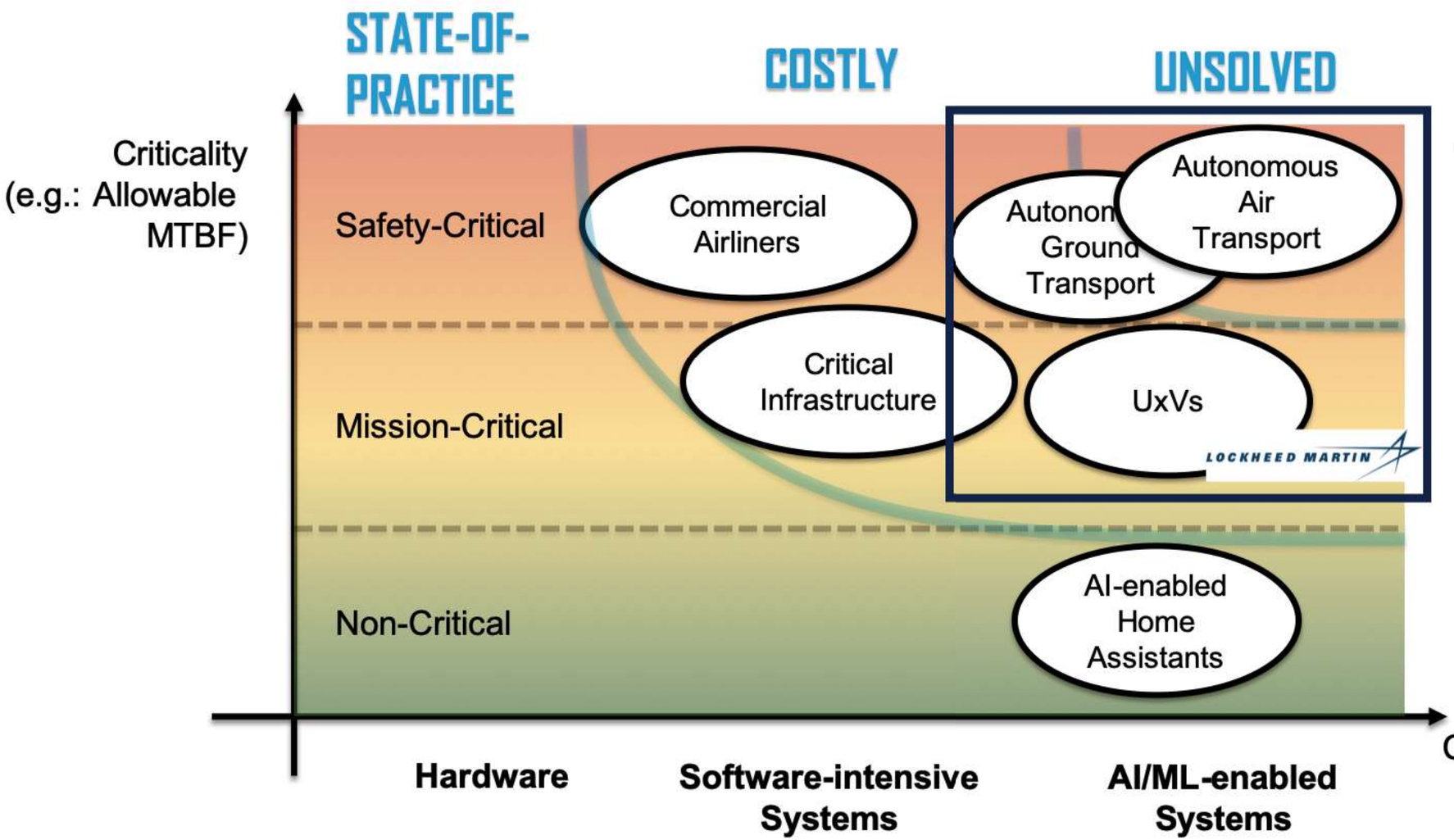
TRUSTWORTHY AUTONOMOUS SYSTEMS

MAURICIO CASTILLO-EFFEN (MAURICIO.CASTILLO-EFFEN@LMCO.COM)
LOCKHEED MARTIN CORPORATION

IEEE TC on Verification of Autonomous Systems Seminar

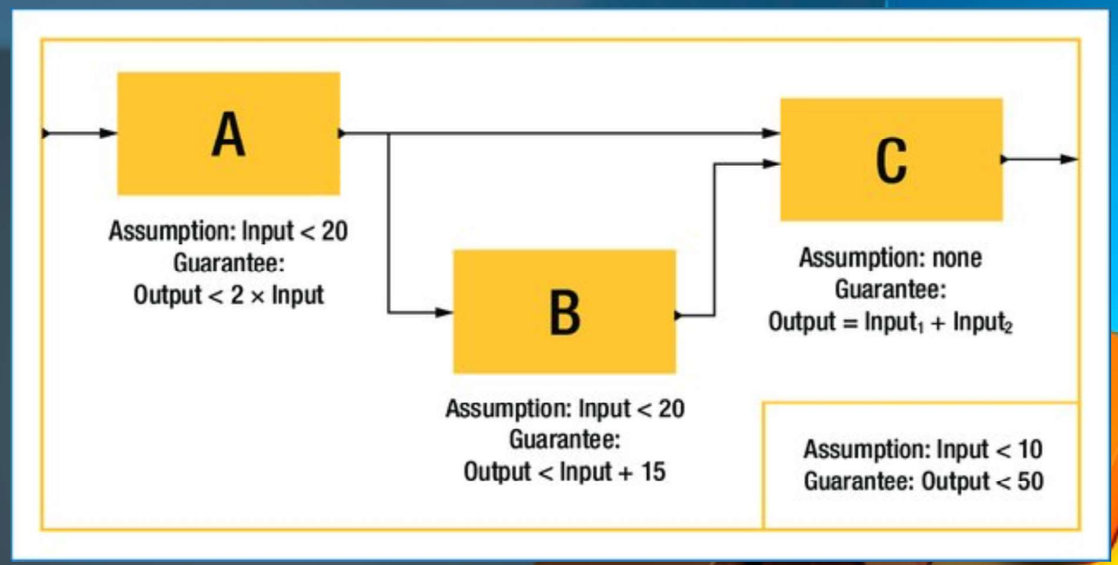
June 4th, 2020

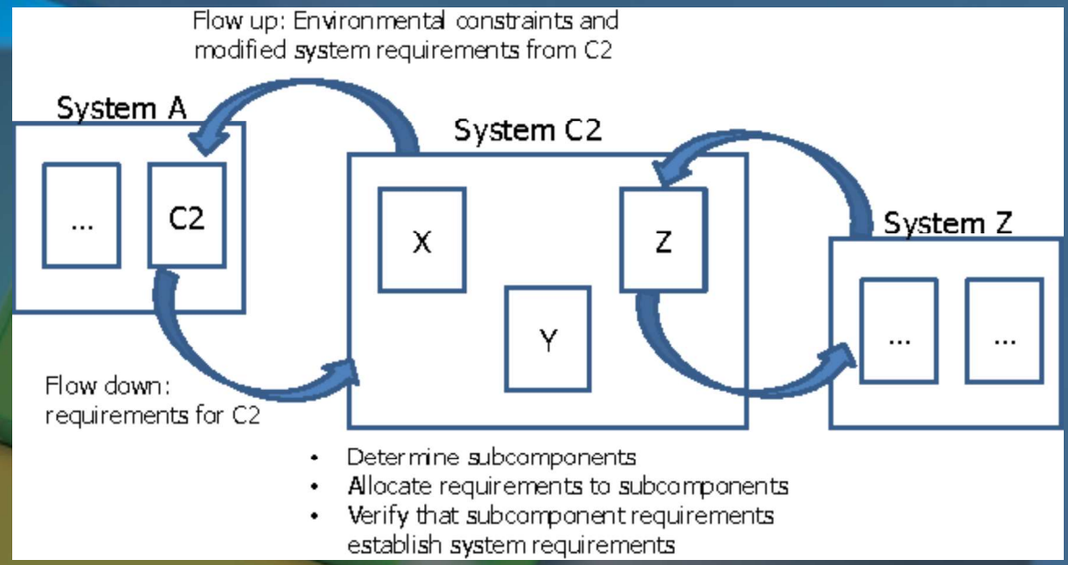
LOCKHEED MARTIN ADVANCED TECHNOLOGY LABORATORIES



TRUSTWORTHY AUTONOMOUS SYSTEMS (TAS)

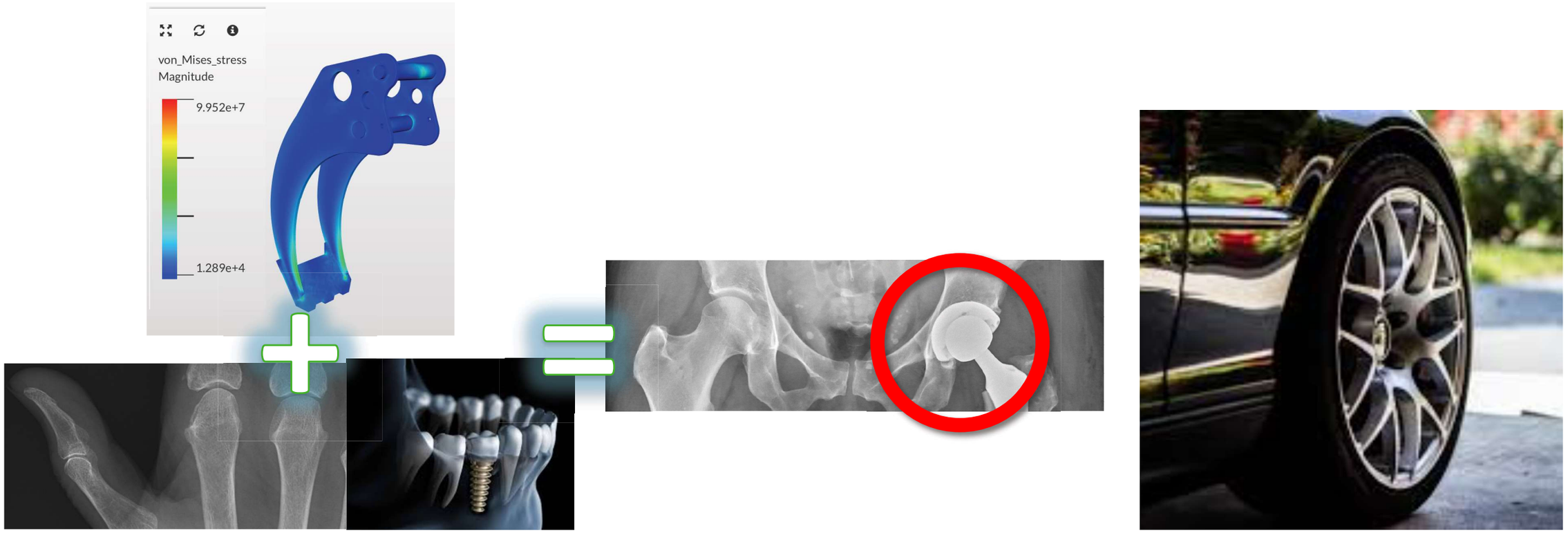
TAS APPLICATIONS

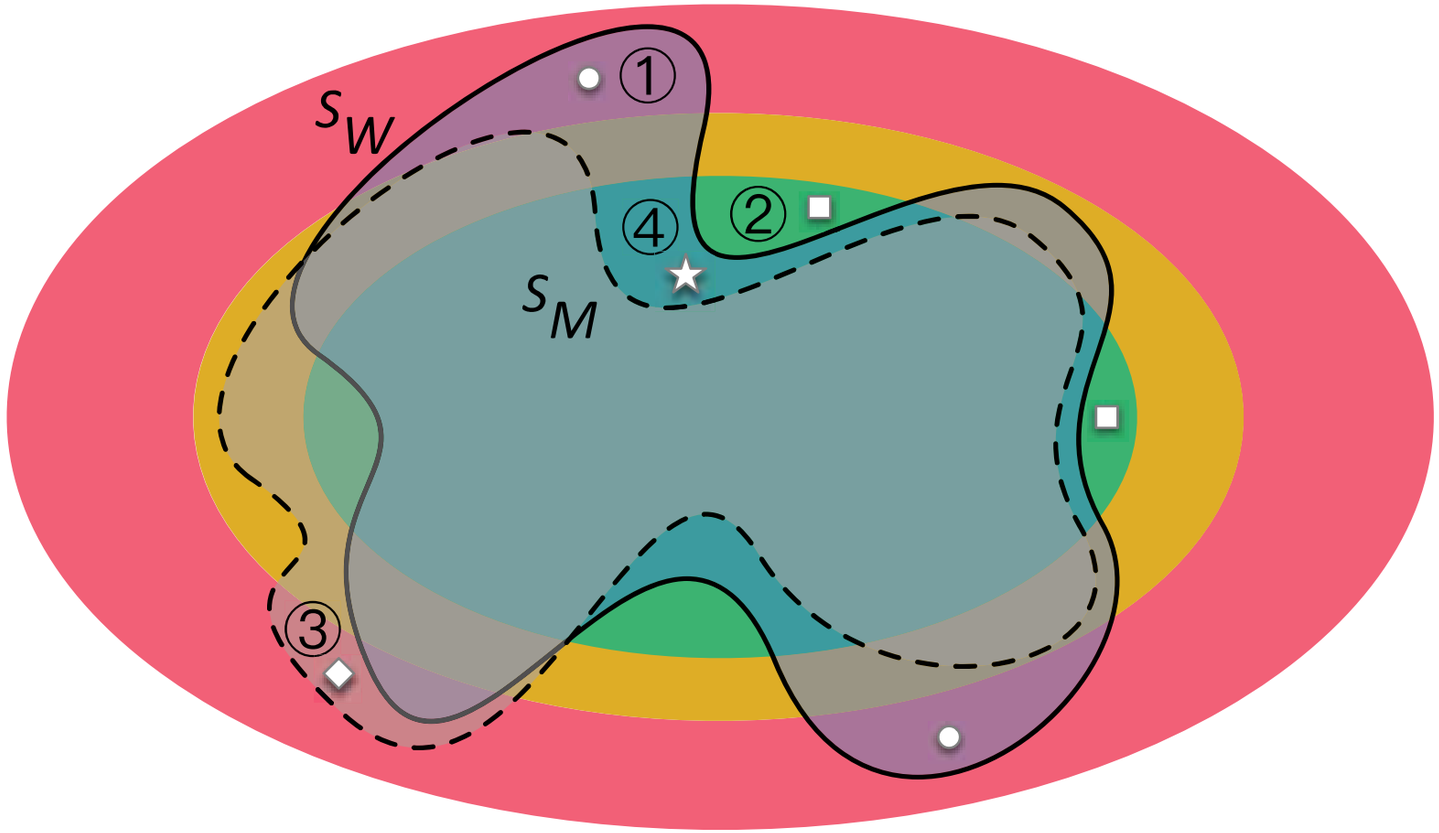




COMPOSITION

EMERGENT PROPERTIES





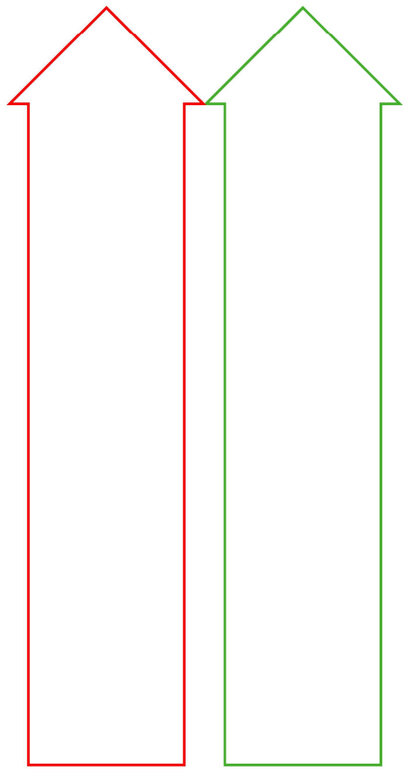
- Desired properties
- Unspecified but harmless
- "Shall not"s
- System's properties
- Model's properties

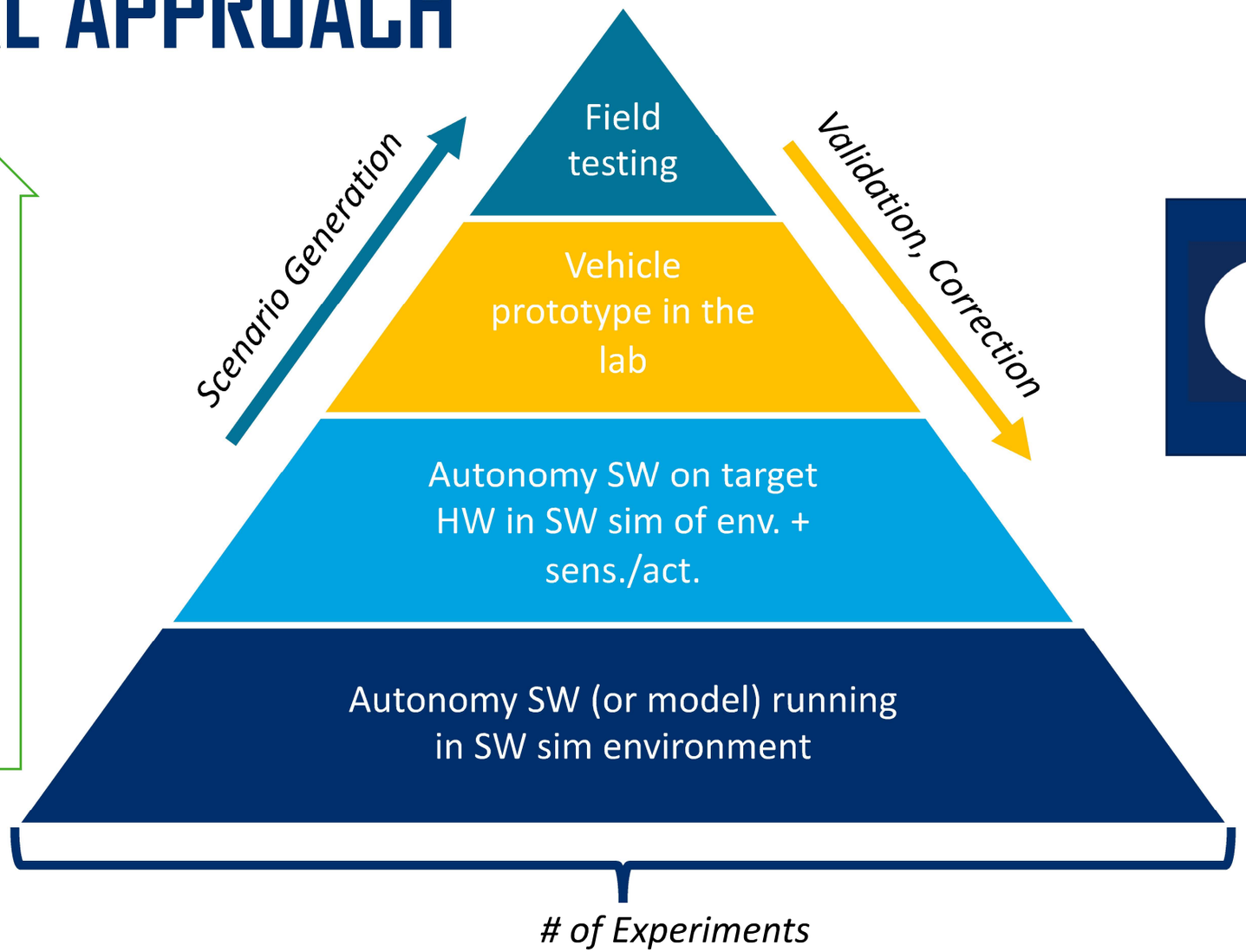
- System's violations of constraints
- System's deficiencies
- False positives
- False negatives

PROBABILISTIC INTERPRETATION

$$
\begin{aligned}
P\left(S_{\mathcal{W}} \vdash \mathcal{R}\right) = & P\left(S_{\mathcal{W}} \vdash \mathcal{R} \mid \; S_{\mathcal{M}} \equiv_{\mathcal{R}} S_{\mathcal{W}}\right) P\left(S_{\mathcal{M}} \equiv_{\mathcal{R}} S_{\mathcal{W}}\right) \\
& + P\left(S_{\mathcal{W}} \vdash \mathcal{R} \mid \; S_{\mathcal{M}} \not\equiv_{\mathcal{R}} S_{\mathcal{W}}\right) P\left(S_{\mathcal{M}} \not\equiv_{\mathcal{R}} S_{\mathcal{W}}\right) \\
\geq & P\left(S_{\mathcal{W}} \vdash \mathcal{R} \mid \; S_{\mathcal{M}} \equiv_{\mathcal{R}} S_{\mathcal{W}}\right) P\left(S_{\mathcal{M}} \equiv_{\mathcal{R}} S_{\mathcal{W}}\right) \\
\approx & P\left(S_{\mathcal{M}} \vdash \mathcal{R} \mid \; S_{\mathcal{M}} \equiv_{\mathcal{R}} S_{\mathcal{W}}\right) P\left(S_{\mathcal{M}} \equiv_{\mathcal{R}} S_{\mathcal{W}}\right).
\end{aligned}
$$

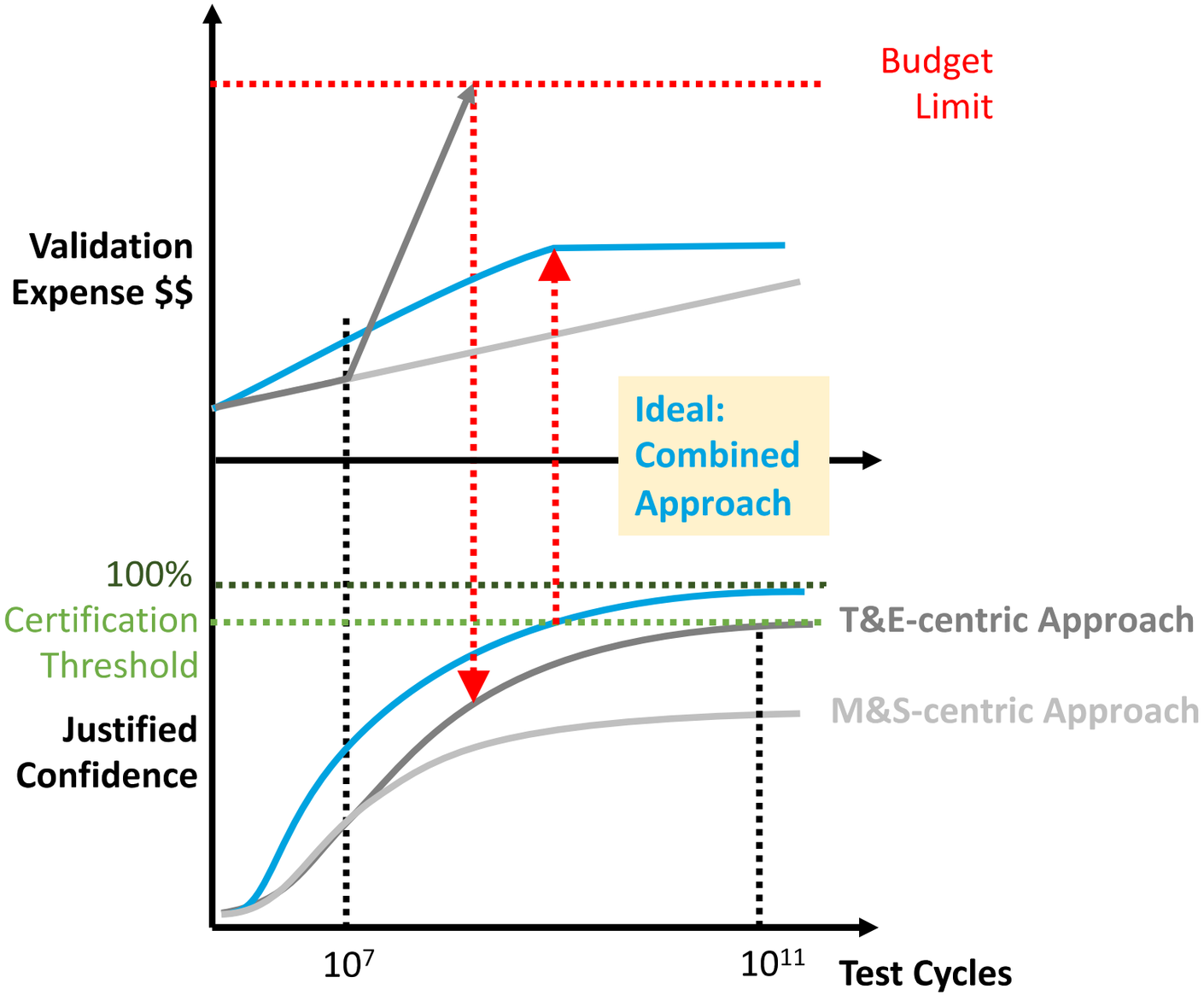
EMPIRICAL APPROACH



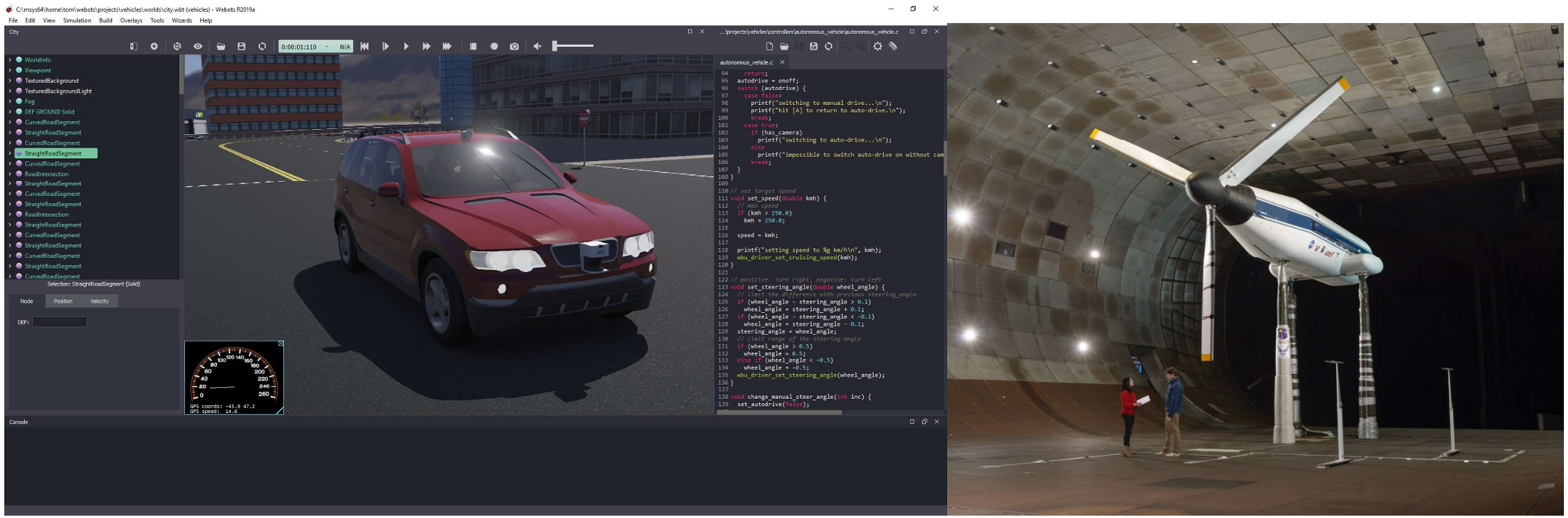


Feedback for Developers

Assurance Evidence

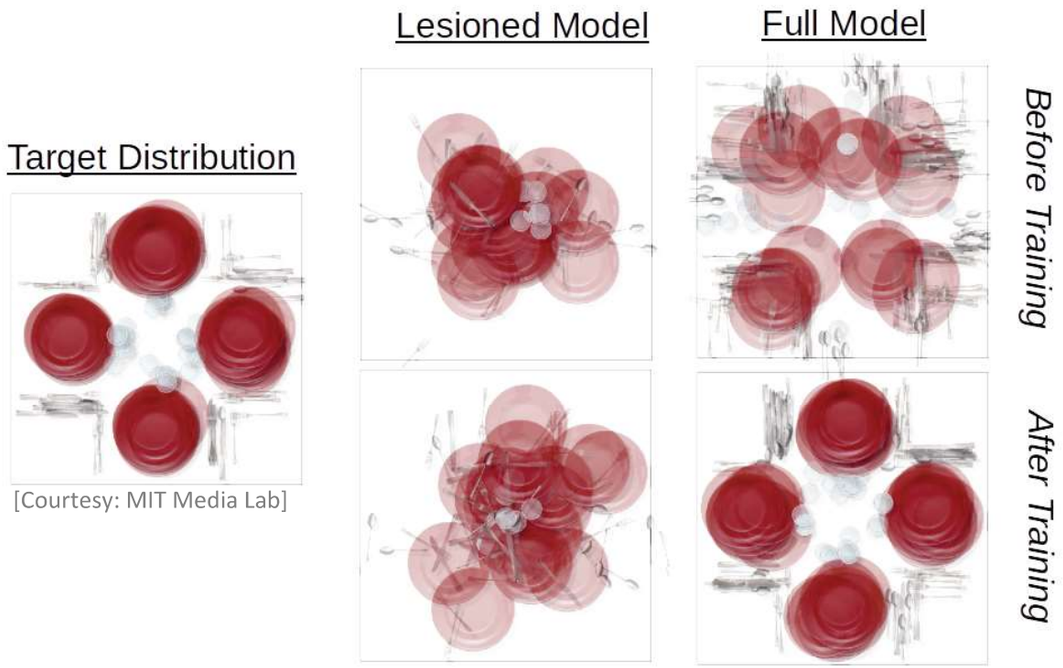

Budget
Limit
Validation
Expense $$
Ideal:
Combined
Approach
100%
Certification
Threshold
T&E-centric Approach
M&S-centric Approach
Justified
Confidence
10^7
10^{11}
Test Cycles

SIMULATION AS AN EXPLORATION TOOL



Challenges: scalability, automation for simulation-emulation-stimulation, data management

REASONING ABOUT VARIABILITY



[Courtesy: MIT Media Lab]

CONFIDENCE QUANTIFICATION

Driving to Safety — How Many Miles of Driving Would It Take To Demonstrate Autonomous Vehicle Reliability?
N. Kalra, S. M. Paddock (RAND Corporation)

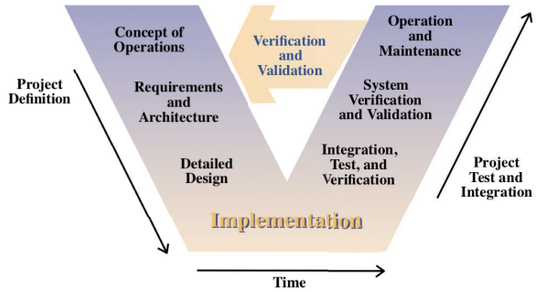
- Hundreds of millions of miles and sometimes hundreds of billions of miles to demonstrate their reliability in terms of fatalities and injuries.
- It would take tens and sometimes hundreds of years to drive these miles.

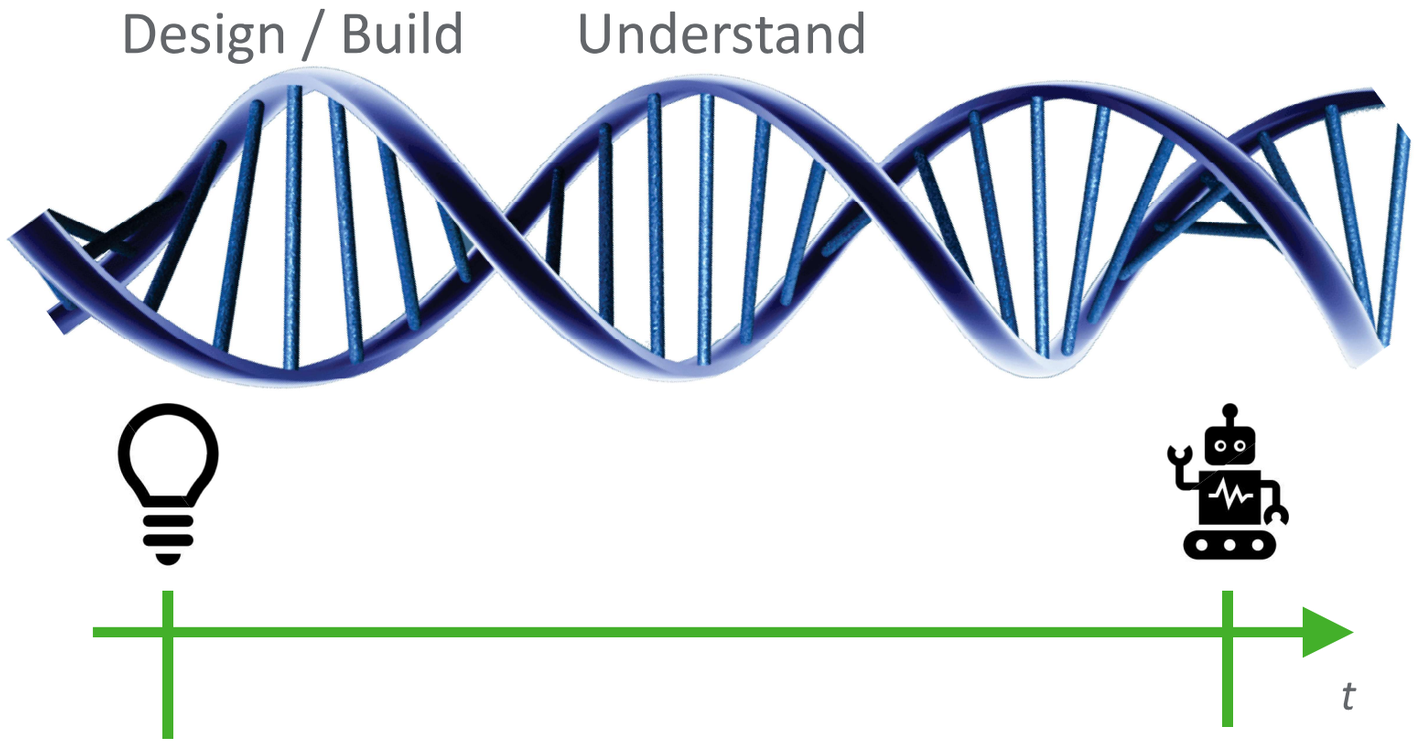
Waymo has driven ~10 million miles on the road and ~10 billion miles in simulation

Alphabet's Waymo valuation cut 40% by Morgan Stanley to $105 billion amid challenges in self-driving car market

PUBLISHED FRI, SEP 27 2019•2:45 PM EDT
UPDATED FRI, SEP 27 2019•3:42 PM EDT

COST OF V&V





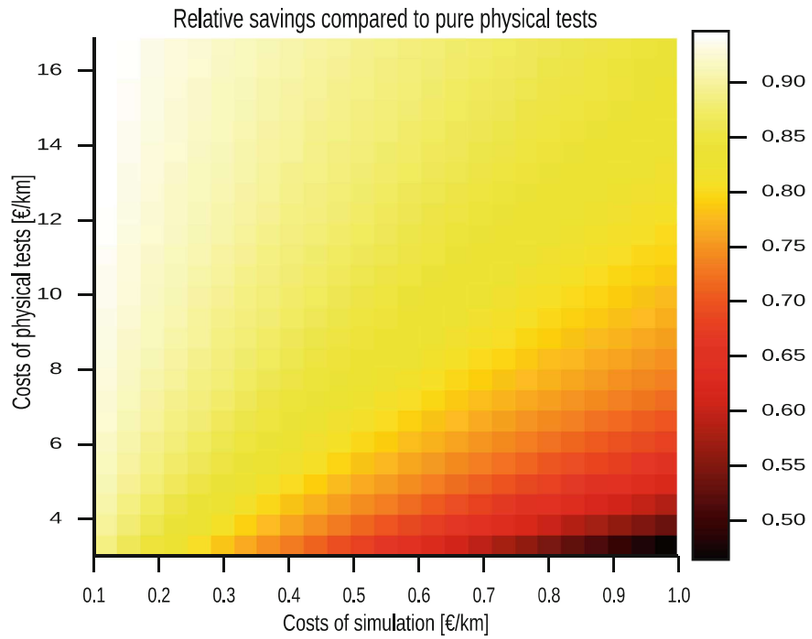


Fig. 2. Comparison of the optimal split and a purely physical testing setting.

Efficient Splitting of Test and Simulation Cases for the Verification of Highly Automated Driving Functions

Eckard Böde[1(✉)], Matthias Büker[1(✉)], Ulrich Eberle[2], Martin Fränzle[1], Sebastian Gerwinn[1], and Birte Kramer[1(✉)]

[1] OFFIS - Institut für Informatik, Escherweg 2, 26121 Oldenburg, Germany
{boede,bueker,fraenzle,gerwinn,kramer}@offis.de
[2] Opel Automobile GmbH, Bahnhofsplatz, 65423 Rüsselsheim am Main, Germany
ulrich.eberle@opel.com

ROAD TO TAS

- A flexible path towards justified trustworthiness where one chooses the most effective assurance activities considering the increase in confidence and cost
- Exploitation of elastic computing resources
- Formal analysis informing empirical exploration
- Formalisms to capture mission variability
- Incorporation of adversarial behavior
- Operational assurance

QUESTIONS?

Email: mauricio.castillo-effen@lmco.com