




Elisabeth  
Uhlemann 

# Don't Worry: Connected Automated Vehicles Are Better Drivers Than We Are and They Will Not Break the Internet!

## Banning Connected Automated Vehicles or Offering Complicated Solutions to Imaginary Problems?

People have always feared new technology. In [1], the authors explain the impact that hours and hours in front of a screen, such as a smartphone, has on our brains, but also notices that all new technology was initially received with hesitation. They give several amusing examples: In the 16th century, we were told that all this new information being available to us now that books could be mass produced would overwhelm and flood our brains. In the 19th century, we were told that traveling above 30 km/h (18.6 mph) was unnatural and would lead to vomiting. A little later in the same century, we were told that the phone was a devil's invention, and will attract thunder, lightning, and evil spirits. Finally, in the 1950s, the TV was said to hypnotize its viewers and make them do insane things.

Rather than generating fear of the smartphone or advising against using it, the authors of [1], targeting kids as their audience, instead focus on how our changes in behavior, when interacting with smartphones, affect our health. No need to ban or stop using the smartphone, just think and act smart to use the benefits and avoid

the drawbacks. The same approach should be taken when considering autonomous vehicles. We should not expect autonomous vehicles to solve all problems with inattentive, drunk, or sloppy humans in the neighboring car, and ban them all if they fail. For me personally, it is still safer to be surrounded by autonomous vehicles with a high lowest level, a level that never brake any traffic rules, than by human drivers with a higher average behavior. Variations in humans are extensive. This is what we should be fearing: human errors, which can happen any time, even during perfect road conditions.

Connecting autonomous vehicles will make them even safer. The vehicles are then able to share sensor data to form situation awareness unattainable to the human brain. Worried souls will argue that this causes security problems. However, there is no need to connect the interconnected vehicles to the Internet. Sensor sharing can and should be done locally. If Internet is needed, it is better to let each individual vehicle have its own connection to the Internet, if and when desirable. Keep in mind that surfing the web does not need to be done using a vehicle as the platform. It can of course be done with the vehicle as user interface, but this type of connection should be clearly separated from the network interface providing traffic safety.

Similarly, upgrading the vehicle software, which can save hours and dollars in workshop costs, does not need to be done while traveling on the freeway. Just as you would not use the vehicle lidar to find a good nearby restaurant, you should not use the connected vehicle safety system to connect to the Internet. Keeping the different networks separate should be as intuitive as not using your lawn mower to buy items on Amazon.

Still, calming down the people worrying about the safety of autonomous vehicles or the security of connected vehicles is still comparably easy, as logical reasoning can be used and eventually this new technology will not seem so frightening. However, when considering a third group—the technical salespeople—it is not straightforward. I will still make an attempt of calming things down by addressing the latest worry: that connected vehicles will break the Internet by generating massive amounts data. Technical salespeople have produced a bunch of white papers seeking investments and spectrum in order to offer complicated solutions to this made-up problem. More on this below.

## Toward Autonomous Vehicles

### *Humans as the Main Cause of Accidents*

Waymo has reported one million miles without a safety driver with its

robot taxi. The summary of accident statistics is 20 collisions (or contact events), two of which required reporting to the National Highway Traffic Safety Administration. No human injuries are reported in any of the cases. All collisions with other vehicles are deemed to have involved a human who broke the traffic laws or drove carelessly. In 55% of all incidents, a stationary Waymo vehicle was hit from behind. Nine of the collisions resulted in no damage to any vehicle.

In the event with the highest severity of the 20 collisions, the Waymo vehicle was struck in the rear while slowing down for a red light, by a car driven by a teenager driver. The rearward facing video recording suggests the teenager was looking at a cell phone held near the steering wheel immediately prior to the collision.

### *Tesla Autopilot Not Responsible for Crash*

The National Transportation Safety Board (NTSB) has now completed its investigation of a run-off-road crash involving a Tesla model in April 2021. The NTSB found no evidence that Tesla's driving assistance, Autopilot, was being used at the time of the incident. Instead, the NTSB determined that the probable cause of the vehicle crash was the driver's excessive speed and failure to control his car, due to impairment from alcohol intoxication in combination with the effects of two sedating antihistamines, which resulted in a roadway departure, tree impact, and a post-crash fire.

Since 1968, the NTSB has issued nearly 150 safety recommendations addressing impaired driving, and the issue area "Prevent Alcohol- and Other Drug-Impaired Driving" is currently on the NTSB's Most Wanted List of Transportation Safety Improvements. Speeding is also one of the most common factors associated with motor vehicle crashes in the United States, and "Implement a Comprehensive Strat-

egy to Eliminate Speeding-Related Crashes" is another issue area on the NTSB's Most Wanted List. The NTSB has advocated for vehicle technologies, including passive vehicle-integrated alcohol impairment detection systems, advanced driver monitoring systems, and intelligent speed adaptation, to help reduce crashes caused by alcohol impairment and excessive speed. Requiring these technologies and/or incentivizing them through consumer information programs is necessary to achieve widespread installation according to NTSB.

## **Connected Vehicles**

### *Will Connected Vehicles Flood the Internet?*

There have been some statements recently—e.g., in a joint report by Global X ETFs and the *Wall Street Journal* [2] and by the Automotive Edge Computing Consortium (AECC)—that connected cars may "break the Internet." How do you break the Internet, one may wonder? According to a white paper by AECC [3], this will happen as 31 million vehicles with embedded forward-facing cameras will be sold in Western markets in 2025. Not so remarkable perhaps, but apparently these cameras will generate up to 10 Exabytes of data per day and this is to be processed by off-board resources [3]. This would indeed be a challenge, but why should forward-facing cameras generate data that need to be processed off-board? I have a backwards-facing camera on my car to help me check that I do not hit people, walls, or animals when reversing. Why would anyone want to save or process all of the data this camera generates and why do it at some off-board location? And, finally, why will a forward-facing camera be any different?

I do agree that the number of connected vehicles will increase and thereby likely also the amount of data that will be sent to the cloud or needs to be processed by edge units. However, I do not understand the doomsday

prophecy from AECC: "As the connected car market rapidly expands beyond luxury models and premium brands to high-volume, midmarket models, the industry will soon reach a tipping point. The volume of vehicle data generated will overwhelm existing cloud, computing and communications infrastructure resources" [4]. It is interesting that my view can differ so drastically from the authors' view. Since there are close to no references in the white paper explaining why the data generated by the sensors in the (luxury) cars would need to leave the car, I decided to check the considered application areas more carefully to determine where these massive data flows may occur and, more importantly, if these flows are indeed required for proper application functionality. The following five use cases are considered by the AECC in [4]: high-definition mapping, intelligent driving, insurance, V2Cloud cruise assist, and mobility as a service.

For maps, it is clear that it is not enough to be connected to nearby vehicles; a connection to the Internet is needed. However, the authors do realize, like the project SAFESPOT [5] already did many years ago, that building a local dynamic map will require a layered architecture. A static high-definition map can thereby be downloaded beforehand and complemented with regional information, which does not change that often, and finally information about surrounding vehicles, which can and should be obtained directly from the surrounding vehicles. In other words, no need to flood the Internet for this.

Regarding intelligent driving, the white paper authors realize that there is a need for onboard sensors and also sensor sharing between vehicles located nearby. However, for some reason, they seem to think it is necessary to involve the cloud. I am again quoting: "[o]ne goal is to give drivers a complete and dynamic picture of their driving profiles so that exhausted drivers in unsafe cars get off the road. Edge servers can instruct the

vehicle on what data to send to the cloud and help to preprocess the data before it is sent... .A driver monitoring his or her performance/alertness on a road trip is likely to move from one edge server's region to the next during the journey. The ability to transfer a data session from one edge server to another again becomes critical" [4]. Why would onboard sensors who detect lack of driver alertness want to inform the cloud? The exhausted driver is in the same vehicle as the sensors and thereby also the actuators, which can be used to alert the driver (like flashing dashboard lights, reducing the temperature, creating nudging sounds, etc.). Sending such personal data as drowsiness detection to the cloud and keeping some edge server busy determining which data to select to be sent to the cloud would not only imply an unnecessary delay, but would also entail a privacy and security risk without any foreseeable performance gain. Intelligent driving can be realized by using sensor information from onboard sensors and combining it with sensor data from nearby vehicles shared via vehicle-to-vehicle (V2V) communications. No need to involve the Internet for this as it is only locally available data that is of interest.

Regarding insurance, the authors conclude that insurance companies are interested in collecting driver data to reward good drivers and also to get information from accident areas. An example given is that drivers can be prompted to photograph skid marks on the road to document causes of accidents. However, driver monitoring data, should it be shared with insurance companies, does not need to be sent on an hourly or even daily basis, but rather as statistics of dangerous driving over a period of time. This is something that can be downloaded from a vehicle when, e.g., at a workshop service or when determining next year's insurance fee. Similarly, prompting drivers to photograph skid marks when accidents occur is not likely something that would lead

to breaking the Internet. Or at least, the communication intensity for insurance purposes is obviously lower than streaming services for home entertainment. The understatement you may detect here is indeed intended.

For the use case V2Cloud cruise assist, which is said to be "an evolution of intelligent driving into a more flexible service model," two cases are considered: a mechanism called vehicle-to-cloud-to-vehicle service (V2C2V) and expediting the process of moving information from the vehicle to the cloud. It is quite clear that V2V has a lower delay than V2C2V. Since a low delay is of essence for intelligent driving, a higher traffic safety will be obtained by not involving the edge, the cloud, or the Internet at all, and instead communicating directly with the vehicles within range using V2V. Thereby we also remove the need for coverage, as we do not require the presence of a base station. This in turn will make the system more fail-operational as a single point of failure (the base stations) is removed. For nonsafety cases, it is not straightforward to imagine why two vehicles in close proximity would communicate. The white paper suggests this "service scenario is especially effective when used to broadcast information to vehicles that need the same information, by utilizing the combination of neighboring vehicles, roadside units and others" [4]. However, since this presumably is traffic safety related information (or else roadside units would not be involved), it is still much easier to use direct peer-to-peer communication and transmit to all within range. A stationary roadside unit can collect information from cars that previously passed and broadcast the information downstream. That way, no advanced data processing is needed: all within range will receive the message, and all out of range are likely not affected by the information. The only other example of nonsafety data transfer involving roadside units I can imagine is commercials—informing about upcoming burgers—and again,

vehicle connectivity should not be used for this. Better to use the cellular network and mobile phones for this type of cruise assist.

The second case where V2Cloud cruise assist is argued to be useful is to move the massive amounts of data from the vehicle to the cloud. It remains to be shown where these massive amounts of data will come from. I do however agree with AECC as stated in [3] that the amount of data sent by a vehicle is on par with the amount of data that needs to be received by a vehicle, and thereby the upload speed is as important as the download speed for vehicular communications. However, I fail to see why we should expect any massive amount of data being uploaded or downloaded. When connecting a vehicle, we are connecting a system, not all of the individual sensors of this system. Any potential sensor sharing is done locally, e.g., from the vehicle in front or around an intersection, and thereby does not affect the Internet. In addition, as concluded already in 2011 [6], when the penetration increases, more and more processed data can be transmitted, and this will compensate for the increase in the collective bandwidth. We may need to interact with the vehicle from a distance or control it, but before any sensor data or vehicle state information is transmitted, sensor fusion is made. This sensor fusion is best done within the vehicle as the type of fusion needed is brand specific. The control decision that is transmitted to the vehicle is small as this is processed actuator data. Transmitting such processed data will require much less bandwidth.

The last use case is mobility as a service. As more and more vehicles connect, data connected to mobility as a service will increase, but will this increase be at a level or magnitude that would break the Internet? There is no high-definition video that needs to be shared, only app information about location. Already today, we keep track up buses and kickbikes. I would argue that a few more

connected shared vehicles or taxis is not going to be a game changer here.

The same way that the Internet is not one thing that can break, connecting a vehicle is not going to be made via just one link. We need different networks and connectivity points, depending on the data that is to be shared with the outside world. Very little data need to be shared outside the immediate surroundings of a vehicle, and even less needs to be processed by off-board resources. Therefore, we should not design our future networks to be able to cope with all of the data that is possible to generate if you add together all possible sensors in a vehicle. That is a worst case, which is unrealistic (like designing hardware for the possible case that the sun explodes). We should design our networks to handle services that are suitable to run over this or that particular network architecture. There is no need to spend money on reducing the delay of V2C2V, when V2V is faster. Also, there is no need to assign loads of spectrum to a technique that cannot handle all possible use cases. The different networks, personal, local, cellular, and Internet complement each other, and everybody loses when salespeople try to make them compete.

## Cellular Communications

### *Airplanes and 5G*

As has been the case in several other countries, the U.S. Federal Communications Commission proposed auctioning off bandwidth for 5G in 2018. However, in contrast to other places, the frequencies auctioned off were in the C-band. These frequencies can be close to those used by radio altimeters (RadAlt), an important piece of safety equipment in aircrafts. Because the proposed 5G deployment involves a new combination of power levels, frequencies, and other factors, and operate in proximity to air fields, the U.S. Federal Aviation Administration (FAA) has been forced to impose restrictions on flight operations using

certain types of RadAlt equipment close to antennas in 5G networks. As of July 2023, aircraft equipment must be “5G tolerant.”

The aircraft RadAlts give aircrafts information about current height from the ground and provide connectivity needed to, e.g., land in poor weather. Given the 5G deployment, time is running out for airlines to meet the proposed regulatory deadlines in the United States to retrofit or modify RadAlts. The modification is needed to ensure that the RadAlts will not suffer interference from 5G C-band transmissions coming from towers located near United States airports and approach paths. In January 2023, the FAA proposed an Airworthiness Directive, which gives airlines until 1 July 2023 to install new RadAlts or upgrade existing ones with new filters to utilize instrument landing systems at affected United States airports. Furthermore, from 1 February 2024, aircraft that have not been retrofitted with filters or new RadAlts will be banned from operating in United States airspace.

A temporary compromise was met in 2022 between the FAA and two 5G telecom providers, which avoided massive flight disruptions. Under the deal, the telecom providers AT&T and Verizon agreed to restrict power levels of their 5G C-band towers near airports and approach paths. That compromise is, however, set to expire in July 2023.

Although AT&T and Verizon have indicated a willingness to extend the informal agreement, maintaining their voluntary limits on transmitting power beyond the 1 July expiration date, there is not yet any such deal with the remainder of the telecom industry. In the same month, up to 19 additional telecom providers are expected to introduce 5G services in the C-band and they are not part of the existing voluntary deal. It should be noted that asking airlines to quickly invest huge amounts of money on the basis of an informal agreement is an inappropriate way forward. The

FAA estimates the cost of compliance at US\$26 million based on US\$26,000 per retrofit for approximately 1,000 aircraft. Since the frequency spectrum auction, which raised billions of dollars for the U.S. government, airlines have borne the cost of modifying thousands of aircraft to enable them to operate in the presence of 5G transmissions.

## Internet of Things

### *Commuter Trains Are Alerted About Earthquakes in California*

The new train alert technology utilizes the U.S. Geological Survey ShakeAlert system to automatically stop or slow Metrolink trains before impacts of shaking occur. ShakeAlert is an earthquake early warning system that provides important data within seconds of an earthquake being detected, including the earthquake’s location, magnitude, and estimated shaking, so people and systems can be alerted before the shaking begins. In case of an earthquake, an alert gets sent to the train control system, allowing the train to either slow down or stop in the event of an earthquake.

## References

- [1] M. Wänblad and A. Hansen, *Skärnhjärnan Junior*. Stockholm, Sweden: Bonnier Fakta 2021.
- [2] “Network overload? Adding up the data produced by connected cars.” Visual Capitalist. Accessed: Mar. 15, 2023. [Online]. Available: <https://www.visualcapitalist.com/will-connected-cars-break-the-internet/>
- [3] “Coordinating the connected car and network edge to avoid breaking the internet,” Automotive Edge Computing Consortium, Wakefield, MA, USA, White Paper, Oct. 2022. [Online]. Available: <https://aecc.org/wp-content/uploads/2022/10/white-paper-advancing-connected-vehicle-technology.pdf>
- [4] “Connected cars: On the edge of a breakthrough,” Automotive Edge Computing Consortium, Wakefield, MA, USA, White Paper, May 2021. [Online]. Available: [https://aecc.org/wp-content/uploads/2021/05/MWL\\_-\\_AECC\\_whitepaper\\_-\\_Design\\_v2.0.pdf](https://aecc.org/wp-content/uploads/2021/05/MWL_-_AECC_whitepaper_-_Design_v2.0.pdf)
- [5] SAFESPOT. [Online]. Available: <http://www.safespot-eu.org/sp3.html>
- [6] E. Uhlemann, “Communication requirements of emerging cooperative driving systems,” in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Las Vegas, NV, USA, 2011, pp. 281–282, doi: 10.1109/ICCE.2011.5722584.

VT