

Day 3: Thursday, June 18



SAFE AUTONOMOUS VEHICLES?

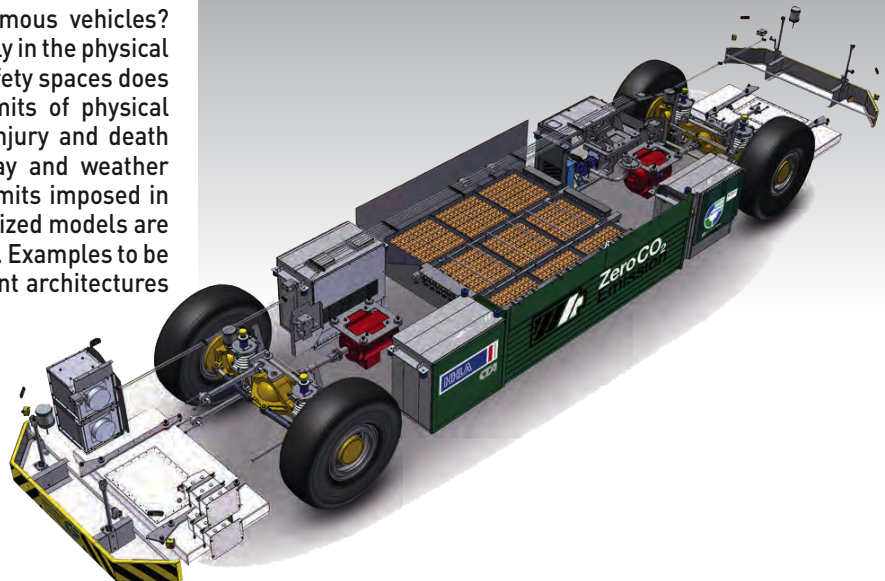
DR GRAHAM HELLESTRAND,
CEO, EMBEDDED SYSTEMS
TECHNOLOGY, USA

ABSTRACT: Can physical testing produce safe autonomous vehicles? What proportion of safety spaces are covered economically in the physical testing of a vehicle? How much of dimensionally huge safety spaces does 1,000,000 miles of autonomous driving cover? The limits of physical testing are imposed by design and state of vehicles; injury and death from intentional scenarios; pollution; location, roadway and weather conditions; and state of drivers and pedestrians. The limits imposed in simulated scenario testing using high-fidelity parameterized models are those of natural science, including physics and chemistry. Examples to be presented include unsafeness of DSRC, and fault-tolerant architectures for autonomous control.

ivT: Can you comment on the similarities/differences in the level, or types of testing required, between autonomous off-highway equipment and autonomous cars?

GRAHAM HELLESTRAND: High-fidelity vehicle models enable full ISO 26262 analysis of risk and the dynamic verification of operation of components, subsystems, systems (for instance, vehicles), and systems of systems (many vehicles in traffic) against their respective specifications. Whether vehicles are on-road, off-road recreational or off-road industrial, high-fidelity models of each enable verification against specification, including for safety.

The complexity of traffic, speed of vehicles, multiplicity of object types, required short reaction times in autonomous control, and the need to communicate among vehicles, infrastructure, and animate and inanimate objects to operate safely



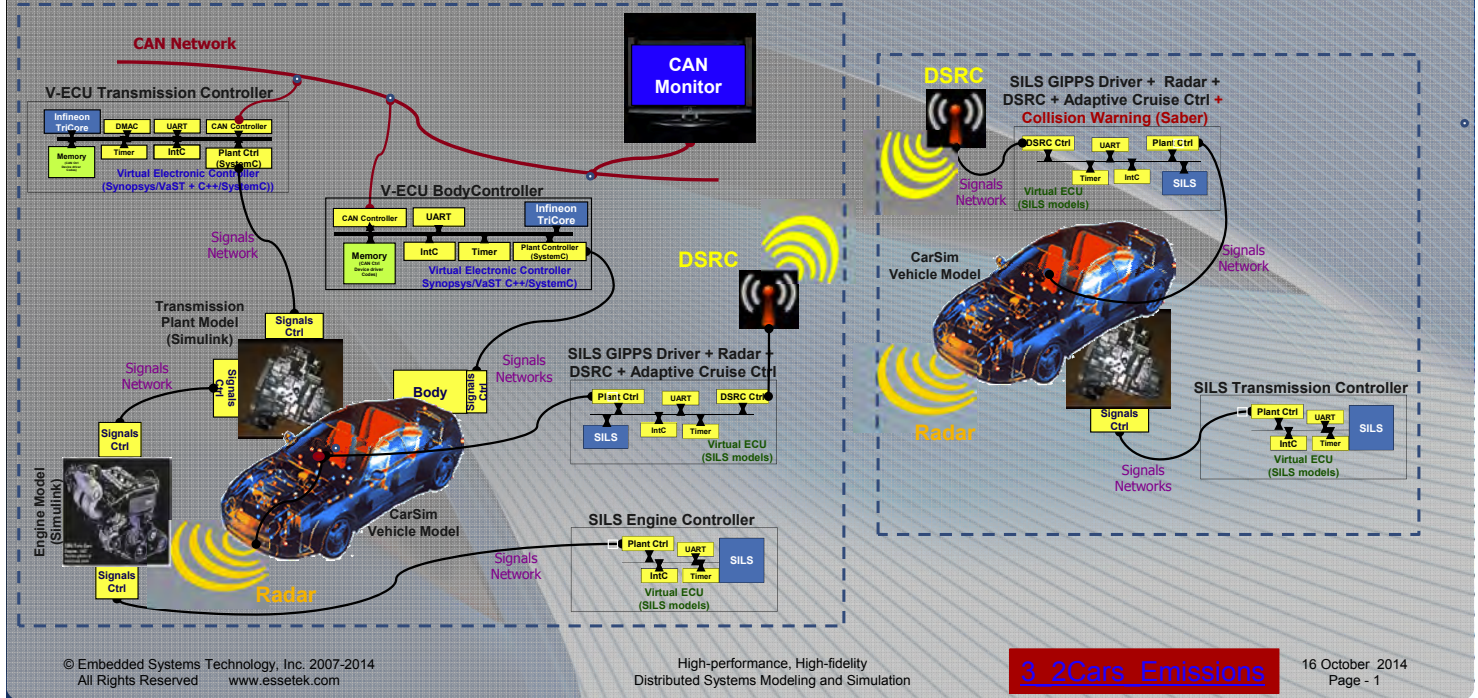
and to resolve prisoner dilemma scenarios may cause crashes rather than avoid them. Such dilemmas also apply to autonomous industrial vehicles. The terrain to be navigated by mining vehicles, together with their sheer mass leads to different driving reaction requirements and collision avoidance strategies – and thus different scenario and test cases.

Both categories of vehicles and control are subject to issues associated with communications technologies due to atmospheric conditions, as well as channel congestion – for wi-fi/DSRC in particular. The production of emissions is far more

serious than the incidence of death and injury due to collisions. So in terms of testing, in all cases cited above, the use of high-fidelity vehicle, terrain and communications models, together with high-performance simulation, enables the rigorous testing of both on-road and off-highway vehicles and traffic. To demonstrate systems, and systems of systems, safety the testing scenarios must include those where death and serious injury will result. In modeled systems, the degree of rigor in safety assessment and testing makes the incorporation of tests and scenarios that result in death *de rigueur*; on the

Communicating Systems of Systems (mobile) Safety & Mobility

EST



other hand, such testing involving physical systems and drivers is practically totally avoided due to reasonable societal taboos and cost.

iVT: How much redundancy/safety back-ups needs to be built in to production autonomous vehicles? This can be determined empirically with the use of statistics, modeling and simulation. No guesswork should be countenanced in the arena of autonomous vehicles.

The inputs for calculating safety include: (i) the expected failure rate distributions of individual hardware control, communications and plant (electrical, hydraulic, mechanical and thermodynamic) components, subsystems and systems and what the resulting physical failures and their effects will be; (ii) the expected distribution of software errors in control and communication code; (iii) the expected distribution of dynamic errors in cache, RAM and Flash memory causing random errors in software binary code; and (iv) the distribution of expected changes in all of the distributions in (i) & (ii) over time up to whatever limit in years is desired. The effects

ABOVE LEFT: Still's iGo intelligent automation solutions enable autonomous control of its production trucks

LEFT: Gottwald's battery AGVs were featured in iVT Advanced Lift-truck Technology International 2012

caused by software errors – both embedded and those caused by static or dynamic errors in memory devices – can be computed during simulation. It may be possible to build expected failure modes into the models of hardware components, their effects on subsystems, and their aggregated effects on systems – thereby, avoiding the tedium and errors of estimating these prior to simulation.

Certain statistical calculations can be performed manually with this approach. However, the complex interaction of probabilities over the thousands of components will require modeling and simulation, as will any dynamic behavior due to failures. In particular, the longitudinal studies over time will require a history of wear and tear on each component, and these will have an impact on the probability of component, subsystem and system failure over time – a task best suited to simulation.

Running 1,000,000 simulations, 1-10,000 at a time, on typical huge server farms, will be the norm for these studies. Each study may involve scenarios of simulated minutes to simulated hours. The resolution of time in the simulation will determine

the amount of computation required and hence the time taken to perform each simulation.

Calculation of failure and deduction of safety requires a considerable level of accuracy in both models and simulation. It is clear that for scenarios involving multiple vehicles, the parallelization of simulation is a requirement. For high-fidelity models, there's a further requirement to parallelize systems into subsystems and, likely, subsystems into components, while maintaining model accuracy and communication accuracy both between and within models. The requirement with high-fidelity models is to maximally speed up their simulation to minimize simulation run times. A high-fidelity vehicle model undergoing detailed risk analysis and safety assessments involving energy consumption, emissions and collision avoidance computations will require between 4 and 10 cores during simulation.

These studies will determine the unacceptable limits of safety guessed by chance (as the situation is largely, at present), safety by duplication, safety by intentional fault tolerance (say, triple multiple redundancy, hot

AUTONOMOUS VEHICLES

standby, etc). The measure of unacceptability is likely to be the rate of death and injury resulting in measured failures of thought-to-be safe systems.

ivT: How far down the road to fail-safe operation do you feel we currently are? Is the 'glass car' a viable aim?

The statistical studies outlined above indicate studies of fail-safe operations – even accounting for the effects over time of wear and tear – can now be undertaken. These studies will yield a vast data set of analytical data that is impossible to collect by physically testing and driving cars. Necessarily, the data produced by modeling and simulation needs to be compared carefully with measurement data from the field – at all levels. This has largely been done over the past five years for many components and subsystems, but not as yet for systems and systems of systems.

The empirical data sets provided by modeling and simulation, as in the aerospace industry, will directly impact what is considered safe design and this will lead to mandatory improvements in control system and plant design, and, consequently, communicating vehicle and traffic safety. Model and simulation driven specification, architecture and design are the keys to producing a glass car. Even with a glass car, over time it will inevitably develop cracks making it less safe. The determination then will be a very human one – when to get a new vehicle; or, based on the data, when the government requires you to buy a new safe vehicle. I prefer the latter.

ivT: So, what is the problem with DSRC exactly?

The three major issues are:

- Congestion in the wireless channels of DSRC communications. From our extensive simulations, channel congestion causes the inability of even close vehicles to communicate via wi-fi for 10-30 seconds. With the current standards, 100 vehicles within a radius of about 500m will congest the available wireless channels.
- Susceptibility of radio to terrestrial EM noise. In studies of physical vehicles communicating with physical DSRC infrastructure in an

RIGHT: Designed by Martin Rico (see p40) the UAC/ACU is a robot designed to reduce the unloading time of trucks

BELOW: Seegrid's GT10 robotic industrial tow tractor reduces manned travel time



“THE LEGISLATURE WILL BE DECEIVED AND SEDUCED BY TECHNOLOGY GIANTS WISHING TO PROMULGATE THEIR VISION OF MAKING MONEY AND SERVING SOCIETY”

industrial suburb of Sydney in 2009, the wi-fi channel was completely saturated by EM noise, making communication between vehicles and infrastructure impossible.

- Radio communication's susceptibility to atmospheric EM noise.

If DSRC is being used for collision avoidance, absence of communication for even a few seconds with vehicles approaching head on at 60mph is a problem. Inability to communicate for 10-30 seconds is very dangerous. DSRC to be used as the sole, or the main, sensor for collision avoidance is unacceptable. It must be coupled with at least two other sensors – video plus lidar or multiple radars at different frequencies – to be a major actor in safety.

DSRC's advantage is its ability to communicate useful information – such as, type of control system in use in an approaching vehicle – information that can be used in intelligent collision avoidance. Radar, lidar and video do not provide such information but this is critical for decision making about safety.

ivT: Is the main obstacle to widespread autonomous vehicle use currently legislative rather than technological?

In my book, it remains safety and safe engineering specification, architecture, design, verification and validation (*à la* aerospace).

The legislature is dominated by lawyers, accountants, ex-union delegates, bureaucrats. Asking the legislature to make complex,

intelligent decisions about safety involving the assessment of statistical, modeling and simulation data to back-up safety claims is not positively unsafe. There is insufficient data to make such decisions about safety as yet. Until the massive simulations involving safety take place, the data sets used to make decisions are sparse and inadequate.

The legislature will be deceived and seduced by technology giants wishing to promulgate their vision of making money and serving society.

Ironically, it was legislature that mandated the correct safe processes for engineering aerospace vehicles – and that took just a couple of thousand spectacular deaths every couple of years, or so. It seems the less spectacular 1,000,000 crash deaths per year and 10,000,000 thoracic, coronary and other medical deaths per year due to automotive engineering warrants less attention.

Data is required to foil this very unscientific mechanism of legislative decision making.

ivT: Can you outline a few key points of your presentation?

- The lack of adequate data sets to justify statements and claims about the safety of ordinary vehicles, let alone autonomous vehicles.
- The incipient nature of modeling, simulation and statistical analysis of dynamic systems in the automotive industry.
- The lack of legislative requirement to use modeling and simulation in Automotive in comparison with Aerospace, where it is mandatory. Interestingly, the latencies associated with collision avoidance and other critical control are much shorter in automotive vehicles than in civilian aerospace vehicles.
- Off-highway – with respect to modeling and simulation – is amenable to exactly the same tools and analyses as the on-road sector. **ivT**

BOOK ONLINE NOW!

3-DAY PASS €1,050 • 2-DAY PASS €950

www.autonomousvehiclesymposium.com

