1

Safety Expectations for Consumers, OEMs, and Tier 1 Suppliers

Every business involves sales based on customers trusting that their expectations will be satisfied. This trust by the customer is based on a belief that ethical business practices are the norm and not the exception. The customer expects to be satisfied and receive value for money. No one expects to buy disappointment, and the global automotive business is no different in this regard. To some extent, the belief in ethical business practices is supported by the observance of regulatory enforcement. Media coverage of investigations and recalls adds credibility to this belief. Consumers believe that being treated ethically is a right, not a privilege. There are consumer expectations of performance, prestige, and utility. Part of this utility is trustworthiness.

Trustworthiness

Trustworthiness includes quality, reliability, security, privacy, and safety, and expectations of trustworthiness are increasing. Advocates of quality publish competitive results for quality among competing automotive vehicle suppliers. Competing vehicle suppliers reference these publications in marketing campaigns targeting consumers' belief that they are entitled to the highest quality for their investment in an automobile. Fewer "bugs" in new cars are expected; taking the vehicle back to the dealer in two weeks due to an initial quality defect is no longer acceptable to automotive consumers. The consumer expects improved reliability to be demonstrated by longer life with fewer repairs. Consumers review warranties for length and coverage as a way to improve their confidence that potential future maintenance expense will be manageable. Comparisons are made of warranty repairs to support purchasing decisions. Consumer advocates track reliability for this purpose; it is a product differentiator.

When they purchase a vehicle, consumers expect that the vehicle will be secure and robust against cyber attacks. No loss of service availability is expected due to hacking of vehicle systems. Security of entry mechanisms is expected to be robust against cyber attacks by potential thieves. Even though successful hacks are in the news, it is expected that security considerations sufficient for lifetime protection are included in the vehicle design. If updates are needed, no intrusion or loss of availability is acceptable. Privacy of personal information is expected to be protected, even if some information is used to provide vehicle

Automotive System Safety: Critical Considerations for Engineering and Effective Management,
First Edition. Joseph D. Miller.

service. Ethical treatment of data concerning driving behavior, locations visited, and frequently used routes is expected. Permission to share this data may not be assumed. Privacy is considered a right, and enforcement is expected.

Perhaps most important are expectations of safety. Even when advanced convenience features are included in a vehicle, the consumer expects that there is no additional risk. The risk of harm is expected to be the same or less than it was before the features were added. When consumers acquire and operate an automobile, they are demonstrating an acceptance of the risk of operating the vehicle based on the current state of the art, and this state-of-the-art assumption does not include an assumption of increased risk. Consumers may not cognitively be accepting a state-of-the-art risk – they may not even be aware of what the state-of the-art risk is at the time of purchase. Nevertheless, they accept it by their actions. They purchase the vehicle knowing that there is a risk of harm when operating a road vehicle. This indicates accepting state-of-the-art risk.

Consumers have an expectation of safety. What is this expectation? How can risk be determined to be consistent with the state of the art at the time of purchase? This determination depends on the definition of *safety* and how that definition is employed in automotive practice. There are several candidate definitions to consider. *Safety* has been discussed as meaning "no accidents." This is aspirational; consumers are expected to welcome the freedom to operate a vehicle without the risk of accidents, especially if such freedom from accidents can be achieved at a reasonable cost. While useful for some analysis [1], the current state of the art for automotive vehicles has not yet advanced to this stage. Convenience features are being added to move in this direction, and vehicle manufactures reaffirm such shared aspirations in their marketing campaigns. The news reports on progress and setbacks along the journey to reach this aspirational goal of automotive technology. Clearly it has not been achieved – it is not yet the state of the art for automotive safety. Still, consumers purchase vehicles knowing there is a risk that they may have an accident and die while driving a vehicle, and they drive anyway. They accept this risk by their actions. Consumers know there is a risk of death to their loved ones who travel in the vehicle they purchase. Still, they drive their loved ones – they have accepted the risk.

Another definition of *safety* is "absence of unacceptable risk" [2]. The definition may be applied in any situation or scenario, whether related to the automotive industry or not. In this definition, safety is not absolute; the concept of risk is introduced. *Risk* is defined as the combination of the probability of harm and the severity of that harm. *Harm* is defined as damage to persons or, more broadly, as damage to persons or property. *Acceptable* in this context is ambiguous in that it implies that someone defines what risk is acceptable.

A similar definition is the "absence of unreasonable risk" [3]. This definition is also used in non-automotive scenarios or applications. However, it is the definition chosen for the functional safety standard used in the automotive industry. It seems reasonable to conclude that the consumer accepts that the risk is not unreasonable if they purchase or drive the automobile. While the consumer prefers the risk did not exist at all and that there were never any automotive accidents, by their actions they have shown that they consider the risk not unreasonable when considering the benefits provided by driving. This is the basis for the automotive functional safety standard, ISO 26262.

To not be unreasonable, the risk must not violate the moral norms of society. These moral norms may change over time, as do the expectations of consumers. However, the norms of society are not aspirational. Recalls occur if it is discovered that these norms might be violated

due to an issue with a vehicle. Since the current rates of various accidents, including fatal accidents, are the norms of society at the time a vehicle is purchased, they define reasonable risk for the consumer. Consumers decide the risk is not unreasonable when they make the decision to purchase a vehicle. The consumer does not expect that the vehicle will put people at a greater risk than other cars already on the road do – the consumer does not expect to purchase a defective or an inherently unsafe vehicle. Rather, the consumer expects the risk to be the same or less, depending on information they have received through the media or dealership concerning the new state-of-the-art features that are included. Even new features that do not have data to confirm their safety, from years of experience on public roads, are expected to improve, not diminish, the state of the art with respect to safety. Consumers consider this not unreasonable. They consider this safe.

Consumer Expectations

The consumer may choose to purchase a vehicle differentiated by advanced driver-assistance features not yet included on all the vehicles in service. Even if these advanced driver-assistance features are available for vehicles on the road, there may not be sufficient data to determine the risk to society of these features. Improvements and additions may be made to these features, or there may be more interactions of these features with other automotive systems that have the potential to cause harm. Now the expectations become less clear because they are not based on data that includes the influence of these advanced systems.

Expectations are influenced by advertising, news data about similar features, and personal experience. There has been much in the news about automated driving without these vehicles being broadly available to consumers. Still, expectations are being influenced by information provided by the media. Media reports of fleets of automated vehicles raise awareness of the many successful test miles as well as any errors or accidents that are publicly reported. This information may raise or lower expectations of advanced driver-assistance features that have some similarity to automated features. Automated vehicles have control of steering systems and braking systems in a manner similar to emergency braking and lane-keeping assist systems. Some clarifications might be discerned from the media, which explains the expectations of driver responsibilities and awareness. Expectations of the automated system are clarified; the capability of assistance has limitations.

Nevertheless, such publicity can have the effect of increasing consumer expectations regarding the performance of advanced driver assistance systems (ADAS) that are available. The more publicity there is about automated driving successes, failures, improvements, and goals, the greater the anticipation of its availability. The anticipation of available automated driving features may distort the understanding of the capability of more-limited features. This has been discussed as leading to a cyclic variation in consumer expectations based on experience. The consumer may not fully appreciate the nuanced limitations of an ADAS.

For example, the consumer may initially have high performance expectations for a follow-to-stop radar cruise control system. The consumer expects the system to perform as the driver would perform in all circumstances. This is reinforced by the early experience of having the vehicle slow to a stop automatically while following another vehicle. Gradually this experience leads the driver to not hover a foot over the brake pedal: the driver observes but does not intervene, and confidence starts to build. Then the driver mistakenly expects the Doppler

radar cruise control system to stop for a vehicle that was not being followed and that is sitting still at a traffic light. This is consistent with the behavior expected from a human driver. However, the ADAS does not respond because it ignores stationary objects in its field of view that are not being followed, like bridges and trees. This is a technical limitation of the system but is consistent with the requirements of the design. The consumer's mistaken expectations are not satisfied, and the consumer's opinion of the product becomes less favorable.

The expectations of the consumer are not consistent with the required capability of the ADAS. Further, the system sometimes mistakenly brakes when the vehicle in front slows and then changes lanes. The vehicle in front appears to disappear, consistent with the appearance of a stopping vehicle. Consumer sentiment drops further.

The consumer's experience continues with more successful following, acceleration, and proper behavior when changing lanes. In these scenarios, the ADAS reacts in much the same way as a human is expected to react. The consumer's expectations now are being calibrated. The consumer is ready to intervene when the ADAS's limitations are exceeded but does not intervene when the system is capable of handling situations successfully. Overall, the consumer does not feel the risk is unreasonable. The ADAS is not an automated driver, and it will not handle every situation like a human driver. However, it is pretty good; it seems safe.

Unless the consumer has confidence that their expectations of safety are satisfied by a vehicle, they will not purchase that vehicle. This confidence may be influenced by publicity, publicly reported performance and performance comparisons, and word of mouth. It is clear that consumer expectations of safety are critical to the automotive business, because the safety concerns of potential customers can severely limit sales of a vehicle. Tremendous resources are deployed not only to influence these expectations, but, more importantly, to satisfy them.

Vehicle manufacturers (VMs) expend resources to promote the advances they have made to improve crashworthiness. They spend vast resources to continuously improve the crashworthiness of the vehicles they intend to manufacture. Resources are provided to support development of improved passive safety systems to protect occupants and pedestrians during an accident. Included in these resources are not only provisions for development engineers, but also resources for engineering quality, safety management, and execution of the safety process. These resources are deployed by both the original equipment manufacturer (OEM) and suppliers. Each has its own process and resources to ensure the safety of its own products. They may share and coordinate resources for joint development of safety-related systems; safety resources must be managed effectively in both individual and joint developments. Effective management of a safety organization is discussed in Chapter 2, where evaluation criteria and alternative organizations are evaluated that may be considered equally by OEMs and suppliers. Both the OEM and the supplier have safety requirements to define and must comply with these safety requirements. Regulatory agencies and customers expect this – these expectations must be satisfied.

OEM Expectations

Safety expectations for the OEM or VM go beyond the vehicle not placing the consumer at unreasonable risk. This is only the minimum requirement for a safe vehicle as defined. Evidence of fulfilling this minimum requirement supports confirmation of diligence by

the OEM. The OEM accepts responsibility for this expectation and seeks in addition to differentiate the vehicle in the marketplace by further reducing the risk to the consumer. The VM strives to attain this goal by providing additional resources for continuous improvement in the performance of the safety-related content of the vehicle. This is a resource-consuming and challenging task. Research can be performed to identify areas of opportunity where resources may best be deployed. Realistic goals are established and promoted as future capabilities for the enterprise; these goals can then be used to derive specific objectives for product development engineering to achieve within a specified time period. This allows development to be planned for and resourced, taking into account both the specified time and the process used by the enterprise to ensure that the safety requirements are identified so compliance will be achieved.

Third parties independently rate vehicle "safety" by measuring crashworthiness as well as performance of various ADAS featured on the vehicle. Crashworthiness is evaluated using specific tests to determine the safety margin achieved by the design under repeatable conditions, as well as the absence of potential hazards previously determined, such as ensuring the safety of infants in car seats. ADAS features evaluated include emergency braking for both forward driving and backing the vehicle.

OEMs develop requirements for the vehicle design, specify features to be included, and identify requirements for these features. System safety plays a major part in determining these requirements. For example, it may be determined that to improve safety-related features, the vehicle will contain a safety feature that detects pedestrians approaching the front of the stopped or moving vehicle and that automatically stops the vehicle to avoid a collision with the pedestrian. Requirements at the feature level include the proximity of the pedestrian, scenarios in which the vehicle will be stopped, scenarios in which the vehicle will not be stopped, and a degradation strategy in case of failures. These requirements may be developed by the OEM, jointly with suppliers, or by the suppliers themselves. Arbitration of the priority of a vehicle request from this feature compared to requests from a stop-and-go cruise control or the driver are resolved between the VM and suppliers. Integration of the features may be executed by the OEM or delegated to a "turnkey" capable supplier. Such a supplier may supply multiple safety-related systems, or have the capability to supply other safety-related systems, and can employ this detailed domain knowledge to determine a safety policy for arbitration. Such a policy may require validation as described in ISO PAS 21448. Then the VM supports the validation plan. The VM assumes ultimate responsibility.

The OEM expects evidence that these tasks are complete and ensure safety, e.g. a safety case. This evidence includes proof that the relevant standards have been satisfied by the process employed to complete the tasks. There should be evidence that sufficient analyses have been performed to provide confidence that the requirements are complete because of the systematic elicitation of requirements through safety analyses. The OEM also expects the vehicle to meet regulations applicable to the performance of included systems. For example, if a stability control system is included, then regulations concerning stability control for each nation in which the vehicle is to be offered must be met. There may be regulations concerning ADAS that also need to be met. Meeting these OEM safety expectations helps ensure that consumer expectations are met.

The consumer may not be aware of the systematic methods employed to elicit and verify safety requirements; they also may not be aware of the tests performed to prove that the

applicable regulations have been met (although some testing may be presented in advertisements). Nevertheless, these systematic methods help ensure that only safe, fault-free systems are released to the general public. Success in meeting these safety expectations can be achieved by completely determining the safety requirements and completely complying with them. Requirements must be met for the entire vehicle life cycle: the concept phase, design phase, and verification phase, as well production and safety in use, in repair, and even in disposal. The safety lifecycle will be discussed in Chapter 6; it can be tailored for each project, and the scope may change.

Supplier Expectations

Tier 1 suppliers – suppliers providing systems directly to the OEM – expect to provide systems that meet the expectations of the OEM, if the OEM meets the underlying assumptions that are the basis of the design requirements for these systems. For example, a tier 1 supplier may assume that the OEM will limit the braking command of a cruise control system to a safe level in the braking or engine management system. The tier 1 supplier may also assume that the OEM checks messages for transmission errors and takes a safe action. These assumptions are necessary because tier 1 suppliers must develop their technologies in anticipation of future OEM expectations. Such advanced technology development by the supplier may take much longer that the time allowed by the OEM for sourcing systems for a vehicle to be launched in a specified model year. Tier 1 suppliers' scheduling must take into account the lead time to develop the baseline technology needed for the system to be provided by the supplier.

For example, a supplier of a radar cruise control system must develop the essential product technology before the supplier can support a vehicle launch schedule for an OEM. Antenna technology for the frequency band and field of view require extended development time. Encoding the radar transmission to support specific detection goals also requires basic development to be suitable for production intent concepts. The supplier must perform safety analyses to determine the safety requirements, and evidence is required for compliance with these requirements. Compliance with some requirements is assumed based on assumptions for the OEM, such as vehicle behavior in case the system indicates an internal fault, mounting alignment, and an unobstructed field of view. The OEM must confirm these assumptions, or equivalent assumptions and measures need to be agreed on before sourcing. For example, external detection of a faulty system by another tier 1 supplier may be managed by the OEM. These assumptions by the supplier become requirements for the OEM. Evidence of verification is needed for the OEM safety case; this evidence is traceable to the assumption, and compliance is expected.

Further expectations of suppliers and OEMs are supported by standards such as ISO 26262. This standard provides requirements for the roles of the supplier and the customer that support the joint development of safety-related systems. Sharing safety analyses, the resulting safety-related requirements, and other work products is specified for joint development. Collaboration by OEMs and suppliers while creating standards helps to vet the standard and support completeness of the requirements with respect to the standard's scope. OEMs from many nations participate in determining these requirements with tier 1

and tier 2 suppliers internationally. In the case of ISO 26262, the scope is limited to road vehicle functional safety.

Functional safety is the safety of the system as related to functional failures. The difference between this and system safety will be discussed in Chapter 3. Nevertheless, the standards are intended to provide a common language and frame of reference for OEMs and suppliers. This frame of reference includes evidence of compliance with standard requirements, such as work products. OEMs and suppliers agreed in ISO 26262 to have a development interface agreement (DIA) to structure the work and exchange of information concerning functional safety. The DIA is framed in the context of customer expectations, which will also shape the requirements for system safety and influence the expectations of both parties of the DIA.

Consider Figure 1.1, which illustrates critical safety considerations that could be easily overlooked. Consumer expectations for a new vehicle are top center and the highest

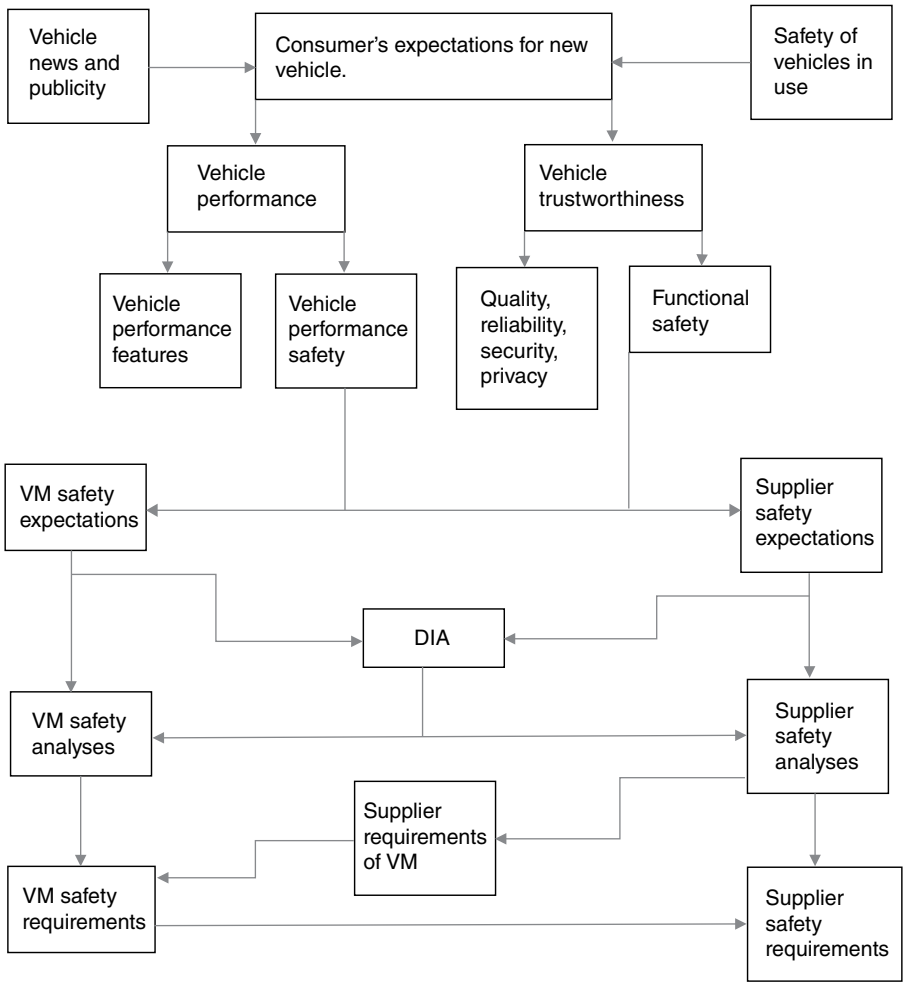

Figure 1.1 Flow of expectations concerning automotive system safety.

priority. These expectations of improved vehicle safety only contribute to the safety of vehicles in the field if the OEM and suppliers satisfy those expectations sufficiently that the consumer purchases the vehicle. Therefore, the influence of information about vehicles in the field as well as from publicity is a logical driver of these expectations. Often, advertisements demonstrate the advantages of new active safety features: for example, an accident is avoided because of an action taken by the advanced safety system. On the other hand, the news may report the failure of an autonomous system in a particular scenario, as well as the overall reduction in accidents due to advancements in safety systems.

Figure 1.1 shows that expectations of consumers include input to the vehicle's performance and functional safety. These expectations are made known to the VMs and suppliers through buying preferences for advanced systems of one VM over those of another VM. Information published about reliability and privacy as well as security and quality also influences consumers' purchasing preferences. These preferences are a fundamental input that shapes the goals that VMs and suppliers expect to achieve. This input is included in the collaboration between tier 1 suppliers and VMs. Suppliers compete to differentiate the features of the systems they supply based on their ability to satisfy consumer demands.

Shortcomings identified by consumer feedback to VMs are also acquired by tier 1 suppliers and used to guide improvements in subsequent systems. This fosters greater collaboration between VMs and suppliers. In order for this collaboration to meet the expectation that the vehicle is as safe as vehicles in the field, the standards that provide guidance to achieve the safety of vehicles in the field must be taken into account. Figure 1.1 shows the DIA as referenced in ISO 26262. It provides guidance for supplier selection as well the roles each collaborating party plays. All members of the relationship strive to meet the requirements and meet consumer expectations.

So, what critical aspects may be overlooked? Consider the following list:

1) Calibration of consumer expectations for vehicle features considering vehicle news and publicity. Limitations of performance and availability are communicated: for example, availability of the system may be limited, or it may be automatically switched off in inclement weather. System performance may not be sufficient to maintain the vehicle's position in the lane during high-speed or sharp-radius curves.
2) Determining field data related to vehicle features and ensuring that safety is not worse than that in the field. Accident data is a source of such information and can be obtained, for example, from the National Highway Traffic Safety Administration (NHTSA) National Automotive Sampling System (NASS) General Estimates System (GES). This data can be used to determine the risk of certain accidents and the severity of injuries in the field.
3) Including safety of the intended function (SOTIF) in the DIA or equivalent. SOTIF is out of scope for ISO 26262; ISO PAS 21448 [4] discusses SOTIF. From this publicly available specification (PAS) requirement, tasks can be derived and assigned to each party to establish and achieve the goals of the PAS. These could include determining sensor limitations as well as establishing and executing a model and vehicle-based validation strategy.
4) Systematic safety analyses by both the VM and supplier, e.g. architecture and software, and sharing the assumed requirements with each other. These may include failure

detection and performance during a failure. The analyses may include a hazards and operability study (HAZOP) of the system architecture as well as the software architecture so the parties can systematically agree on a failure-degradation strategy. Modifications may result from the analyses.

These are critical considerations because they relate to safety requirements. Considering these demonstrates diligence with respect to protecting consumers and other users of public roads.

These requirements all flow from consumer expectations but are easily overlooked because they appear to come from independent sources. Customer expectations, accident databases, independent standards, and systematic safety analyses may seem to be unrelated. For example, an engineer may look at customer requirements and assume that they are complete. The customer requirements are extensive and cover performance requirements, the product concept, and perhaps some design-specific details. Verification requirements and validation requirements are also addressed. Eliciting requirements from systematic software architectural analyses is not required to comply with these extensive customer requirements. Nevertheless, to meet societal norms, such analysis of systems in the field is required, to avoid unreasonable risk. Similar systems in the field may have had such systematic analyses performed to increase confidence that the requirements are complete. The analyses demonstrate that actions were taken to ensure compliance with requirements; this is a reasonable expectation. Requirements, elicitation, and management will be discussed in Chapter 8.

Engineers install failsafe safety mechanisms as a safety system is designed and not as a result of systematic analyses. The original system concept may include safety mechanisms that are deemed appropriate; such safety mechanisms are at different levels and provide redundant protection. Good engineering judgment is exercised, but not in the context of what is expected as described previously. It can be difficult to show that all required safety mechanisms have been included: experience, rather than systematic analyses, may be a basis for this judgment, and the measures may have sound reasoning. Faults are inserted, and the correct operation of the safety mechanism is demonstrated. This verification of the safety mechanism is traceable to the safety mechanism requirement. Nevertheless, the evidence of completeness illustrated in Figure 1.1 is not available. It can be difficult to support with high confidence an assertion that there are no missing requirements. Such confidence of completeness comes from a structured requirements elicitation method rather than judgment alone. Systematic safety analysis is an accepted method to perform this elicitation: this is a critical consideration for system safety.