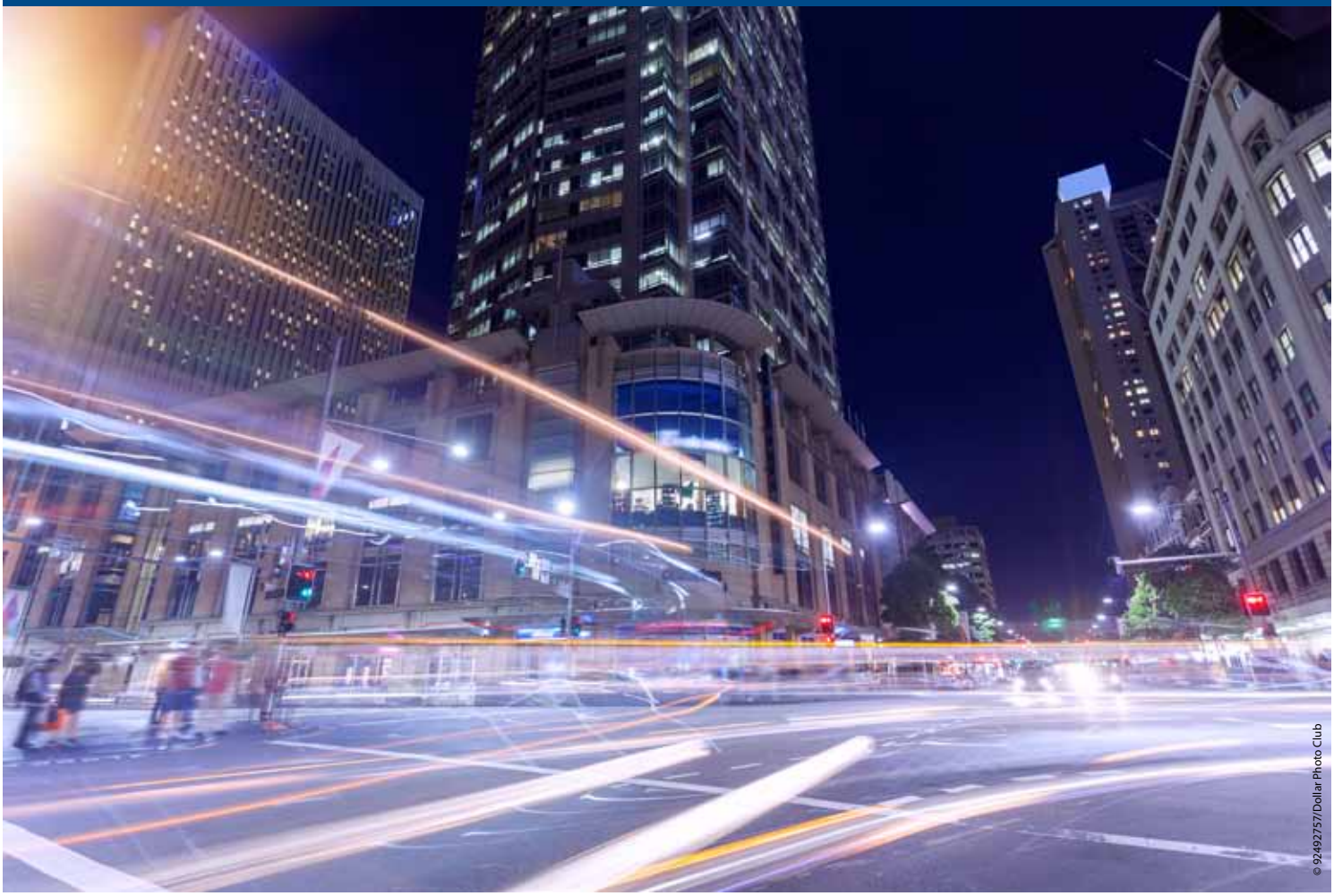
Following the Fault Lines in Autonomous Vehicle Designs



MOUSER ELECTRONICS

Following the Fault Lines in Autonomous Vehicle Designs

By Paul Golata, Mouser Electronics

Specialisation is the primary strategy for abstracting complexity into sets of manageable tasks. When a specialised task is sufficiently understood and encapsulated such that its input and output tolerances are well defined and can be reliably enforced, automating it can produce further productivity gains. One of the secrets to successfully automating a task is ensuring appropriate fault handling between each of the specialised processes, regardless of whether it is performed by a human or a machine.

Fully self-driving cars are perhaps the most ambitious examples of autonomous vehicles, including aircraft and spacecraft, to date (see Autopilot versus autonomous). Self-driving cars are conceptually no different from any other automated vehicle system except that they must not only be able to proficiently operate the automobile but successfully execute contextually relevant collision avoidance and rerouting autonomously in real-time. To date, no commercially available automated vehicle system accomplishes this ambitious goal in all normal operating environments.

Navigating Through the Systems

The National Highway Safety Administration (NHTSA) and Society of Automotive Engineers (SAE) have each published a formal classification system for automated vehicles. The NHTSA 14-13 system focuses on the capabilities of the vehicle control system and its ability to relieve the driver of driving responsibility.[1] The SAE system is based on the amount of driver intervention and attentiveness required. Each level is briefly described below.

The NHTSA system defines five levels, (Level: 0, 1, 2, 3, 4), of vehicle automation:

Level zero (0) places the driver in complete and sole control of the vehicle at all times.

Level one (1) encompasses vehicles with one or more specific control functions, such as electronic stability control or pre-charged brakes, where the vehicle assists the driver to regain control of the vehicle faster than possible by acting alone.

Level three (3) automation includes automobiles that enable the driver to cede full control of all safety—critical functions—under certain conditions—to the vehicle. The vehicle monitors and notifies the driver when the control needs to transition back to the driver. The driver is expected to be available for occasional control, but with a comfortable transition time.

Level four (4) represents the ultimate goal of self-driving vehicles that are able to perform all safety-critical driving function and monitor roadway conditions for an entire trip. It is assumed the driver, if any, will provide destination or navigation input, but is not required for control of the vehicle at any time during the trip.

The SAE standard, J3016_201401 defines six levels, (Level: 0, 1, 2, 3, 4, 5), of vehicle automation (Figure 1):[2]

Level zero (0) maintains that the driver is responsible for all aspects of driving, but the vehicle can provide automated warnings.

Level one (1) expects the driver to be able to perform all driving tasks at any time, but be able to take advantage of assistance systems for steering or acceleration/deceleration systems such as cruise control, lane keeping, and parking assistance systems.

Level two (2) requires the driver to be able to detect when to take control over of any active automated system.

Level three (3) permits the driver, under limited conditions, to safely focus on tasks other than driving, but to be ready to take over when notified by the vehicle.

Level four (4) expands the scenarios that the automated vehicle can safely operate, but requires the driver to determine when it is safe to do so. If the vehicle automation is appropriately activated, the driver may place their attention elsewhere.

Level five (5) requires no human intervention except to start the system and provide a destination.

SAE Automated driving levels as defined in standard J3016. Source: SAE

Level Set Expectations

Driving a vehicle involves decisions based on potentially hundreds of such as speed of travel, time of day, and weather. Both the NHTSA and SAE automation taxonomy systems define a spectrum of shifting responsibility between the driver and the automated vehicle control system. However, while each automation level is a subset of the higher levels and builds up the capabilities that the automated control system can handle, there is an opposite reduction in requirements for the driver.

The numbering of the levels suggests a ranking of complexity, but a vehicle operating in a highly controlled environment at slow speed could conceivably operate at the higher levels of automation and be completely inappropriate for operation in any other environment. An example of an automated system could be an inventory picker robot. This is a robot that operates in a controlled environment and can quickly move through its inventory to select the desired items and deliver them to an interface point. Within the controlled confines of the picker robot, the picker mechanism can move freely and quickly without worry of collision or of hurting someone. Fail-safe interlocks prevent the robot from operating when there is someone inside the robot's operating area.

In practice, a driver and automated vehicle may be operating together across multiple levels for a given subset of driving functions and environmental conditions. The mutually exclusive nature of the automation levels does not easily accommodate dynamic shifting back and forth between the levels. In fact, as the automation level increases—but short of the highest level of full automation—the driver holds the final responsibility for the vehicle. They must know more and more about the conditions that the automated system can safely operate in to responsibly decide when to activate and deactivate it.

It is for reasons like these that as the level of complexity and capability of an autonomous vehicle system increases it becomes more important for the system design and operation to focus on how the human operator and the autonomous system communicate and collaborate with each other. This communication and collaboration is especially important in the detection and response to faults or unanticipated driving conditions.

SAE level	Name	Narrative Definition	Execution of Steering and Acceleration/ Deceleration	*Monitoring* of Driving Environment	Fallback Performance of *Dynamic Driving Task*	System Capability *(Driving Modes)*
***Human driver* monitors the driving environment**						
0	**No Automation**	the full-time performance by the *human driver* of all aspects of the *dynamic driving task*, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a
1	**Driver Assistance**	the *driving mode*-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	Human driver and system	Human driver	Human driver	Some driving modes
2	**Partial Automation**	the *driving mode*-specific execution by one or more driver assistance systems of both steering and acceleration/ deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	**System**	Human driver	Human driver	Some driving modes
***Automated driving system* ("system") monitors the driving environment**						
3	**Conditional Automation**	the *driving mode*-specific performance by an *automated driving system* of all aspects of the dynamic driving task with the expectation that the *human driver* will respond appropriately to a *request to intervene*	System	**System**	Human driver	Some driving modes
4	**High Automation**	the *driving mode*-specific performance by an automated driving system of all aspects of the *dynamic driving task*, even if a *human driver* does not respond appropriately to a *request to intervene*	System	System	**System**	Some driving modes
5	**Full Automation**	the full-time performance by an *automated driving system* of all aspects of the *dynamic driving task* under all roadway and environmental conditions that can be managed by a *human driver*	System	System	System	**All driving modes**

Figure 1: SAE Automated driving levels as defined in standard J3016. Source: SAE

Automation at What Cost?

Automation is only worthwhile if it reduces the cost of performing a task. The reduction in cost can come in many forms. In factory settings, there could be a reduction in the amount of manpower needed to produce a given volume of product. In extreme environments, automation can enable necessary tasks to be performed that are too dangerous to be performed by a person. For vehicle environments, automation can help make operating the vehicle safer. However, automation by itself does not make operating a vehicle safer; rather, the improvement in safety often comes from freeing up the operator's cognitive load so that they can focus more of their attention on higher value tasks.

For example, rather than an aircraft pilot using precious cognitive capacity focusing on keeping the plane level, an autopilot enables the pilot to spend more time and energy performing troubleshooting to resolve a fault before it becomes a failure, or scanning the environment for upcoming hazards and planning on how to avoid them. The automation levels specify a shrinking cognitive load on the driver as the level increase, but as long as the driver is responsible for taking over the vehicle at any time, there is a real risk that the driver will be unprepared to respond in a timely fashion to an emergency condition that the automated control system does not know how to handle. Airline pilots repeatedly undergo training for known possible fault conditions and they typically have several minutes after the autopilot flags a problem to figure it out and take corrective action. In contrast, when a problem arises in an automobile, the driver may only have a few seconds, less than the typical human response time, to respond to an emergency that they have no prior experience handling.

A well-designed interface between the driver and the vehicle control system can help prevent the driver from becoming bored and letting their attention drift from the road. As long as the driver retains the ultimate responsibility for the vehicle, the vehicle needs to be ensuring that the driver is receiving relevant situational awareness of what the control system is doing, what it is planning to do, and why it is planning to do that. The vehicle should be continuously updating the driver with the results of its self-health checks, and informing the driver when and why its decision making is less than 100% certain.

This could free up the driver to focus on contextual awareness that the vehicle control system currently has no capability in. It would also permit the driver to focus on unusual changes in road conditions, communicating and negotiating with other drivers, adjusting to rapid speed changes, understanding the intent of other driver's by focusing on their "telegraphing" (for example: wheel position), and understanding how the decisions the vehicle control system is making is affecting the other drivers on the road so that they can also avoid colliding with you.

If the driver and vehicle are working in a collaborative manner, it becomes easier to understand how the vehicle is performing on the road and to discover the best ways to introduce new software capabilities. This last point is critical until automobiles become completely independent from the driver/passenger because the vehicle control system must evolve with the dynamic environment that defines driving. Lessons learned must be pushed out to existing cars via regular software updates, especially as the design team learns how to shoulder more of the decision responsibility for when it is appropriate for the control system to remain in control of the vehicle.

A vehicle does not need to be able to fully self-drive under all road conditions. The way to get a vehicle to perform any tasks in a fully autonomous, and possibly unmanned manner, is to make sure that it can reliably identify when it is operating under the correct set of road conditions and enable it to decline activating full self-driving when it cannot safely handle the current situation. If the set of conditions it can successfully operate is large enough to be useful it will be a valuable system even though it cannot operate under all conditions.

References

http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+Department+of+Transportation+Releases+Policy+on+Automated+Vehicle+Development

http://standards.sae.org/j3016_201401