Assurance cases in an era of smart and collaborative cyber-physical systems – pain points and ways forward

Martin Törngren, Professor
https://www.kth.se/profile/martint
Mechatronics and Embedded Control Systems,
Machine Design, KTH - Royal Institute of Technology

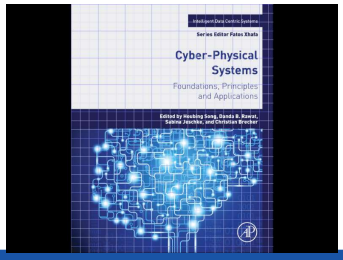
Innovative Centre for Embedded Systems

About the lecturer - Dr. Who?

- Prof. at KTH in Embedded Control Systems since 2002
- Architecting and MBSE, Automated vehicle safety,
- KTH and industry competence network - www.ices.kth.se
- Scandinavian System and Software Safety Conference

PLATFORMS 4CPS

CyPhERS



Safety (and assurance) cases

Safety case: "… a structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment" - NASA System Safety Handbook ver. 1 (2014)

Assurance case: "A documented body of evidence that provides a convincing and valid argument that a specified set of critical claims regarding a system's properties are adequately justified for a given application in a given environment" – MITRE (2005)

Applied in one way or the other in many domains
(safety standards, sometimes directly connected to regulations),

Typical safety case content

Core content

- Environment description (airspace system)
- System description, system change description
- Aircraft capabilities and flight data
- Accident / incident data
- Pilot / crew roles and responsibilities
- Hazard analysis, risk analysis, risk controls, …
- …

Safety risk management plan

- Hazard tracking and treatment
- Safety performance monitoring

FAA (8900.1, FSIMS, vol. 16, UAS), Courtesy of Ewen Denney

Cyber-physical systems (~2006)

Integration of computation, networking and physical processes where CPS range from minuscule (pace makers) to large-scale (e.g. national power-grid).

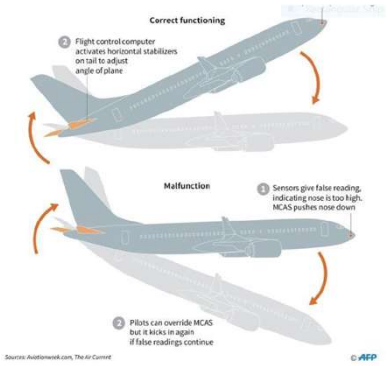
Not new but characterized by

- Live, collaborative, ”smart” and automated
- Integration: Technology, systems, domains, life-cycle
- Business model evolution
- Open society scale deployment

Unprecedented opportunities, societal reliance and risks

CPS trends and melting pot

Boeing 737 MCAS

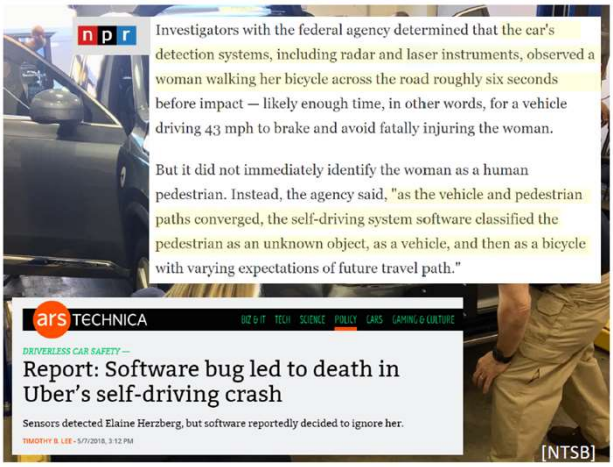


After two flight crashes:

A <u>compelling</u>, <u>comprehensible</u> and <u>valid</u> case?

The Maneuvering Characteristics Augmentation System (**MCAS**) flight control law **was designed and certified** for the 737 MAX **to enhance the pitch stability** of the airplane – so that it feels and flies like other 737s (Source: Boeing).

Uber crash March 2018



A <u>compelling</u>, <u>comprehensible</u> and <u>valid</u> case?

Dealing with inherent dynamic risk

www.youtube.com/watch?v=HjtiiGCe1pE&feature=youtu.be

Reflections

Safety represents a continuous struggle!

- Safety cases are non trivial even for current CPS

The automation paradox is more relevant than ever

Indicators/metrics (leading/lagging); roles; safety culture; …

The CPS paradigm shift however imposes new challenges

The million or trillion dollar question?

By FE Bureau: https://www.financialexpress.com/education-2/what-will-shape-future-smart-cities-of-india-find-out-here/968678/

Assurance cases in an era of smart and collaborative CPS

- Initial scenarios
- Analysis:
  Complexity of CPS; Drivers
  Effective SC's/AC's
- Directions:
  Strategy; Complexity;
  Barriers and operational risk management
- Wrap-up

Autonomy: Basic functions

Observation

Localization

Object detection & classification

Planning and generation

Control

Vehicle dynamics

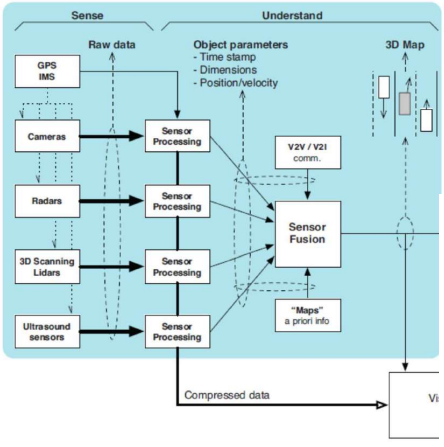
Energy management

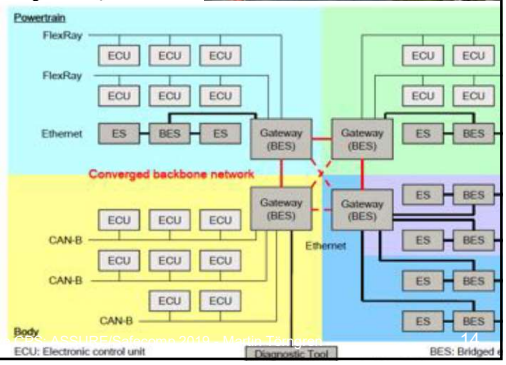
Steering

Propulsion

Braking

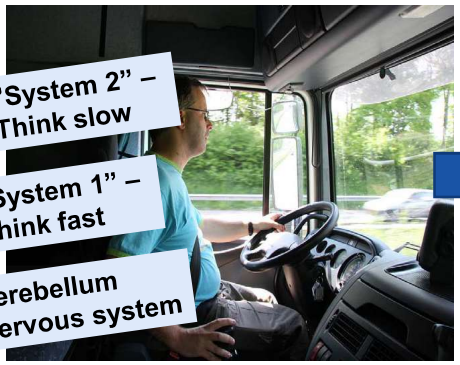
Unprecedented capabilities and complexity





Breaking new ground – generalized knowledge

ADI – ”Autonomous Driving Intelligence”



By Veronica538 (Own work)
[CC BY-SA 3.0 (http://creativecommons.org/licenses/by-sa/3.0) or GFDL (http://www.gnu.org/copyleft/fdl.html)], via Wikimedia Commons

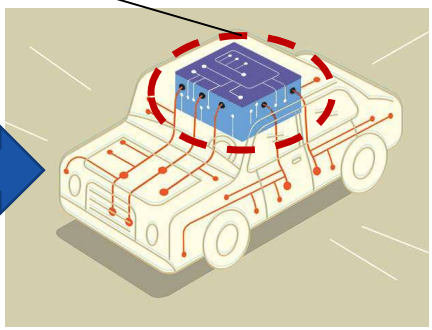
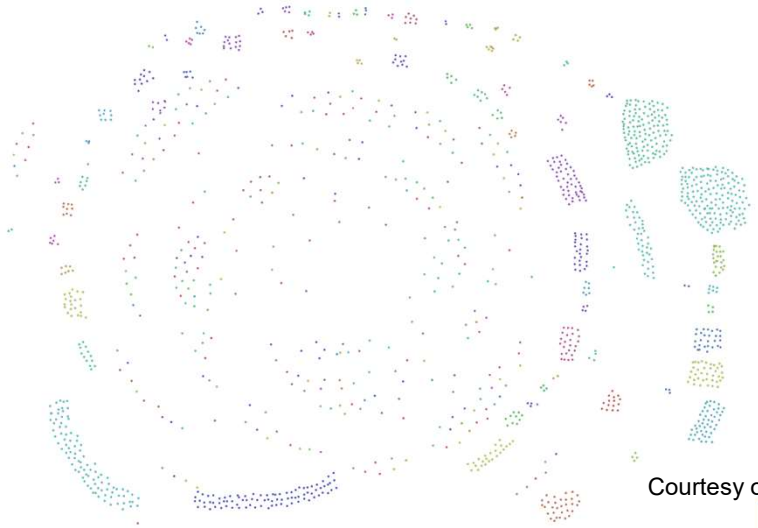


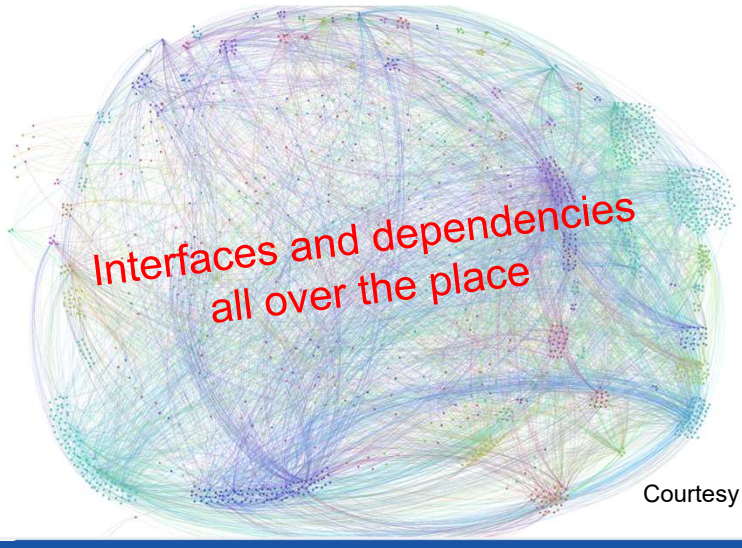
Illustration: Harry Campbell, IEEE Spectrum
http://spectrum.ieee.org/cars-that-think/transportation/self-driving/nxps-bluebox-bids-to-be-the-brains-of-your-car

1500 logical nodes – example Scania production vehicle, 2013



Courtesy of Scania

14000 connections – same Scania production vehicle example, 2013



Courtesy of Scania

The "Cyber Physical" tension

Dimension	„Cyber Domain"	„Physical Domain"
Example Disciplines	Logistics	Aeronautics
Typical Life Cycle	< 2-3 Year	> 10-30 Years
Business Model	Dynamic Value Network	Static Supply Chain
Development Approach	Continuous Delivery	Implement-Commission-Operate –Decommission
Dependability Focus	Security	Safety (and certification)
Platform Approach	Max. virtualization/Cloud	Min. virtualization/RTOS
Example Technologies	Big Data, Online Learning	Control Synthesis

Composability yet an unresolved challenge

A key CPS challenge: Combinations of deterministic models are non-determinstic

Image: Wikimedia Commons

```
void initTimer(void) {
    SysTickPeriodSet(SysCtlClockGet() / 1000);
    SysTickEnable();
    SysTickIntEnable();
}
volatile uint timer_count = 0;
void ISR(void) {
    if(timer_count != 0) {
        timer_count--;
    }
}
int main(void) {
    SysTickIntRegister(&ISR);
    ... // other init
    timer_count = 2000;
    initTimer();
    while(timer_count != 0) {
        ... code to run for 2 seconds
    }
    ... // other code
}
```

$$\dot{\mathbf{x}}(t) = \dot{\mathbf{x}}(0) + \frac{1}{M}\int_0^t \mathbf{F}(\tau)d\tau$$

No notion of timing at the SW level

Courtesy, Edward Lee, UC Berkeley

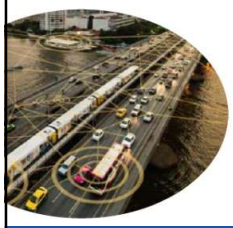
Challenge further aggravated by non-predictable multicore platforms

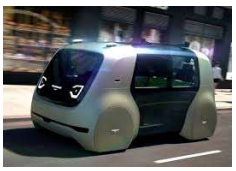
Future CPSoS – some safety challenges

Built in risk metrics – acceptable risk
Collaboration models – behaviors and anomalies
Perception, awareness, assumptions
Openness and uncertainty of environment
Evolution, upgrades, learning
Deep learning robustness and failure modes
Higher levels of automation => Automation paradox
Transitioning periods
Exposure, severity, security
Interactions and governance in systems of systems
…

Cyber-physical systems

Arthur C. Clarke:
Any sufficiently advanced technology is indistinguishable from magic



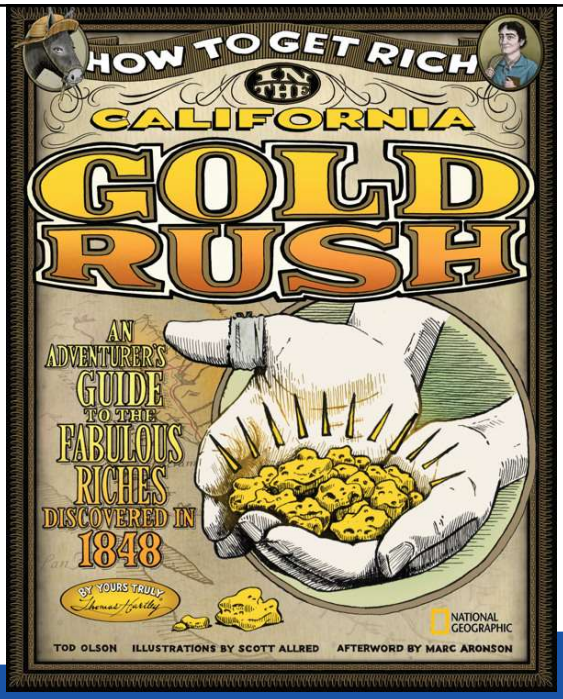


What drives AV development?

Business MIT Tech Review:
- **Can We Put a Price on Autonomous Driving?**

- Transport services: ~ Trillions of dollars!
- Traffic accidents: 100's of billions of dollars
- Traffic efficiency, productivity and public health: - II -

The beginning of wisdom is to call things by their proper name – attributed to Confucius



Today: Billions poured in to get to the Trillions!

Key question: When will the Gold emerge?

1849 – Gold rush

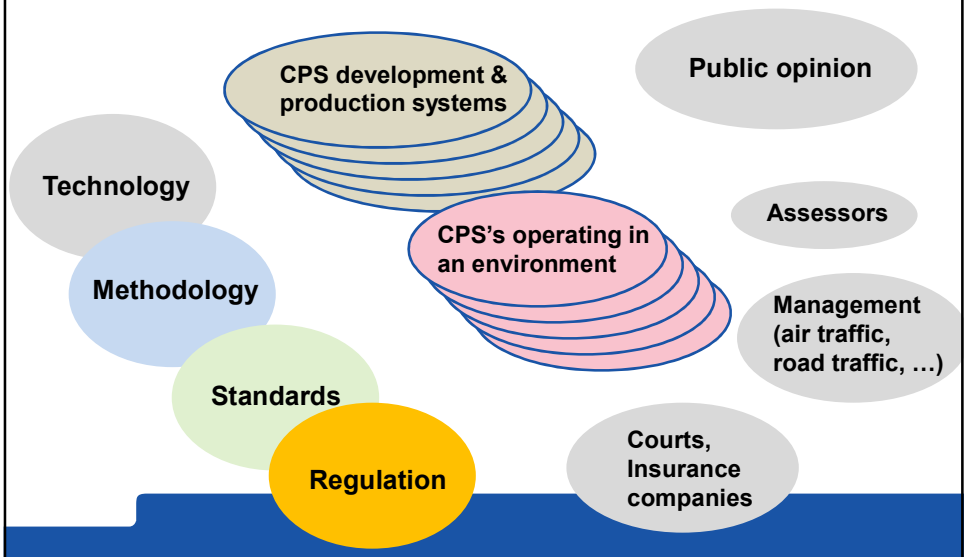
Several parallel gold rushes!

Automated driving/ transportation services

1000? IoT platforms

Strong market forces!
Partly unregulated areas!

Intricate role of safety cases and gaps



Effective assurance cases – essentials (SCC, SafeComp, AD, SCSSS, …) and challenges

Effective: … actually improving safety, providing useful description for certification and court cases/accidents, adding value to the engineering process

Cost and competition pressure

Human – computer interaction

Requires multi-domain expertise, collaboration and humility

- Human psychology and biases

Methodology, mindset and organization (Robin Bloomfield)

- Systematic and Systemic (Hillary Sillitto)
- Safety culture

Assurance cases in an era of smart and collaborative CPS

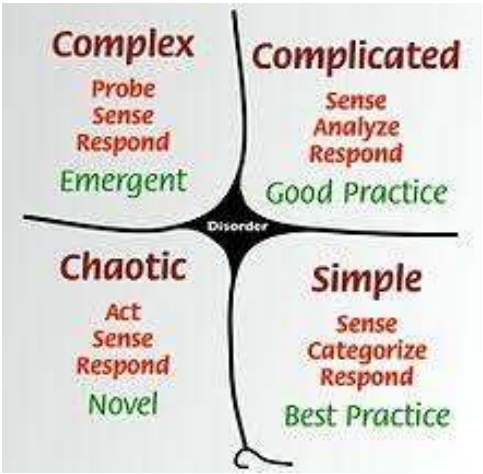
Initial scenarios

Analysis:
Complexity of CPS; Drivers
Effective SC's/AC's

Directions:
Strategy; Complexity;
Barriers and operational risk management

Wrap-up

Systems engineering insights and needs for new methodologies



- ➔ complex environments and uncertainty
- ➔ composability – dependencies, trade-offs and side effects

The Cynefin model

Current level 3 testing for AD/AVs

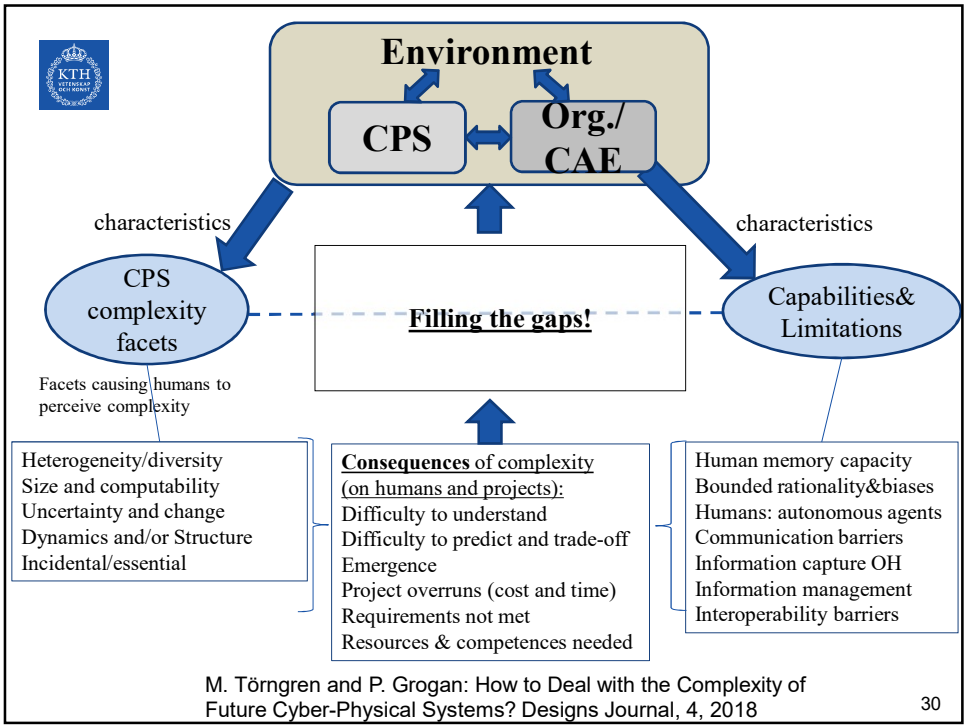
Current tests in the automotive are not well controlled!

Aerospace:

- Simulation, formal methods and rigorous processes.
- Minimizing testing to mitigate risks – Controlled experiments
- **But … safety requires continuous efforts!!!**

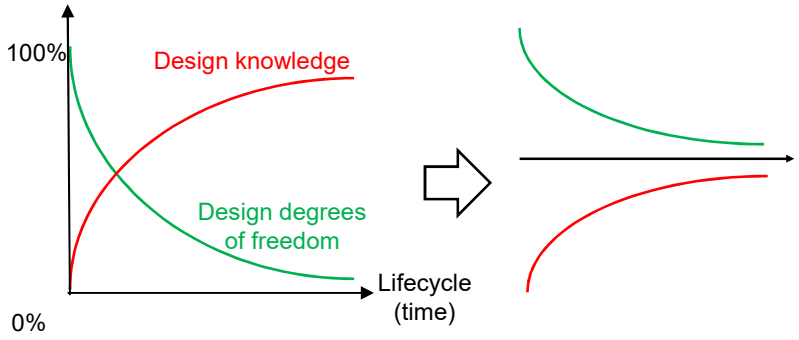
Safety case for level 3 testing (Phil Koopman)

- An AV testing platform with safety driver
- Non fruitful blames: victim, technology, safety driver
- To be expected: Pedestrian on road; Failures; Solo human drop-out
- The better autonomy the more difficult situations!



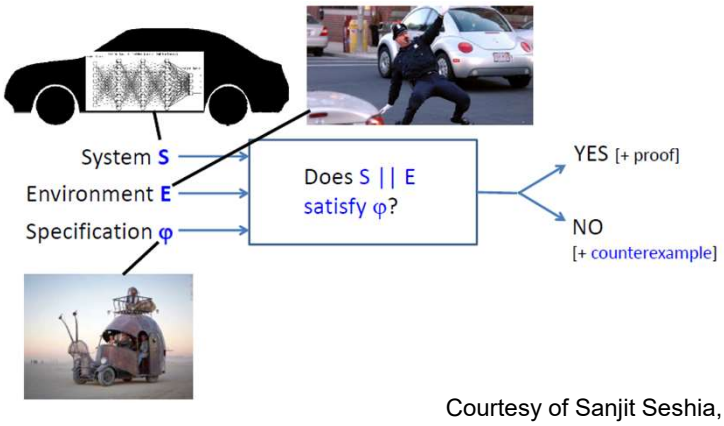
M. Törngren and P. Grogan: How to Deal with the Complexity of Future Cyber-Physical Systems? Designs Journal, 4, 2018

Managing an increasing cone of uncertainty



- **Uncertainties in system and environment**
- **Resilience; fault-tolerance; survivability**
- **Operational management at system and SoS level**

New challenges and opportunities for formal methods



Courtesy of Sanjit Seshia, UC Berkeley

Need for new methods

Abstractions - e.g. smart ways of describing environments, coverage metrics

Systematic uncertainty management; awareness

Platform based design: Supervisor architectures supporting minimal risk conditions

Formal methods, simulation and machine learning

Tools managing heterogeneous, distributed. Interdependent and changing information;

- Multiview modeling and contract based design

Assurance cases in an era of smart and collaborative CPS

Assurance cases in an era of smart and collaborative CPS

Importance of safety initiatives during a paradigm shift

”Simplicity is complex” (Hermann Kopetz)

- Complexity management; and awareness!
- Architecting and new methods: model-based engineering
- Cynefin: ”Safe” exploration and testing of advanced CPS

Safety cases are non trivial even for current CPS

- Building trust
- The automation paradox is more relevant than ever
- Education and training! Systems thinking!

Leading indicators/metrics

- Risk metrics – and agreements on behaviors at SoS level

Some references for further reading

Martin Törngren and Paul T. Grogan. **How to Deal with the Complexity of Future Cyber-Physical Systems?**, Journal of Designs, Vol. 2, No. 4, 2018

Naveen Mohan and Martin Törngren. **A practical simulation toolchain for the early verification of Functional Safety Concepts**. Accepted for SAE World Congress, 2019.

Martin Törngren et al. **Architecting Safety Supervisors for High Levels of Automated Driving**. 21st IEEE Int. Conf. on Intelligent Transportation Systems, Nov. 2018.

Lars Svensson et al. **Safe Stop Trajectory Planning for Highly Automated Vehicles**. IEEE Int. Vehicles Symposium, 2018

Naveen Mohan et al. **ATRIUM - Architecting Under Uncertainty**: For ISO 26262 compliance. IEEE SysCon 2017.

Sagar Behere and Martin Törngren. **A functional reference architecture for autonomous driving**. J. of Information and Software Technology, 2016. Elsevier.

Xinhai Zhang et al. **Architecture Exploration for Distributed Embedded Systems**: A Gap Analysis in Automotive Domain. 12th IEEE Int. Symposium on Industrial Embedded Systems.