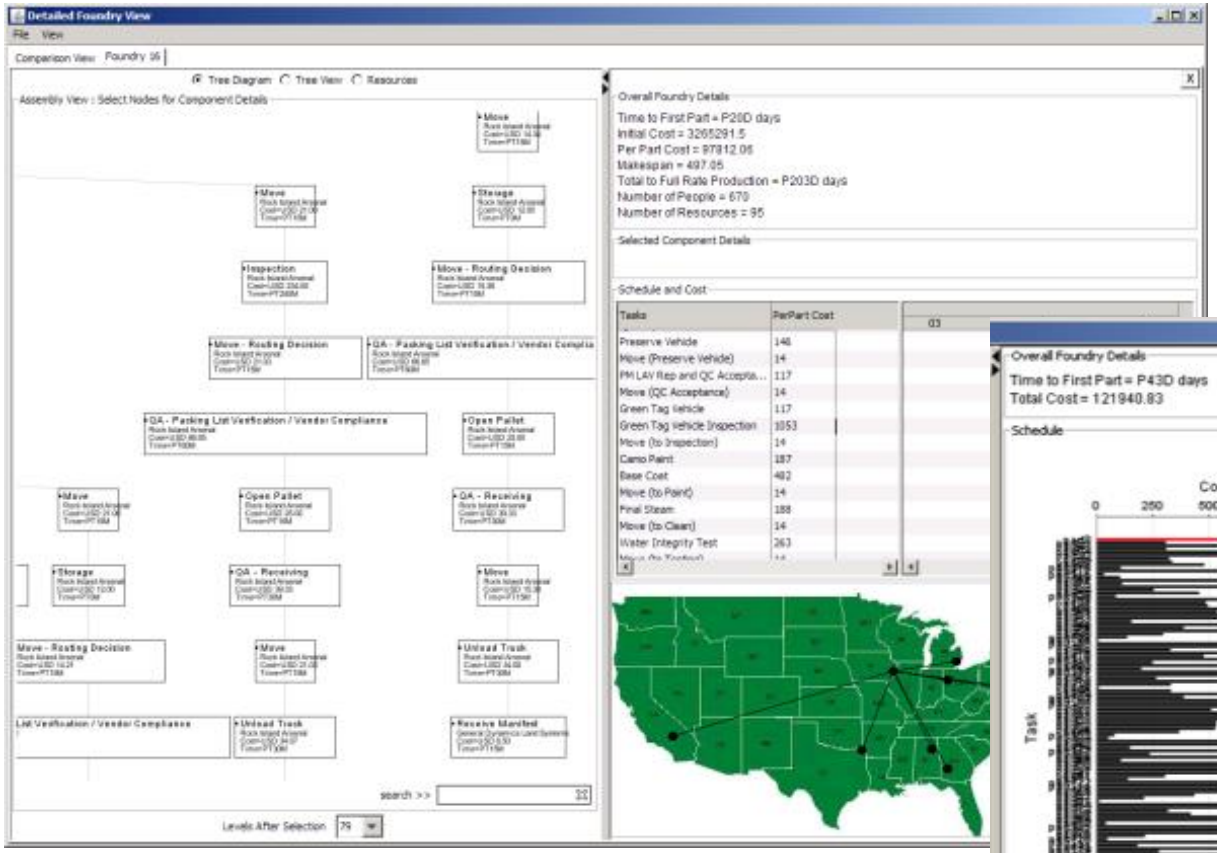
Source: Xerox PARC

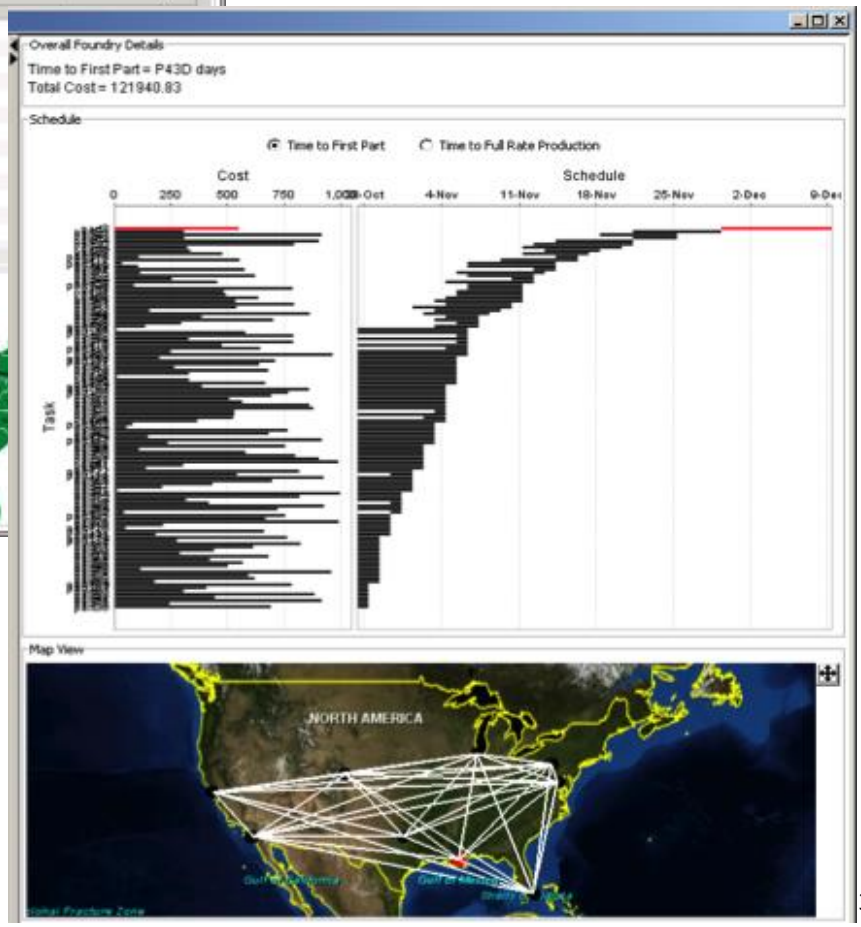
Foundry configuration tradespace exploration



Source: Penn State ARL

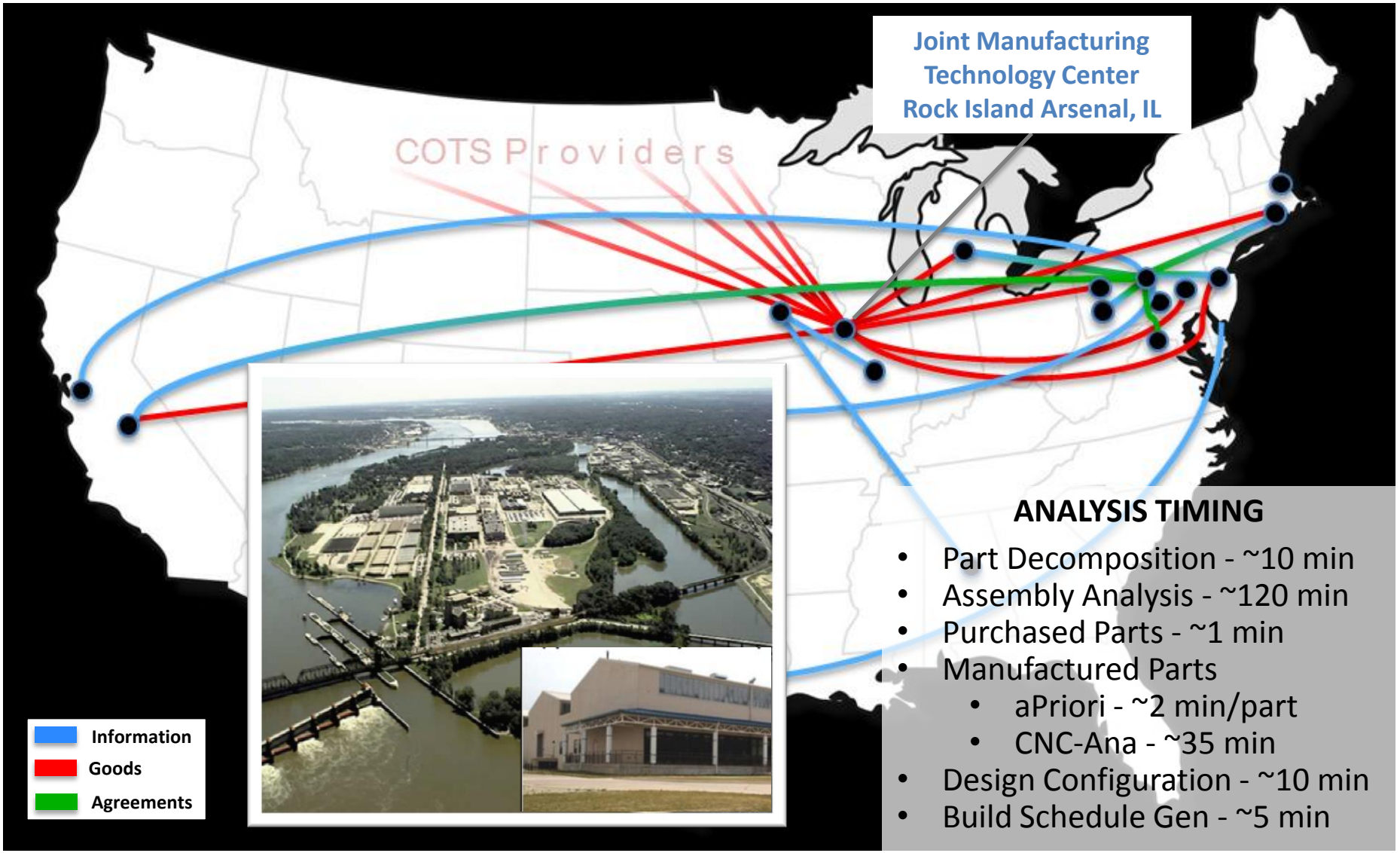
Sequencing & scheduling





Source: Penn State ARL

Tasking the distributed foundry & feedback to design



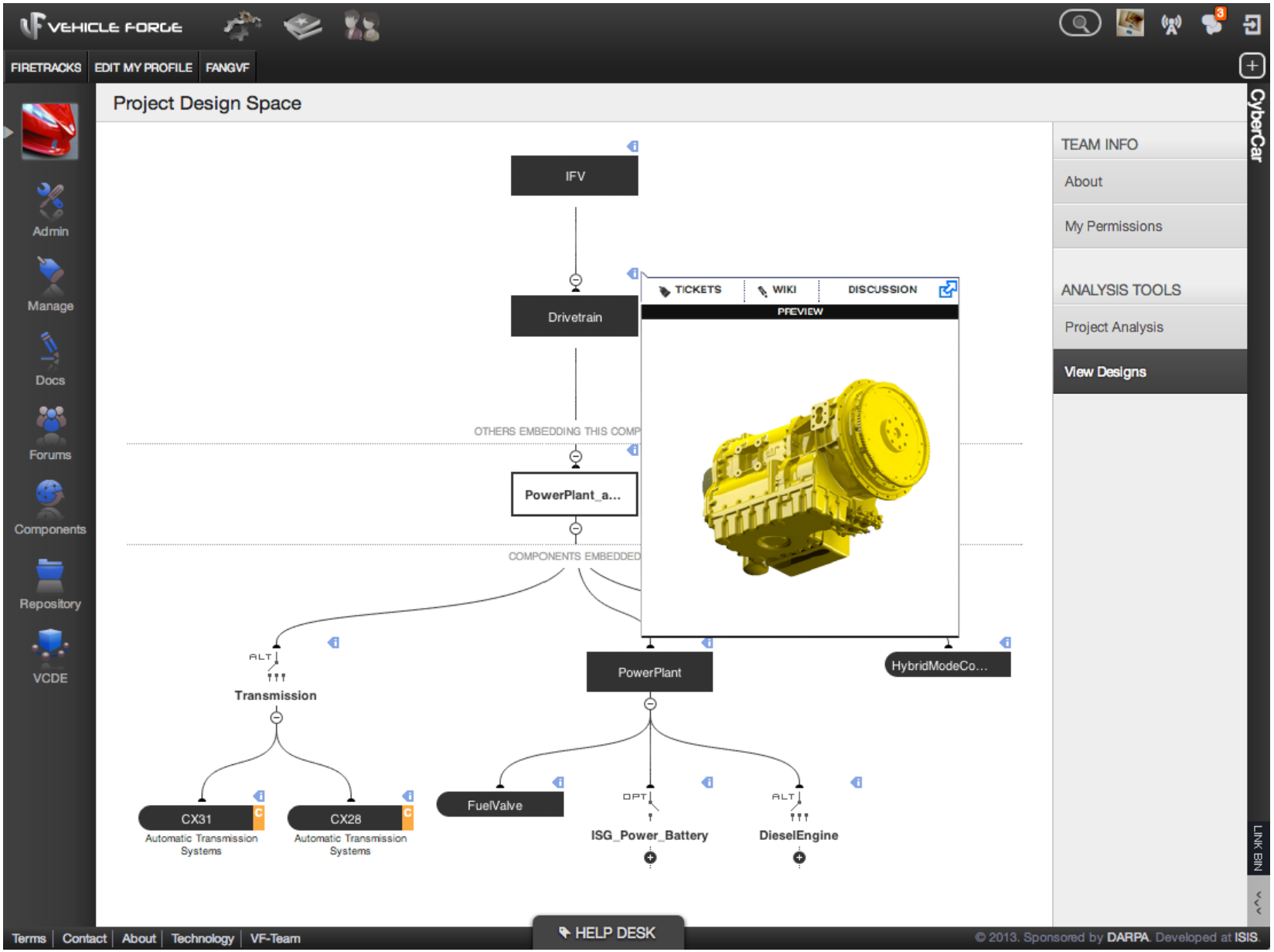
ANALYSIS TIMING

- Part Decomposition - ~10 min
- Assembly Analysis - ~120 min
- Purchased Parts - ~1 min
- Manufactured Parts
  - aPriori - ~2 min/part
  - CNC-Ana - ~35 min
- Design Configuration - ~10 min
- Build Schedule Gen - ~5 min

Source: Penn State ARL

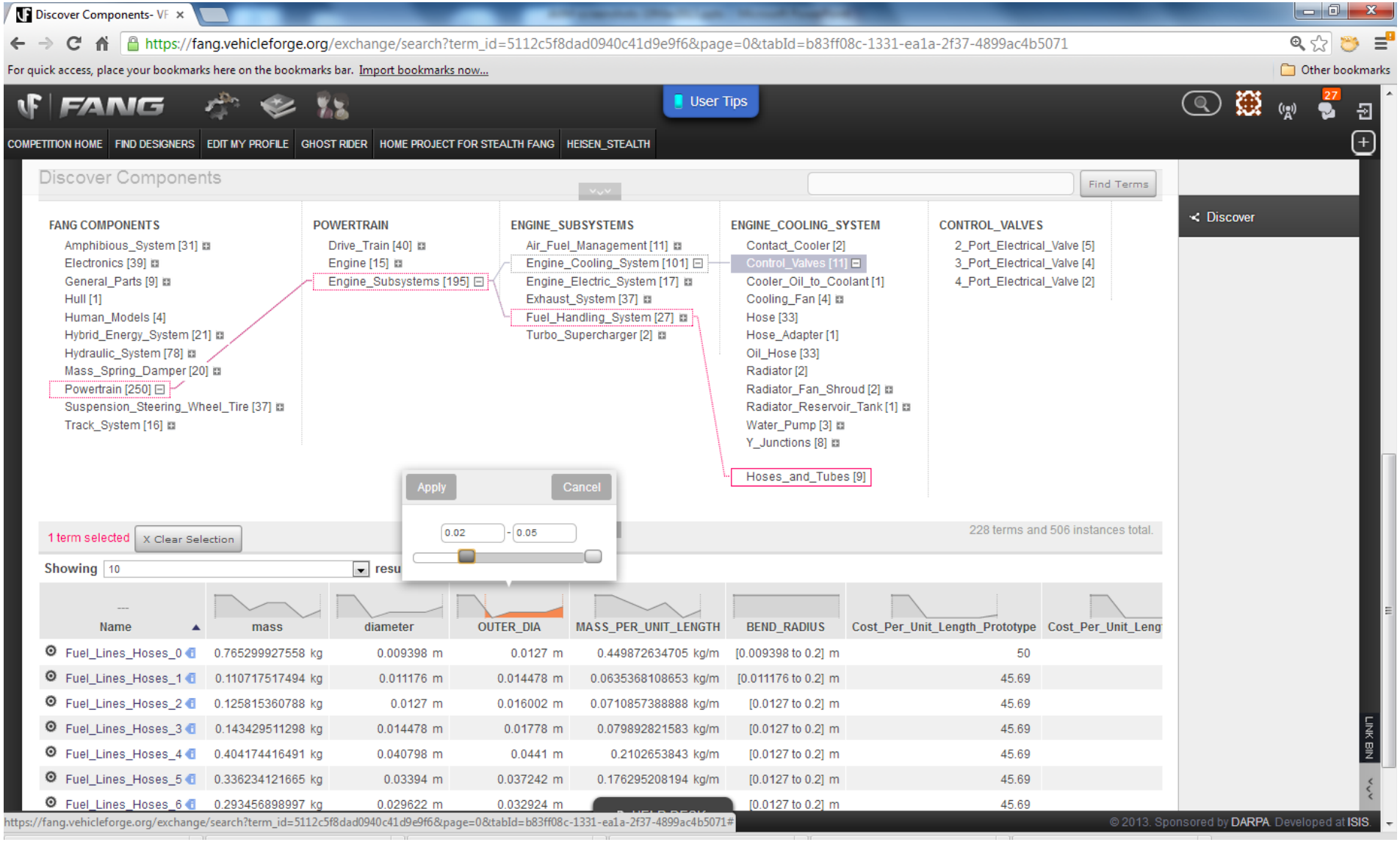
Ecosystem

Collaboration platform—configuration control



Source: Vanderbilt ISIS

Collaboration platform—component model ontology



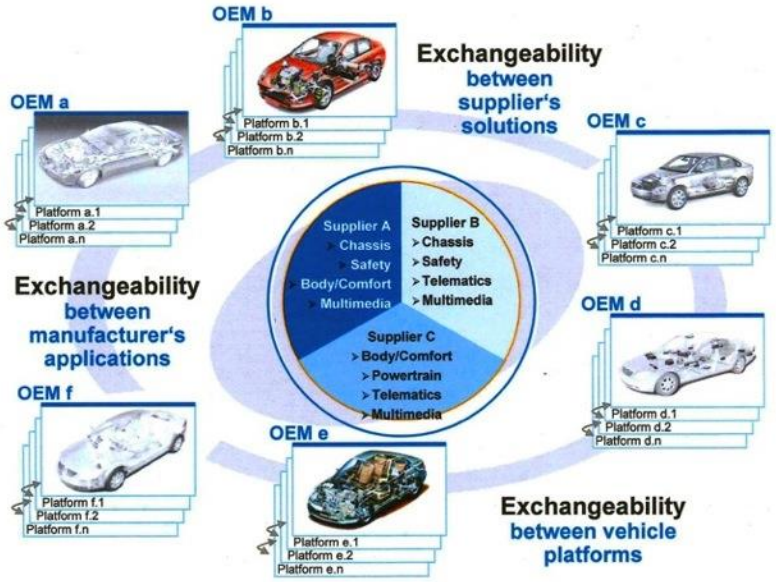
Source: Vanderbilt ISIS

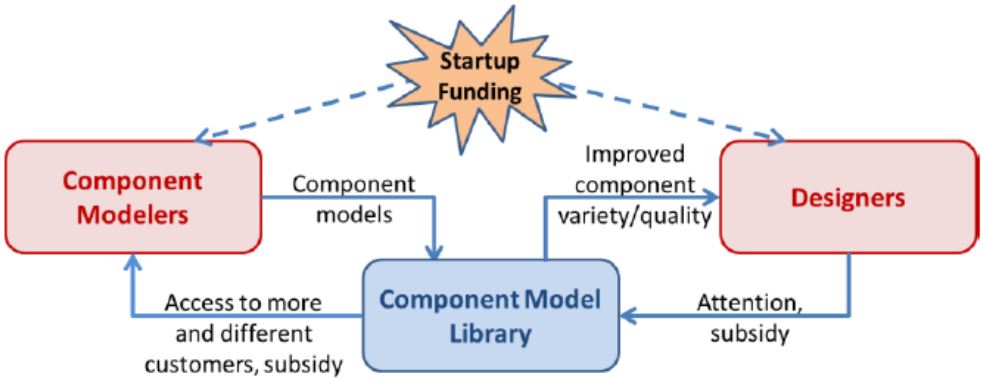
Collaboration platform—immersive multi-user visualization

Sources: Electrotank; Vanderbilt ISIS

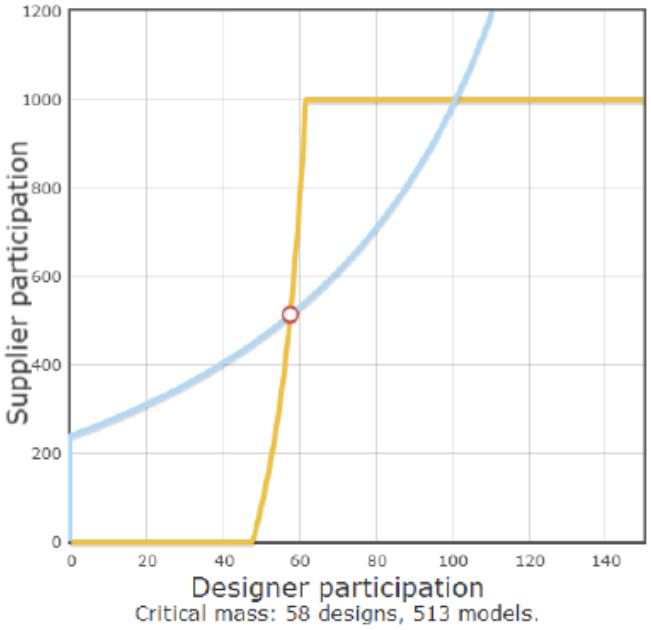
Critical scale for a model-based product ecosystem

AUTOSAR Consortium





Two-Sided Market Model



Boston Fusion ROM Estimate of Investment Scale

	Open IP	Closed IP
Cross-Market Subsidy Favors Designers	Market Never Self-Sustaining	$342M
Neutral Subsidy	$675M	$445M
Cross-Market Subsidy Favors Component Modelers	$581M	Market Never Self-Sustaining

Sources: Ferrari, A. *An Overview of (Electronic) System Level Design: beyond hardware-software co-design,* SFM-06:HV, Univ. of Urbino 2006; Jorge Tierno, Boston Fusion

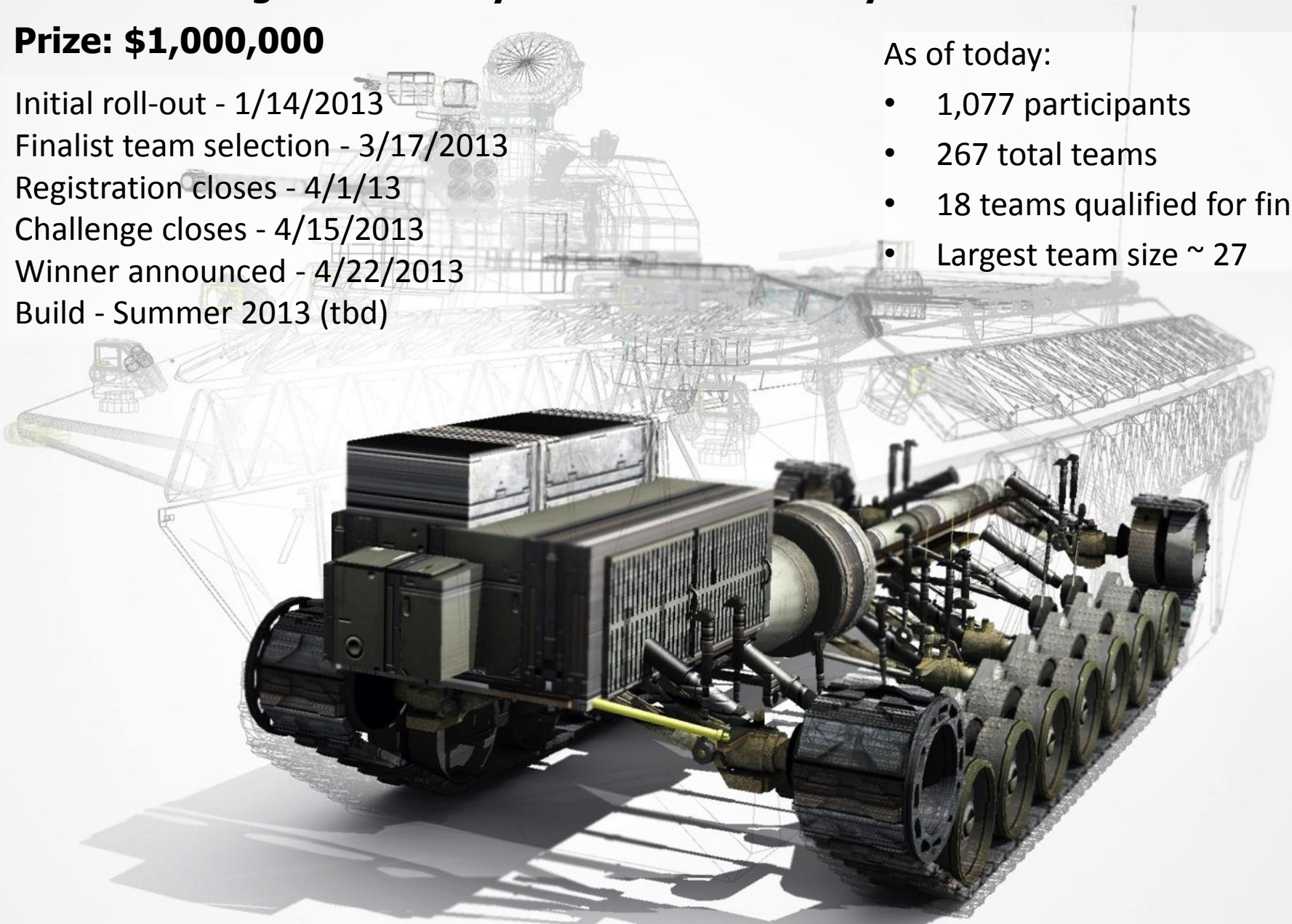
FANG Challenge 1 – Mobility and Drivetrain subsystems

Prize: $1,000,000

Initial roll-out - 1/14/2013
Finalist team selection - 3/17/2013
Registration closes - 4/1/13
Challenge closes - 4/15/2013
Winner announced - 4/22/2013
Build - Summer 2013 (tbd)

As of today:

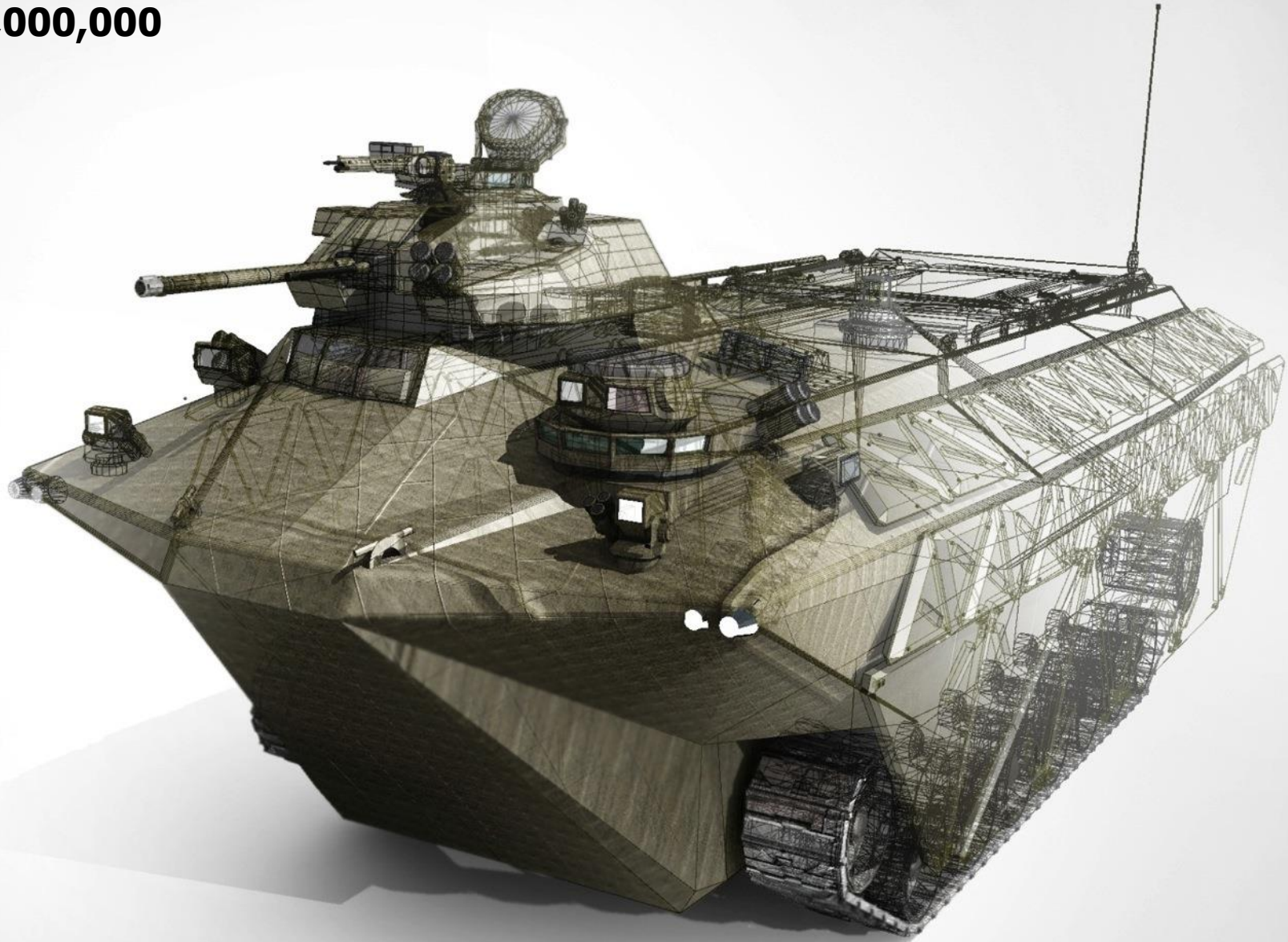
- 1,077 participants
- 267 total teams
- 18 teams qualified for finals
- Largest team size ~ 27



www.vehicleforge.org

FANG Challenge 2 – Chassis and Structural subsystems

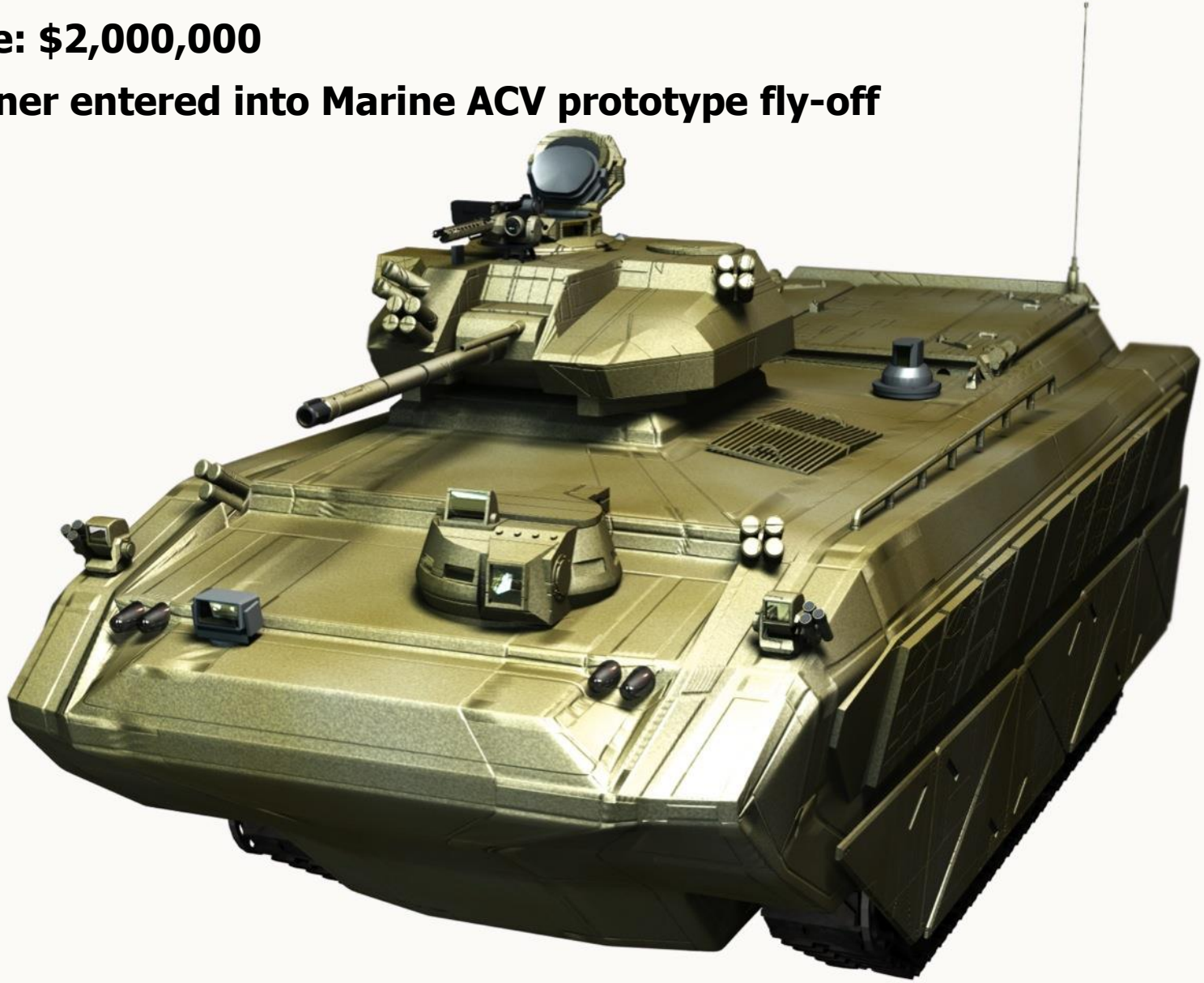
Prize: $1,000,000



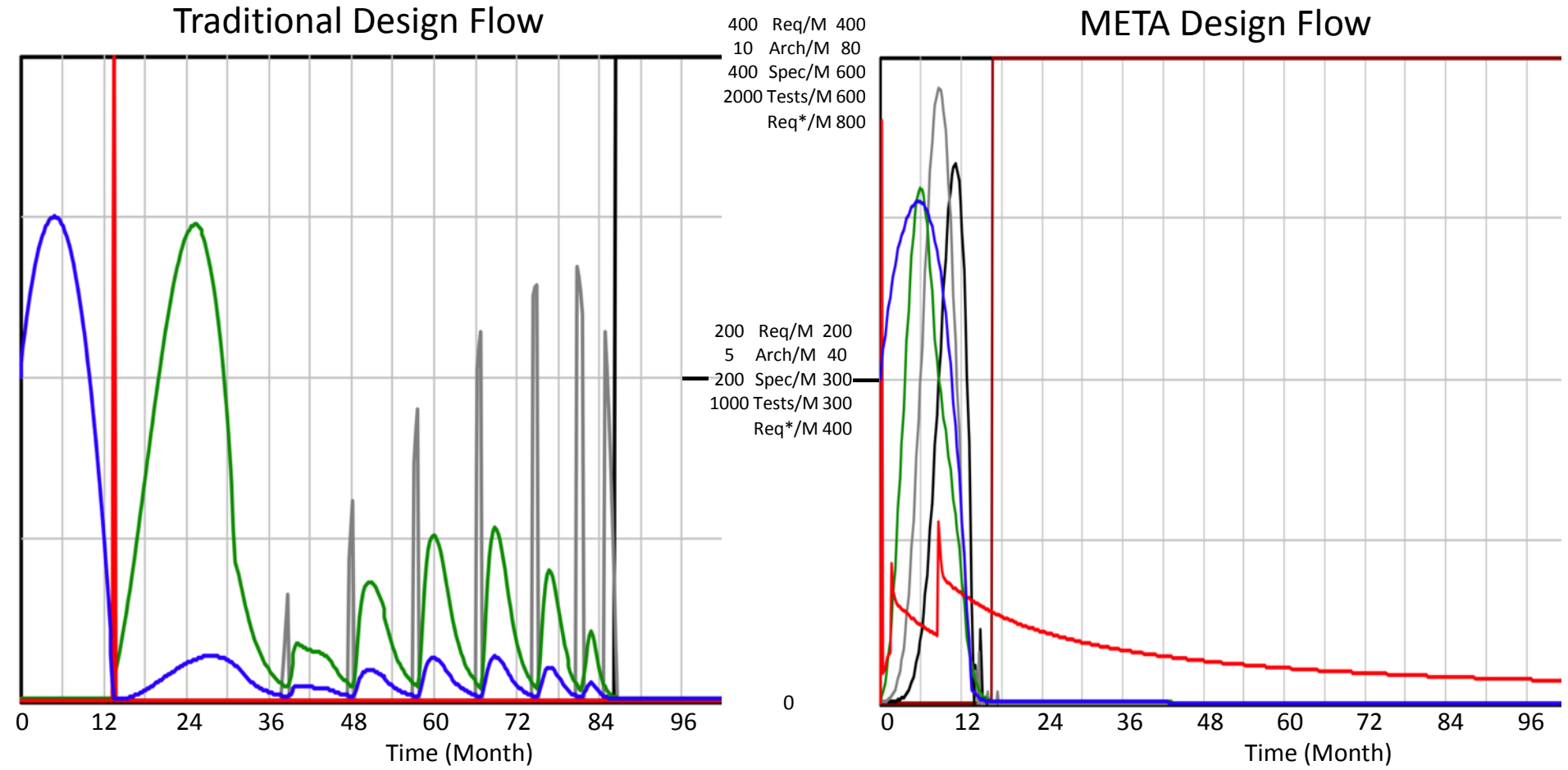
FANG Challenge 3 – Full Vehicle Design

Prize: $2,000,000

Winner entered into Marine ACV prototype fly-off



Modeling shows promise for 5X time compression



Source: Olivier de Weck, MIT

For more information:

FANG Challenges: http://www.vehicleforge.org
Source Code: http://www.cps-vo.org

DARPA PM: nathan.wiedenman@darpa.mil

Me: eremenko@alum.mit.edu

Coming soon… special issue of Journal of SE!