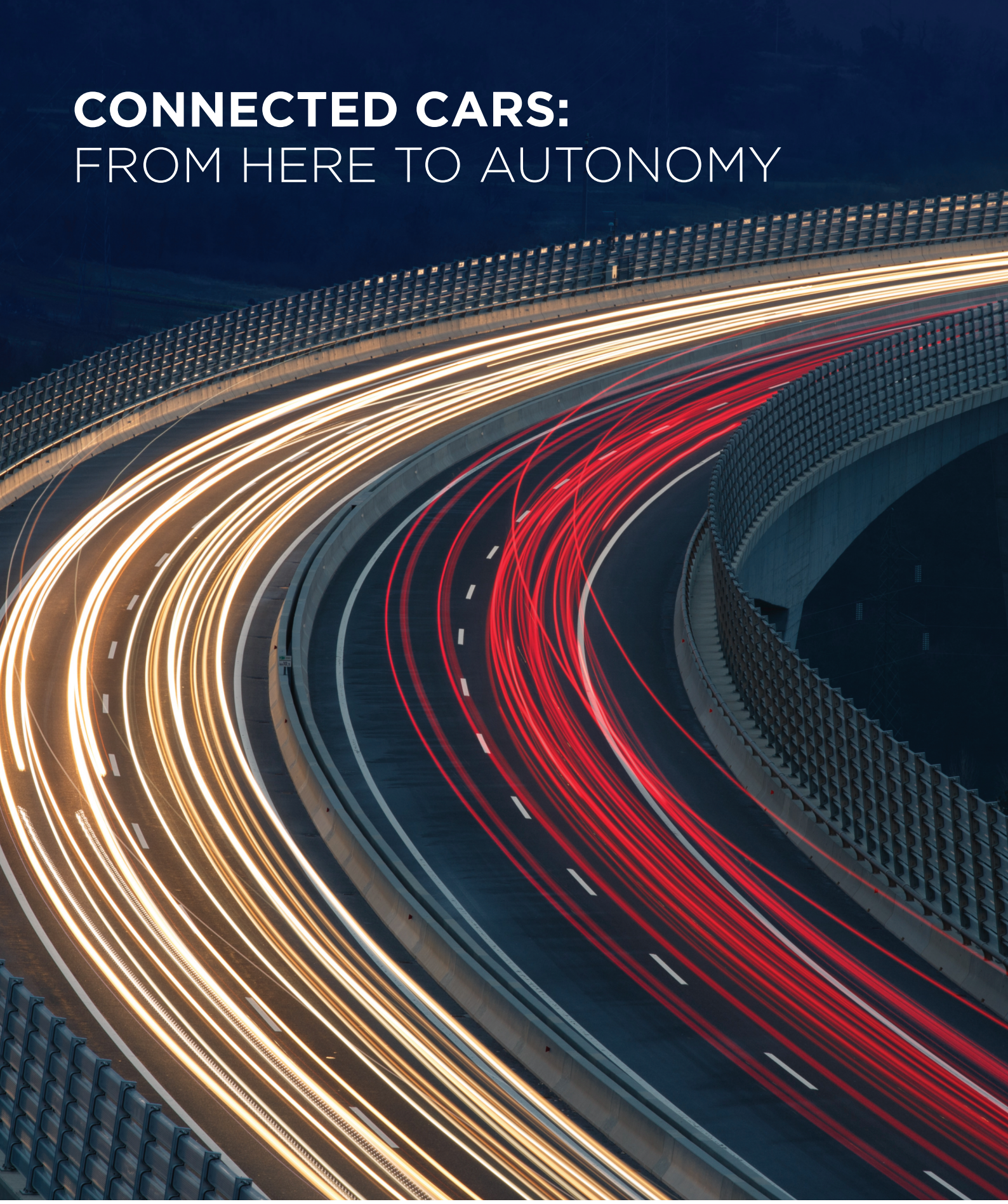
CONNECTED CARS:
FROM HERE TO AUTONOMY



Lead Sponsor:

gemalto
security to be free

Section Sponsors:

cisco

f5

European Global Navigation Satellite Systems Agency

InterDigital

Volkswagen

Published by

MOBILE WORLD LIVE

EXECUTIVE SUMMARY

Our global survey, conducted in November and December 2016 with nearly 1,000 respondents, uncovered significant understanding of the issues facing the wider deployment and monetisation of connected cars, along with significant enthusiasm for connected car technologies and services in general and autonomous driving. Respondents, perhaps recognising the increased media interest and new offerings that are already coming to market, gave highly positive responses as to when they expect connected cars to arrive in their markets. A total of 60% expected connected car roll-outs to be well underway within two years and 36.4% stated that deployments were already happening in their countries.

That enthusiasm reflects the potential of connected cars to transform the experience of road travel for consumers and to redefine the business models of car makers, road operators and providers of supporting services such as insurers, location-based service providers and in car entertainment suppliers. Almost half (48.8%) of respondents expected monetisation of connected cars to be achieved by 2020, underscoring the wealth of opportunities for the connected car to become a hub for other monetised services.

However, our respondents were not blinded by entirely positive visions of the connected future of cars and recognised that the challenges facing the market are numerous and substantial. Network technology itself was not seen as a significant issue, with just 11.6% of respondents identifying insufficient bandwidth or throughput as an issue for connected cars.

However, 36.6% identified patchy network coverage as the main connectivity deficiency that has potential to hold the market back.

Challenges surrounding securing connected cars have garnered substantial media coverage and the majority of users (60%) either strongly agreed or somewhat agreed with the statement: “I don’t know how to secure my connected car application or where my weak links are”, demonstrating an understanding of the complexities and risks associated with enabling secure connected cars. This was underscored when just over 70% agreed that security capability could be a key differentiator in their purchase of a connected car.

Of course, early connected cars are just a stepping stone on the path to greater automation and, ultimately, autonomous driving. At a time when the vast majority of vehicles are unconnected and huge questions remain to be answered about security, network coverage, business models and integration with other technologies, that seems distant but respondents agreed the direction of travel is towards autonomy. Even though caution exists, and 70.4% singled out trust in autonomous car providers being essential for the concept to gain mass market acceptance, the advantages are understood, with 54% of respondents agreeing that autonomous cars will be safer than traditional non-connected vehicles.

We are today at the tipping point when the connected car moves from a sci-fi vision of the future to a market reality. This survey reveals strong appetite for the benefits connected cars will bring that is only tempered by realistic caution regarding the security, standardisation and business model challenges that remain to be overcome on the journey to fully autonomous driving.

In partnership with

gemalto
security to be free

CONTENTS

Sponsored by:

gemalto
security to be free

THE CONNECTED CARS MARKET

Sponsor's Comment: Gemalto

Transform transportation with secure connectivity and automotive services

"The Internet of Things and leading edge connected car technology is transforming the transportation industry, causing a profound paradigm shift that is much like the one that occurred when motorised vehicles were first introduced in the early 1900s. IHS predicts that by 2020, 55% percent of new vehicles will be connected, with the average vehicle possessing the computing power of approximately 20 personal computers and featuring more than 100 million lines of programming code according to McKinsey. This is unleashing a new breed of features and services including autonomous driving, vehicle-to-vehicle (V2V) and V2X communications or car sharing capabilities that are forever changing our relationship to cars and driving.

As the survey reveals, automotive services are taking a lead role in driving the future of the industry. They are establishing new markets, optimising convenience and economy, enabling new players in the ecosystem and providing new revenue streams and monetisation schemes that benefit the entire value chain – from carmaker and MNO to service provider and driver. As we move forward and embrace self-driving cars, pay-per-mile insurance and embedded payment solutions that allow drive by transactions, the survey also reveals the critical role that trust plays in success. People and enterprises need to trust that their vehicle and connected systems are protected against cyber-attack and that the integrity of data is safe and secure.

As the global leader in digital security and IoT technology, Gemalto is committed to delivering the solutions, services and platforms needed to help automotive industry stakeholders **Connect, Secure and Monetise** the next generation of connected vehicles, with solid Identity Management. We hope this survey provides meaningful insight that helps all automotive players plan successful strategies for unleashing the power of connected vehicles and transforming our world for the better."

In late 2016, when our survey was running, it became clear that connected cars are becoming mainstream. The launch of Lync & Co, the new vehicle service being provided by Chinese car maker Geely, shows a new way of thinking about how consumers will buy and use cars and suggests a move to an as-a-service model. Inevitably this will require connectivity to enable security, insurance, charging and maintenance. Yet this is just the tip the of the connected cars iceberg, which ultimately could lead to fully autonomous vehicles.

We decided to scope out just how large our respondents see the connected cars iceberg as being and, in order to get them thinking about the scale, scope and prospects for the market, invited them to answer the open question: What type of use cases do you see coming in the connected car?

The spread of responses ranged from the expected – autonomous driving, assisted driving, fleet management and maintenance, usage based insurance (UBI), navigation, driver education, safety and entertainment – to the less expected, which included: artificial intelligence, healthcare, augmented reality and advertising. Many of these connected car use cases will form the foundations of entirely new markets and enable new entrants and existing players in the automotive and connectivity value chains to find new revenues.

This confidence that there is money to be made in connected cars was borne out by the next question which asked whether respondents felt the industry is ready to monetise the connected car. Although it's early days, a surprising 21.14% felt the industry is ready at the time the survey was conducted in December 2016, with a further 11.79% answering that the industry will be ready in 2017. That equates to almost one third of respondents seeing the industry as ready to monetise the connected car within 12 months.

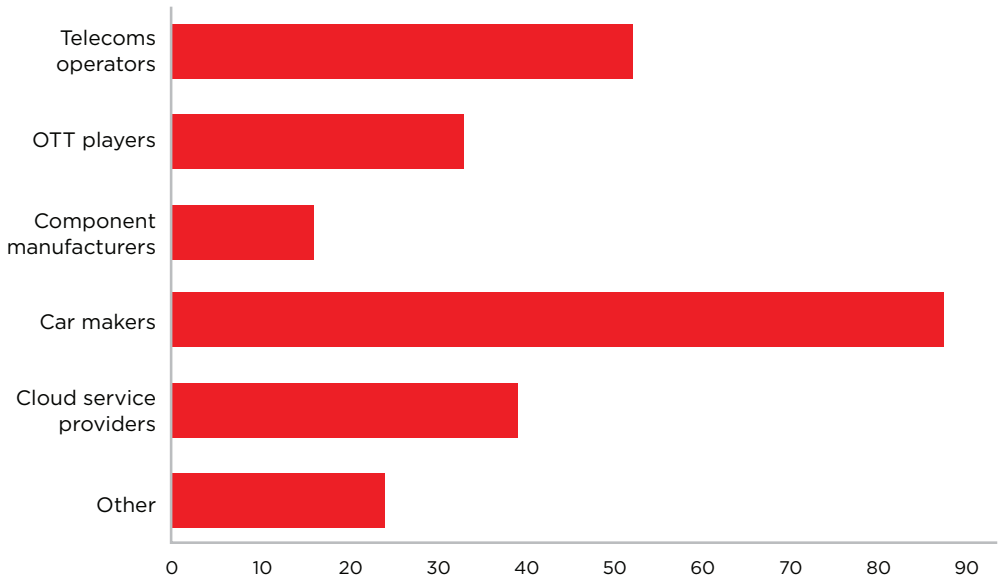
The majority (48.78%), however, feel it will take a little longer with monetisation readiness achieved by 2020. Just under 20% of respondents exercised caution, stating that they don't think the industry is ready to monetise the connect car yet and don't know when it will be.

While there's a general confidence that connected car services will be able to be monetised within 12 months among respondents, such revenues will take longer to become a significant part of their businesses. When asked what percentage of their revenue they expect to come from connected cars in the next 12 months, 82.11% of respondents said they expected it to account for less than 10%. At the other extreme only 1.05% of respondents expected connected car revenues to exceed 90% of their business's revenue.

Encouragingly around 10% of respondents said they expected 10-30% of their revenue to come from connected cars in the next 12 months, which seems an accurate reflection of market expectations for a sector that is still largely in the trials and pilot project phases and remains reliant on yet to be deployed technologies for many of the projected services – (and revenue streams) – to take off.

Responses to this question are clearly dependent on the type of business respondents are in and the services they plan to offer but when asked which type of company is best positioned to exploit the connected car trend, 34.6% of respondents said they felt car makers were best placed. Next best placed were telecoms operators with just over 20% of respondents selecting them. The results then reflected the increasingly software-driven value chain with cloud service providers third best placed with 15.5% of respondents choosing them. Significantly, cloud service providers outstripped component manufacturers (6.4%) but were closely comparable to over-the-top (OTT) providers, which 13.1% of respondents opted for.

What type of company is best positioned to exploit the connected car trend?



In order to further our understanding of the connected cars market in late 2016 we then asked a series of questions asking respondents to rate a series of statements on a scale of 1-5 where 1= strongly agree, 2= somewhat agree, 3= neither agree nor disagree, 4= somewhat disagree and 5= strongly disagree.

The first statement we made was about 5G connectivity. We said: Only when 5G becomes a reality will connected cars flourish. There was a mixed response to the statement with 28% of respondents saying they somewhat agreed with the statement but the next highest response (at 20%) was neither agree nor disagree, suggesting that 5G is understood to be many years away from ubiquitous coverage and unnecessary for many connected car applications. The bulk of the market shows no inclination to view 5G as essential for connected cars to flourish, although the responses suggest a clear appetite for the added capacity the technology will bring to connected cars.

Next, using the same scale, we asked respondents to rate the following statement: Security is one of the biggest challenges in connected cars.

Unsurprisingly, given the significant media coverage devoted to connected car security in 2016 and the hacking of vehicle systems such as a *Wired* journalist's Jeep, 60% of respondents strongly agreed with this statement. A further 27.2% somewhat agreed, giving an 87.2% combined score for those that strongly and somewhat agreed with the statement.

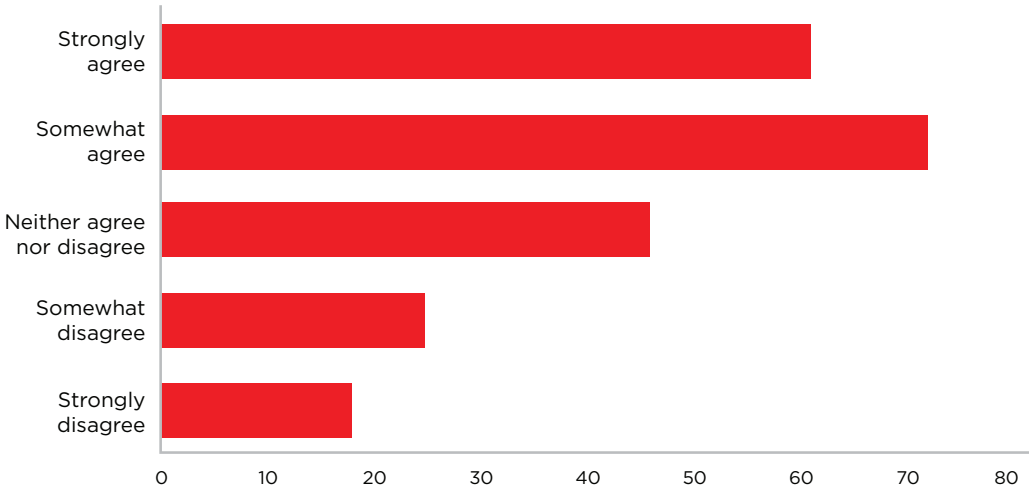
We then turned to the position of car makers as providers of secure connected car services and made the statement: Car makers possess the necessary security skills/capabilities in-house.

This provoked a more fragmented response with only 5.7% of respondents strongly agreeing with the statement. The majority (58.2%) felt the opposite, either somewhat or strongly disagreeing that car makers' in-house security skills are sufficient.

Respondents' fears or lack of knowledge about the level of security threats they face and how to address them in connected cars was underscored in the responses to the next statement. The statement: I don't know how to secure my connected car application, or where my weak links are, was either strongly or somewhat agreed with by 60% of respondents. This demonstrates that, while security is widely understood to be a significant challenge for connected car services, many in the ecosystem still lack knowledge of where threats come from and how to address vulnerabilities.

Encouragingly, just over 8% of respondents strongly disagreed with the statement, suggesting this portion of the market knows how to secure their connected car applications and is well aware of their weakest security links.

I don't know how to secure my connected car application, or where my weak links are. What do you think of this statement?



A growing, if predictable, understanding of the security challenges facing connected cars was demonstrated in the responses given to the next statement: Security needs to be assessed carefully. Protect what matters, where it matters, when it matters.

With 65% of respondents strongly agreeing and 26.5% somewhat agreeing, it's clear that the nuance of achieving security in the moment of threat was understood. Inevitably, security comes at a cost and that cost must be borne by the provider of the service if they are to maintain trust. However, there's an awareness that focusing on what matters rather than over-investing in securing things that don't matter is how the balance will be struck in maintaining security.

It may seem facile to state that security must focus on protecting what matters, where it matters and when it matters but security is only relevant when there is something of value at stake. Something that doesn't matter, doesn't necessarily need to be secured at significant cost and shouldn't be a priority for connected car services.

In spite of the demonstrated heightened awareness of security for connected cars among respondents, the majority (59%) were willing to admit that they either strongly or somewhat agreed with the statement: Security often remains an afterthought when designing connected car solutions.

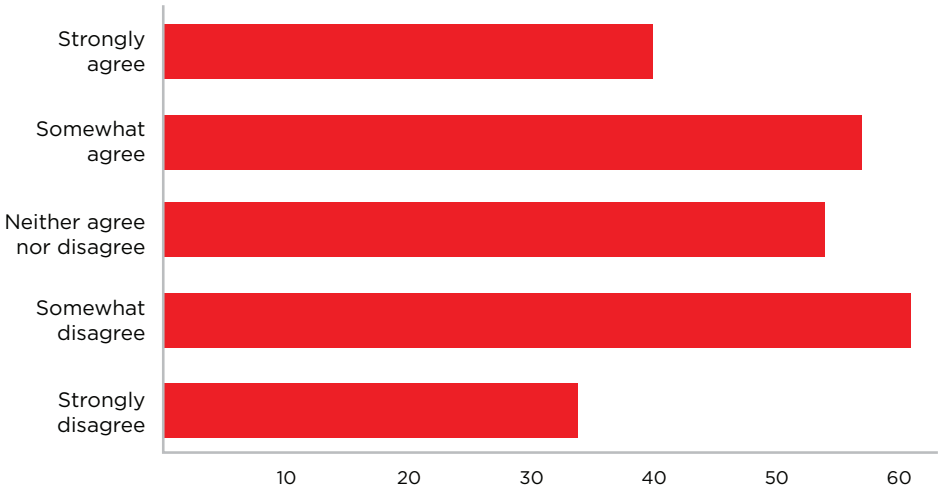
That so high a proportion of respondents acknowledges awareness of and rates the security challenge as one of the greatest facing connected cars, yet also agrees that it's an afterthought in connected car solutions design, suggests a significant disconnect between the future expectation that security issues will be addressed and the current design inputs into services. It may be that movement is already underway in this area with more than a quarter of respondents (27.5%) somewhat or strongly disagreeing that securing remains an afterthought at the solution design stage.

A key reason for that may be that the same ambivalence to making security a priority is present among consumers in the eyes of respondents. We put the following statement to them and received an inconclusive response: Security concerns are preventing consumers from buying a connected car.

Among our respondents, 13.8% strongly disagreed with the statement, while 16.3% strongly agreed with it. Towards the middle ground, fewer somewhat agreed (23.1%) but more somewhat disagreed (24.8%), suggesting that clear views as to whether security concerns are holding the market back are yet to emerge.

Combining the two groups reveals that 38.6% of our respondents disagree that security concerns are preventing consumers buying connected cars, while 39.5% think such concerns are holding back the market.

Security concerns are preventing consumers from buying a connected car. What do you think of this statement?



Whilst the statement regarding whether security concerns could prevent customers from buying a connected car generated an inconclusive response, the answer was clear for our next statement. We asked the extent to which respondents agreed with the statement: Security could be considered a key differentiator when shopping for a connected car.

When those that strongly and somewhat agreed were added together, just over 70% of respondents agreed that security could be a key differentiator in the purchase of a connected car, highlighting that significant consumer concerns about connected car security exist. Almost 34% of our respondents strongly agreed with the statement with less than 8% strongly disagreeing with it.

It's therefore clear that the industry sees security as a key differentiator and high on the list of consumers' requirements from a connected car maker. However, from the results of the previous statement, it looks as though the industry doesn't see security concerns among users as being significant enough for them not to acquire a connected car but, if there's a car available that does have good security, they'll view that as a highly positive differentiator.

The responses to these two questions either suggests an alarming complacency among vendors that users only view connected car security as a nice-to-have feature or that security is routinely viewed as someone else's responsibility and something that will be addressed without holding the market back.

Given the responses to the next statement – Trust is essential for autonomous cars to gain mass market acceptance – that complacency seems misplaced, albeit that the consequences of a security breach in an autonomous car are far greater than those in a navigation app or an infotainment service.

Across the two agree categories this statement drew almost 90% of our responses, with 70.4% of respondents strongly agreeing that trust is essential for autonomous cars to gain mass market acceptance. A further 19.4% somewhat agreed with the statement.

This extremely high percentage of response is likely to be a consequence of the raised stakes of autonomous as opposed to connected driving. For many, the autonomy concept is frightening and unfamiliar and the idea of travelling at highway speeds in an autonomous vehicle from an untrusted supplier is quite simply life-threatening. Put simply, the stakes don't get any higher than that so autonomous cars must focus on maintaining and building consumer trust. It's clear from the response level we've seen here that much work remains to be done to foster greater trust and organisations in the ecosystem will have to focus on protecting the reputation of autonomous cars if they are to emerge from current global test environments into the mainstream.

Delivering Trusted Mobility

The IoT revolution is providing endless opportunities for the automotive industry. Cars are becoming a cornerstone of our connected world and enabling new paradigms to improve our daily lives. To support this transformation, Gemalto offers a broad portfolio of trusted solutions, services and solid Identity Management to **Connect, Secure and Monetize™** the entire connected car and transportation ecosystem.

GEMALTO.COM/IOT

CONNECT. SECURE. MONETIZE.™

ENABLING ORGANIZATIONS TO OFFER TRUSTED AND CONVENIENT
DIGITAL SERVICES TO BILLIONS OF INDIVIDUALS. LEARN MORE AT GEMALTO.COM

gemalto
security to be free

Sponsored by:

European Global Navigation Satellite Systems Agency

CONNECTED CAR NAVIGATION

Sponsor's Comment: GSA

"Cars with futuristic capabilities are in showrooms today, anticipating the continuing investment of the automotive industry in connectivity and the semi-automatisation of driving functions. Yet ultimately, it is the customers' acceptance that will determine the success of fully-autonomous vehicles in the long term and there are two key aspects of great importance for car makers: safety and the cost of these new technologies.

Although most vehicle telematics already provide communications services with basic positioning requirements, many satellite navigation (GNSS) chipset manufacturers are getting ready to acquire new satellites and frequencies leading to a significant improvement of the positioning performances. Apart from the well-known US GPS, new constellations want to pave the way for accurate and highly robust navigation solutions for enhanced driver assistance applications by focusing on the positional accuracy and cybersecurity challenges. The most groundbreaking example is Galileo, the unique global navigation system under civilian control, which is adding additional frequencies, higher resiliency against multi-path and authenticated signals detecting intentional interferences."

Among the early and most compelling connected car services and application enablers is navigation. Satellite navigation has been in use for many years and is already very familiar to consumers, car makers and fleet operators. However, coverage by different satellite networks is not a one-type-fits-all proposition and different satellite connectivity offerings exist across the world and will increasingly support the connected cars ecosystem.

Satellite navigation enabled by GNSS – the Global Navigation Satellite System – represents a telecoms infrastructure that is provided for free by diverse nations across the world, all of which are compatible with the US GPS programme. In order to establish the extent to which respondents are aware of the different satellite connectivity options we asked respondents to select all the satellite systems they have heard about.

As expected the most widely known was GPS and 94.3% of respondents said they had heard of it. Next most well-known was Galileo, which 73.8% had heard of. Galileo was followed by GLONASS with 47.2% of respondents familiar with that constellation and Beidou with 26.6% of respondents aware of it. Following that, the proportion of respondents familiar with other systems and constellations tailed off rapidly, with WAAS and EGNOS scoring around 10% recognition.

We then moved on to ask respondents how many popular GNSS road transportation applications they were aware of apart from assisted driving functions (ADAS). Car navigation led the awareness with 95% of respondents selecting it. This was followed by anti-theft locator applications which were chosen by 77.9% of respondents and fleet management applications which were listed by 76.5% of respondents.

Next came emergency call location, with 68.9% of respondents stating awareness. Intelligent parking was recognised by 50.4% of respondents.

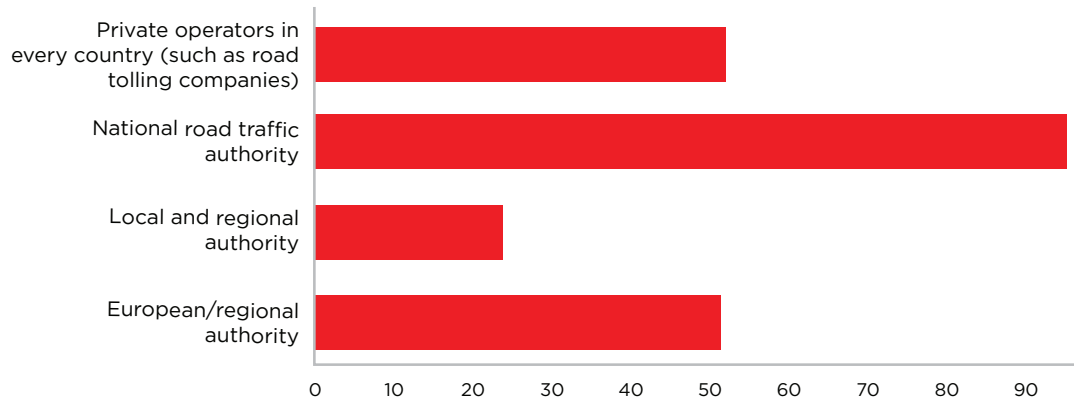
There was a generally high awareness of the most popular applications, such as pay-as-you-drive/insurance telematics familiar to 39.2% of respondents, road tolling and pricing known to 48.2% and congestion charging known to 37.4% of respondents. However, in spite of this awareness of the applications, one respondent commented that most satellite companies are invisible to the vehicle manufacturer and user.

V2I road infrastructure

We then asked respondents which type of organisation they thought should be the operators of vehicle-to-infrastructure (V2I) road infrastructures in order to speed up connected car deployment. 42.8% of respondents clearly identified national road traffic authorities as the organisations that should operate V2I projects but others (23.4%) felt private operators (such as road tolling companies) in every country could be best placed to accelerate connected deployment.

A further group (22.9%) felt that a European or regional authority would be well placed to be the operator of V2I activities. Potentially this number reflects respondents from within the European Union looking to the EU to lead across the community of countries. Finally, just 10.8% felt that local authorities would be suited to be the operators of V2I road infrastructures, perhaps feeling that road networks cover geographies that are too large to be effectively operated on a localised basis.

Who should be the operator of the V2I (vehicle-to-infrastructure) road infrastructures in order to speed up connected car deployments?



> "Coverage by different satellite networks is not a one-type-fits-all proposition and different satellite connectivity offerings exist across the world and will increasingly support the connected cars ecosystem."

Returning from the operational to the technical, we explored how manufacturers are optimising the technology mix for autonomous vehicles. We asked respondents which navigation-related technologies they thought would be in commercial operation from 2020.

Unsurprisingly, GNSS was the most selected with 80% of respondents expecting it to continue to be in commercial operation from 2020. GNSS was followed by 5G which 67.9% of respondents expected to see commercial operational from 2020, a potentially ambitious deployment timescale for a still nascent technology but reflective of the hype surrounding 5G technologies in the market place.

Aside from these well-known technologies, the numbers began to tail off. Next most widely expected to be in operation in 2020 was LIDAR (Light detection and ranging) by 34% of respondents, followed by computer vision (27.4%) and DSRC (dedicated short range communications) with 26.51%. Vehicular Ad Hoc Networks (VANETs) were expected to be in operation by 2020 by 17.21% of respondents, suggesting a steep development path is required over the next three years.

With GNSS clearly identified as an extremely well-established technology today and one that is set to be in commercial operation for many, many years beyond 2020, our survey's focus turned to its performance. We asked respondents which of the following capabilities they see as GNSS' most important performance capability.

Bearing in mind the locational precision that connected cars will require, it's of little surprise that accuracy of positioning was identified by 35.6% of respondents as GNSS' most important capability. Next most important was the availability of the navigation signal, which 22.4% of respondents saw as most important.

Integrity/robustness of the navigation signal was seen as the next most important performance capability, with 17.3% of respondents seeing it as most important and the need for reliability was underlined by the same percentage (17.3%), seeing continuity of the service as its most important capability.

The remaining 7.3% of respondents said that the authenticity of the navigation signal was its most important performance capability, highlighting further that reliability, robustness and authenticity are key requisites for successful navigation services.

Autonomous accuracy

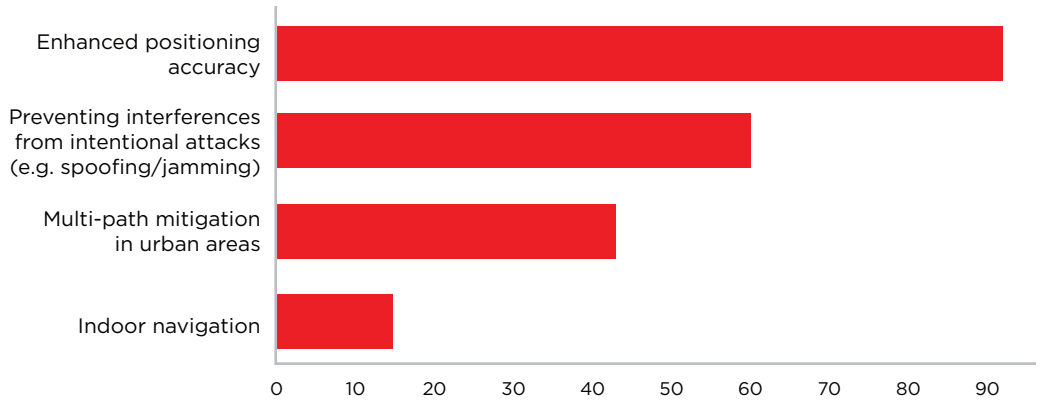
We then looked ahead to the era of autonomous vehicles and asked our respondents what should be the horizontal accuracy of autonomous vehicle positioning using a combination of sensors. Our respondents were clearly thinking of fast moving autonomous vehicles often on busy highways and applications such as the platooning of trucks on highways. 35.3% respondents said the horizontal accuracy of autonomous vehicle positioning should be less than 10cm and responses overall demonstrated a strong awareness among respondents of the accuracy needs of autonomous vehicles. Just 15.4% felt that accuracy of one to two metres would be adequate, 22.1% felt between 50cm to 1m would be necessary and 27.1% felt that an accuracy of 10cm to 50cm would suffice.

As awareness of the precision requirements of autonomous vehicles increases it is to be expected that more respondents would move into the less than 10cm response. This was borne out in the responses to our survey's next question which asked what respondents saw as the main areas of improvement for the use of GNSS and connected cars.

Enhanced positioning accuracy was identified as a main area of improvement by 43.7% of respondents, demonstrating further the importance of accurate positioning for autonomous vehicles. The next most important area of improvement was preventing interferences from intentional attacks such as spoofing or jamming. 28.8% of respondents identified these key security and safety issues as an area for improvement.

The final two options offered in the survey addressed maintaining signal strength either in dense urban areas or in indoor locations. 20.4% of respondents said multi-path mitigation in urban areas was a main area for improvement while almost 7% said the same of indoor navigation.

What do you see as the main areas of improvement for the use of GNSS in autonomous vehicles and connected cars?



We concluded the navigation section of our survey by exploring the issues around cybersecurity in greater depth. We asked our respondents to select from Critical to Unnecessary how important they see provision of an authenticated GNSS signal, which the Galileo system now provides, being in protecting against security threats to autonomous vehicles and connected cars.

40.6% of respondents answered that they see such functionality as critical and a further 38.8% described the capability as important. Just 1.4% of respondents described provision of an authenticated signal as unnecessary, with the remainder describing it as interesting. What's significant here is that more than 90% of respondents view an authenticated GNSS signal as either critical, important or necessary in protecting against cybersecurity threats to autonomous vehicles or connected cars.

Overall, this section of the survey, which dealt with two of the most mature aspects of the connected cars ecosystem – navigation and satellite connectivity – revealed a technology with well-developed functionality and a long lifespan ahead. Further work on positional accuracy and cybersecurity are certainly required but unlike the other areas of the ecosystem many of the international interoperability issues and performance challenges are either resolved or have plans in place to address them.

> "As awareness of the precision requirements of autonomous vehicles increases it is to be expected that more respondents would move into the less than 10cm response."

Sponsored by:

cisco

CONNECTED CAR CONNECTIVITY

Sponsor's Comment: Cisco

"Connected cars hold great potential as part of the IoT boom and present new revenue opportunities and a widened playing field for service providers. This survey is timely and confirms the current interest in the connected car as an evolving platform for mobile services. This is an area of growth, beyond smartphone-based consumer services, and an enabler of new business models for service providers. It also highlights the diverse applications and associated service requirements.

We clearly have some work to do to augment existing networks to be optimal for connected cars; creating ubiquity of coverage with multi-access technologies, and seamless mobility in-between. At the same time dynamic QoS and bandwidth control is required, all without adding complexity or significant cost to network total cost of ownership (TCO).

Cisco is working closely with service providers to transform networks for new opportunities like connected cars. Our principles are to virtualise, simplify, automate and programme mobile networks; creating platforms ready for IoT and the 5G era."

Amidst all the excitement surrounding autonomous vehicles, assisted driving and the rich connected car applications of the future, it's easy to forget that connected cars are a reality already in some markets. As always, this depends on definitions but new vehicles are already routinely shipping with at least some form of connected functionality offered.

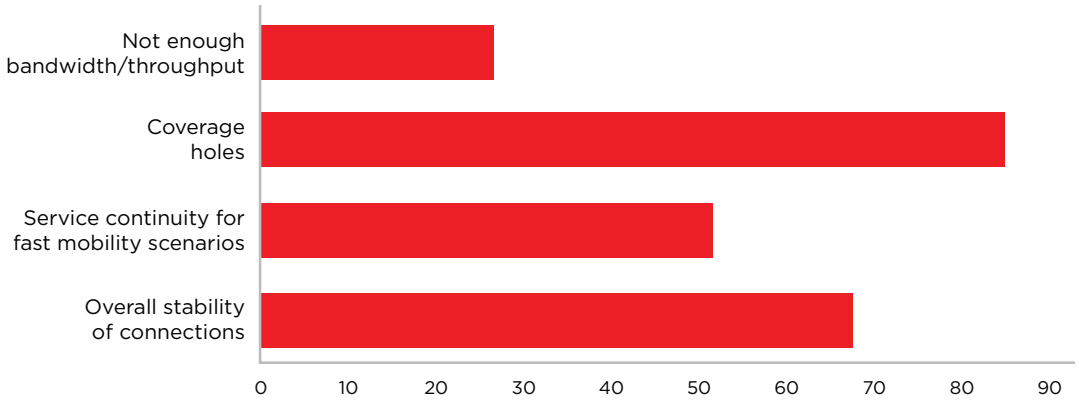
In order to gauge respondents' perception of connected car availability we asked then when they think connected cars will start rolling out in their country. 36.4% said connected cars were already available, 8.9% said they would be available within the next year and 14.4% said they would be available within the next two years. That's positive news, suggesting that almost 60% of respondents expect connected car roll-out to be well underway in their countries within two years.

However, some respondents see roll-out taking significantly longer. 22.5% think it will happen within the next five years but 17.8% stated that roll-out is still too far away to predict. Inevitably this question is open to the vagaries of different markets, their regulations and their existing mobile network infrastructure but the overall expectation of sustained roll-out, which has already started in some markets, demonstrates the traction connected cars are already gaining.

We then turned to network connectivity to explore whether respondents think it is ready to support connected car applications. We asked respondents what they would consider as the main deficiency in the connectivity network for cars today. Coverage holes were identified as the biggest issue by 36.6% of respondents, the largest group. However, the overall stability of connections (29.3%) and service continuity for fast mobility scenarios (22.4%) were also seen as significant deficiencies to be overcome.

The network technology battle appears to have been addressed for most respondents with just 11.6% identifying not enough bandwidth or throughput as network connectivity's main deficiency.

What would you consider as the main deficiency in the connectivity network for cars today?



Nevertheless, our next question revealed that users are split as to whether a combination of LTE and Wi-Fi alone, which are the typical wireless technologies for connected cars today, will be sufficient to support connected cars connectivity requirements for the next five years. 50.86% of respondents felt the two technologies would be sufficient for the next five years but 49.14% thought they would not. Those that thought it would not be sufficient may be considering higher bandwidth connectivity such as 5G and satellite links or looking to some of the low power wireless access (LPWA) solutions coming to market to serve the Internet of Things (IoT). Inevitably, connectivity decisions will come down to the nature of the connected car application to be supported. Some will require high speed, low latency connections; others will simply require stable yet sporadic access to narrowband connectivity.

We then looked to assess where the connected car monetisation opportunities lie for connectivity services providers. We asked respondents to select which segments they thought would present the greatest potential for monetisation. Three of our categories were selected by almost half of respondents. These were incremental average revenue per user (ARPU) from end users (48%), B2B revenue from vehicle manufacturers (49.3%) and B2B revenue from automotive industry players (48.9%).

Sponsorship and advertising were selected by just under a third of respondents, suggesting that more monetisation will be achieved through charging end users, car makers or other types of automotive industry service providers than through paid-for marketing. 33% of our respondents said they see great potential in B2B revenue from content sponsors and 31.7% said they identified B2B revenue from advertising as having strong potential.

It's clear from these responses that there is a wide spread of opportunities for connectivity service providers to monetise the connections they provide. Interestingly, 4.4% of our respondents cited other monetisation opportunities. Among these, insurance was mentioned most often as a source of revenue for connectivity service providers. Applications such as usage-based insurance will certainly require connectivity and insurers may be the organisations most likely to pay for this.

Recognising that it won't just be connectivity that is charged for, we decided to explore further and asked our respondents how many billable parties they thought could be typically involved for a connected car. In the USA, for example, AT&T considers the connected car to be like a mobile device so that the car owner can add their vehicle onto their mobile data plan. In other context it's also possible for the car maker or sponsors to subsidise connectivity charges, so there is scope for several billable parties within the connected car value chain.

Just over half (52.8%) of our respondents thought that there would be three to five billable parties typically involved in a connected car. These would include the car owner, the car maker and third parties. This was the largest group of respondents and was followed in our survey by respondent who thought there would be just one billable party – the car owner (18%) – and those who thought there would be two billable parties – the car owner and the car maker.

Caution clearly exists about the number of billable parties in the connected car ecosystem with just 5.6% of respondents stating there would be more than ten and 6% stating there would be six to ten billable parties.

We then turned to specific use cases and their connectivity requirements. We highlighted use cases including usage based insurance, pro-active maintenance, in-car entertainment and navigation/location services that are already being positioned in the market today. We then asked which network capability would respondents see as the most crucial for facilitating such services.

The largest proportion of respondents (31.3%) selected dynamic quality of service (QoS) control as the most crucial capability. This was followed by bandwidth on demand, which was selected by 19.8% of respondents.

Real-time usage rating and charging was seen as the most crucial network capability to facilitate such services by 17% of respondents, as was analytics which was also selected by 17%. This outcome demonstrates that about one third (34%) of users foresee a need to measure and analyse usage to understand user and application behaviours and charge for them appropriately. Gaining such visibility into the quality and types of experience and connections connected cars have will be critical for enabling providers of all types to learn about what users want and what works. Equally, it will enable accurate charging to the appropriate person or organisation in the connected cars value chain.

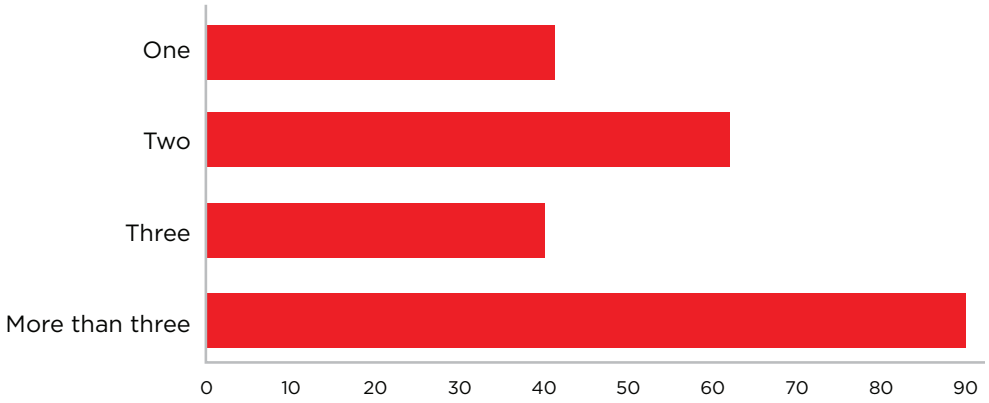
Finally, and looking ahead to more agile network capabilities, 14.5% of respondents selected network programmability through application programme interfaces (APIs) as the network capability they consider most crucial for facilitating connected car services.

Of course, the connected car isn't just focused on one service and many different services are likely to run concurrently. For example, navigation could run at the same time as analytics for UBI or entertainment for back seat passengers. There is a widely varying blend of applications and services that will make up the connected car experience and each will place different requirements on connectivity, some of which may be simultaneous.

For this reason, we asked our respondents how many wireless connections they think a connected car will require. From their responses, it's clear they see the need for multiple connections to be enabled to support the disparate applications and bandwidth requirements of the connected cars ecosystem.

The largest percentage of respondents (38.6%) said they believe that more than three wireless connections will be required by connected cars. 26.6% thought that two wireless connections would be required and 17.2% felt three would be necessary. Only 17.6% of respondents felt that a single connection would be all that connected car services require.

The connected car presents a unique use case in which multiple services run concurrently. Each service has varying requirements and could potentially be served by different wireless technologies and multiple concurrent connections. How many wireless connections do you think a connected car will require?



As Uber, Ford and Tesla are moving towards driverless ride sharing offerings and autonomous driving, cloud accessed services and new communication channels via V2I (vehicle to infrastructure), V2V (vehicle to vehicle) and others are on the connected cars roadmap, there is a need for automation to support such diverse and dynamic communication requirements. We asked our respondents if they agreed or disagreed that the network will likewise need to become automated.

From the response, in which 83.5% of respondents, agreed with the statement, it's clear that the network will also have to become automated in step with the services it supports. In the world of automated applications there's no room for manual configurations or processes in the network which could become a substantial bottleneck for connected car services if it is not able to dynamically and automatedly respond to the demands users and applications place on connectivity.

Sponsored by:

INTERDIGITAL

AUTONOMOUS DRIVING

Sponsor's Comment: InterDigital

"We are on the verge of disruptive changes that will hit one of the largest IoT verticals – the transportation industry. The impact will be multi-dimensional, from the consumer level via self-driving cars, to the enterprise level via platooning trucks and all the way to the society level via Smart Cities. Today, we are only scratching the surface of this multi decade transformation. During this early period, it made a whole lot of sense to take the pulse of the converging mobility and transportation industries, as well as ecosystem participants, to collect their views about where we are going. At InterDigital, we are glad that we partnered with GSMA's Mobile World Live for this survey. Responses are both expected and surprising on different levels. It also reaffirms our view that over time industry evolution will touch and shake the complete value chain and technology stack from sensors to V2V/V2I, OS, cloud, services, analytics and applications layers."

Autonomous driving is one of the ultimate goals of connected car initiatives but the path to it will take many years as the market awaits regulation, legislation and the comprehensive technology and standards ecosystem required to support autonomy. Nevertheless, if the goal is to be made, real work must start now. The good news is that work has started and assisted driving applications are a reality in some markets today.

Connectivity is widely thought to be the enabler of autonomous driving so we asked our respondents to select which types of connectivity are required for the successful commercial roll-out of connected cars. The vast majority of respondents saw our categories of connectivity to other cars, connectivity to city/roadside infrastructure and connectivity to the cloud as requirements but 5.9% of respondents stated that no connectivity is required for the successful roll-out of autonomous driving.

It is to be expected that these respondents believe that autonomous driving can be safely achieved in self-contained vehicles relying on on-vehicle sensors and technologies to avoid incidents. However, lack of connectivity would isolate the vehicle from navigation information for example, so connections would be required to enable that at least.

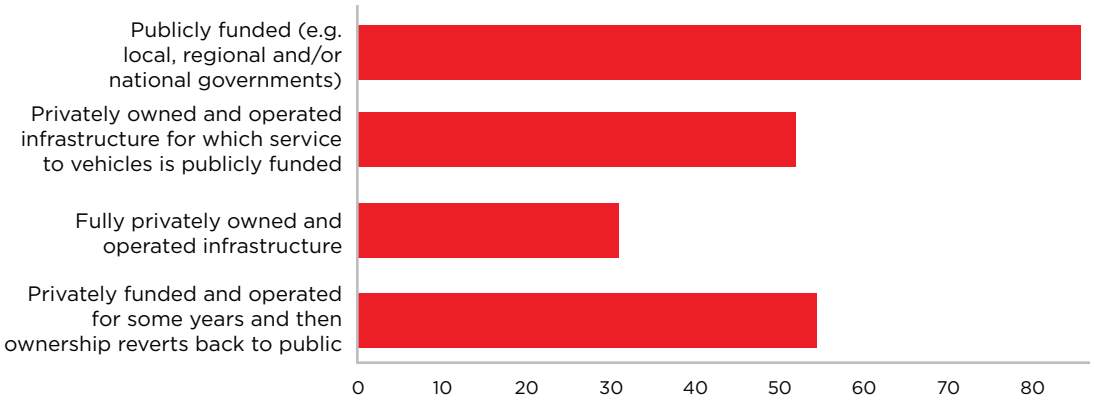
The highest proportion of respondents (79.9%) selected connectivity to city/roadside infrastructure as a requirement, identifying that autonomous driving will require inputs from roadside equipment. Connectivity to other cars was selected by 62.1% of respondents, demonstrating their awareness that autonomous driving relies on being able to recognise and avoid other vehicles. Finally, connectivity to the cloud was selected by 70.3% of respondents, suggesting high awareness of the need to integrate autonomous driving with data and inputs from across the connected cars ecosystem.

We delved further into the reliance of autonomous driving on connectivity by asking whether our respondents see the full roll-out of autonomous driving as being dependent on connectivity being fully available. Just over two-thirds (67.7%) of respondents agreed that connectivity should be fully available if autonomous driving is to be fully rolled-out but the remaining almost one-third (32.3%) did not feel fully available connectivity is necessary. That may seem a surprisingly large percentage given the safety concerns that surround autonomous driving but respondents may feel that extremely frequent connectivity is sufficient to keep autonomous vehicles on the right track.

We then asked which type of organisation will fund the deployment of roadside infrastructure to enable autonomous driving. Our respondents were divided in their answers. Most (38.5%) expected such investment to be publicly funded by local, regional or national governments and a further 23.4% expected the infrastructure to be privately owned and operated but the services to vehicles to be publicly funded. The role of public investment was also underscored by the 24.3% of respondents who said they expected infrastructure to be privately funded and operated for some years before ownerships reverts to the public.

With just 13.7% of respondents saying they expected such infrastructure to be fully privately owned and operated, it's clear that the market expects governments to be at the heart of funding the roadside infrastructure to enable autonomous driving. Private businesses, with the possible exception of the largest toll road operations, typically have only fragmented parts of the road infrastructure so are not best-placed to provide nationwide or even regional infrastructure coverage.

Who will fund the deployment of roadside infrastructure to enable autonomous driving?



Next we turned to vehicle-to-vehicle (V2V) communications and asked our respondents what timeframe they expected these to be deployed within. Most respondents (45.2%) expected this to happen within five years but 28.5% of respondents thought this would happen sooner – within three years. A more pessimistic group of respondents (19.5%) thought that this would happen within a decade and an even more cautious group expected V2V communications to take longer than ten years to deploy. Perhaps this group felt the long lifecycles of already deployed cars would take this length of time to be replaced and the retrofit market would not be able to address a critical mass of vehicles in only a few years.

We then asked the same question but this time regarding the timeframe for vehicle-to-infrastructure (V2I) systems to be deployed. The responses were remarkably similar with 46.8% of respondents expecting this to happen within five years, 27% seeing V2I deployment occurring within three years, 18.3% expecting it to take up to a decade and the remaining 7.8% stating it will take longer than ten years. Again, reasons for the delay are likely to centre around vehicle upgrade and the scale of investment and deployment activity to put the infrastructure in place.

It is becoming clear that, in order for autonomous driving to take off and be accepted, organisations that can lead developments are required. With this is in mind, we asked our respondents which type of organisation they think will take the lead in enabling connectivity for autonomous driving. The majority of respondents (53.6%) thought a combination of car makers and operating system (OS) providers would be best placed to take the lead in enabling connectivity for autonomous drivers. Car makers on their own were selected by 23.6% of respondents, while mobile OS manufacturers on their own were chosen by just 5.9% of respondents.

This leaves perhaps the organisations most associated with connectivity – the mobile network operators – being chosen by 16.8% of respondents. Perhaps the competing nature of operators in individual markets and a perceived lack of differentiation in their offerings means by far the majority of our respondents did not see them as the type of organisations to take a lead in enabling connectivity for autonomous driving.

It's significant that the respondents chose a combination of car makers and OS providers because it signals an ecosystem of collaborators is required to make autonomous driving a reality. To explore this further we asked our respondents to what extent they think different industries will converge to shape how autonomous driving is enabled. 45.6% responded that they believe different industries will converge greatly to achieve this and this was followed by 32.8% of respondents who felt industries would converge somewhat. A further 19.6% said they expected industries to converge in specific areas leaving just 1.83% of respondents stating that different industries will not converge at all.

Given this expected increased collaboration, but also faced with continued fragmentation between different car makers and equipment vendors, we then asked how rules for autonomous driving decision making will be harmonised across different vehicle manufacturers and equipment vendors.

The most popular response, given by 46.1% of respondents, was that one or more industry standards will be defined and adopted. Next most popular was the response that a de facto standard will be established – such as one based on early autonomous vehicle designs – that others will follow, which was selected by 40.6% of respondents.

Of some concern, 9.1% of respondents stated that no harmonisation will occur and each manufacturer will design their own rules for autonomous driving decision making. This presents significant challenges for the industry if the autonomous driving systems in a BMW don't make harmonised decisions with a Mercedes that is driving towards it.

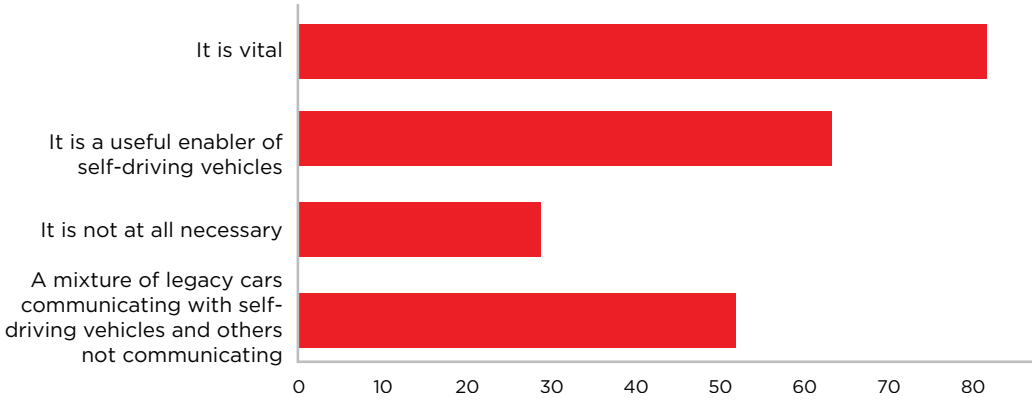
Standard harmonisation

We wanted to examine further attitudes among those who answered that one or more industry standards would be defined and adopted and those that saw a de facto standard being established. Of those that selected those responses we asked how they see autonomous driving decision rules varying geographically. 26.8% said they would be globally harmonised, 34.6% said they would be harmonised per continent, 35.7% said they would be harmonised per country and 2.8% said they would be harmonised per state or region within a country.

Next, we moved on to explore the likely outcomes for legacy cars in the autonomous driving era. We asked our respondents how necessary is it to enable legacy cars to communicate with self-driving vehicles. 36.2% of respondents viewed this as vital while 12.8% thought is was not at all necessary. Almost 28% said they viewed enabling legacy cars to communicate as a useful enabler of self-driving vehicles, while 22.9% of respondents said a mixture of some legacy cars communicating with self-driving vehicles, while others do not, would be acceptable.

> "It is becoming clear that, in order for autonomous driving to take off and be accepted, organisations that can lead developments are required."

How necessary is enabling legacy cars to communicate with self-driving vehicles?



We then asked how significant the challenge of enabling legacy cars to communicate with new, self-driving vehicles is. 45% of respondents said the technical and regulatory challenges are substantial, while 20.4% said they were confident that systems can be retrofitted to existing vehicles. A further 17% said that the hit and miss nature of communications support from legacy vehicles will create confusion for the public in terms of interaction with self driving vehicles.

The most significant concern for the development of self-driving vehicles is that 17.5% view failure to enable legacy vehicles as a showstopper, stating that the challenge of enabling legacy cars to communicate with new, self-driving vehicles is so great that it will prevent mass market adoption of autonomous driving.

Finally in this section we asked respondents how long they believed it will be until we see adoption of autonomous driving by 10% of users. The majority of respondents (52.3%) said they expected this to take ten years, while 21.5% said they expected this to take five years to happen. 17.9% of respondents were more cautious, stating that it will take 15 years to see 10% adoption while 8.3% expected adoption by 10% of users to take more than 20 years.

Sponsored by:

CONNECTED CAR SECURITY

Sponsor's Comment: F5

"To achieve a profitable business model, mobile operators, ecosystem partners and automakers will face tremendous pressure from end users and regulators in building a secure and integrated connected car platform. Deep partnerships will be required to address connectivity and vehicle operations to deliver safe and secure apps. Connected cars' greatest security vulnerabilities are in connectivity, navigation and info systems, and the electronic control system. The greatest threat is hacking (59%), followed by malware/viruses (28%). Survey respondents believe that the best means to secure connected cars is encryption with biometrics and firewall.

Transport encryption with SSL and TLS can protect data when implemented correctly. An overwhelming 77% of respondents believe security will be implemented for the connected car to enable autonomous driving within the next three to five years. To capitalise on this opportunity, automakers, ecosystem partners and mobile operators must deliver on an optimal user experience while ensuring absolute data protection, privacy, and user safety."

Security is the elephant in the room that has the potential to severely limit the prospects of the connected car market. Negative headlines involving the potential for cyber criminals to take control of autonomous vehicles are in reality only a small part of the security challenge facing connected cars. On a less newsworthy scale, poor security could lead to data breaches, fraud, identity theft and many other crimes.

The need to address security is therefore a priority in connected cars so we turned to our survey respondents to learn more about their attitudes to security and where they see the greatest vulnerabilities existing. We asked them to select which of hacking, malware/viruses, data theft and traditional theft they see as the greatest threat to connected car security.

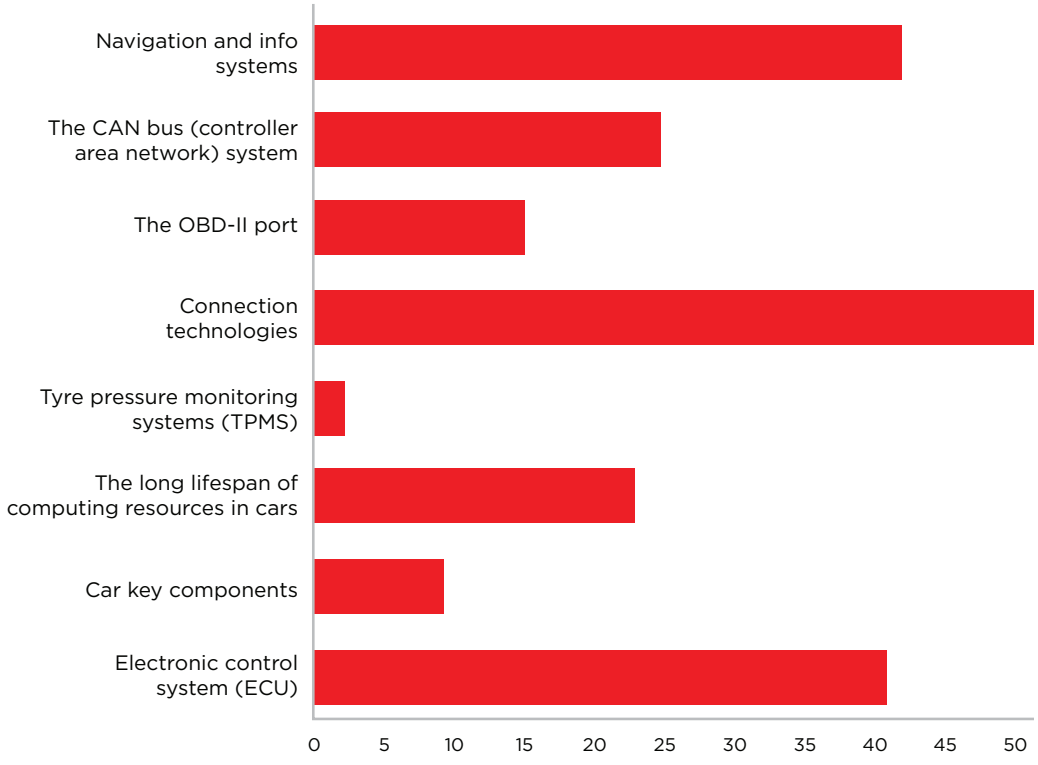
A substantial majority (59.8%) of respondents viewed hacking as the greatest threat. This was followed by malware/viruses which were selected by 28.3% of respondents. Of less concern was theft – traditional theft was seen as the greatest threat by just 4.1% of respondents, while data theft topped only 8.7% of respondents' threat lists.

Next, we moved on to consider who is liable for connected car security. The ecosystem and value chain is large and distributed and therefore a wide range of organisations could hold liability. Nevertheless, the majority of our respondents (53.9%) think car makers are liable for connected car security, with 18.9% citing the connectivity provider as liable. Application providers were selected as liable by 15.6% of respondents and electronics makers by 5.9%.

Interestingly, only 5.5% of respondents felt the vehicle owner was liable for connected car security, suggesting that security will continue to be the responsibility of vendors and service providers rather than the users themselves.

We then turned to address which system or component our respondents identify as connected cars' greatest security vulnerability. The attack surface is potentially large and this was borne out in the fragmented responses of our respondents.

What do you identify as connected cars' greatest security vulnerability?



The most widely identified security vulnerability was in the connection technologies themselves, which were selected by 25.2% of respondents. This was closely followed by navigation and info systems, chosen by 20% of respondents, and the electronic control system (ECU) of the vehicle by 19.5% of respondents.

Other vulnerabilities highlighted were largely to do with vehicle-based technologies. 11.9% of respondents thought the greatest security vulnerability is in the Controller Area Network (CAN) Bus system of the vehicle, 7.1% thought the OBD-II port for on-board diagnostics is the greatest vulnerability and 10.9% chose the long lifespan of computing resources in cars.

There was less concern about specific items of vehicle technology with 4.3% of respondents identifying car key components as the greatest security vulnerability and just 0.9% identifying the tyre pressure monitoring system (TPMS). TPMS has drawn some attention, again in the press, because it provides an exterior point at which vehicle systems can be entered.

Concepts such as hacking vehicles via TPMS, which have been widely reported, do suggest that a substantial amount of hype surrounding connected car security exists but our respondents felt that security is a big issue and much of the hype is justified in order to bring enough attention to the market to help fight back against the criminals.

62.8% of our respondents, when asked whether they felt connected car security concerns have been overhyped, said they had not, a further 21.1% said they thought the current level of hype is fair while just 16% of respondents felt that security concerns are overhyped. The message to take away is that hype about connected car security exists but, for the most part, it is fair and justified.

Over the air security

Picking up on the point raised earlier about the age of computer systems in vehicles, we then asked our respondents to what extent they thought over the air (OTA) software updates would make connected cars more secure. It's clear that being able to update in-vehicle systems and send security patches over the air will help strengthen connected car security and this was reflected in the responses. 44.6% of respondents said OTA updates would help significantly, 24.6% said they would help greatly and 16.7% said they would help moderately.

However, a small core of respondents were unconvinced by the security of OTA updates with 4.6% stating that they will not help at all and a larger group – 9.3% of respondents – stating that they could in fact make cars less secure. These respondents are likely to have assessed OTA upgrades as a potential vulnerability that criminals could hack and disrupt.

We then asked whether respondents believe that sufficient security exists to allow the operation of driverless cars. Only one-third (35%) of our respondents felt that there is sufficient security in place for this to happen while the remaining two-thirds (65%) felt that there was not. Security will therefore have to be enhanced substantially to enable many of the connected car use cases that are set to emerge around assisted driving, autonomous driving and other driving based activities such as platooning of vehicles on highways.

Best security option

Of the means available to enhance connected car security – antivirus, firewall, encryption and biometrics – we asked our respondents to select which they see as the best for securing connected cars. Encryption was selected by the majority (54%) of respondents, suggesting that securing data in communication is seen as a priority. Next came biometrics, which was selected by 26.7% of respondents, suggesting that physical identification is seen as important for maintaining privacy, preventing theft and controlling who can use vehicles and their systems.

Firewalls were selected by 15.5% of respondents as the best means to secure connected cars, with this set of respondents looking to secure the vehicle and the back end as a priority. Finally, just 3.7% of respondents selected antivirus technologies as the best means to secure connected cars.

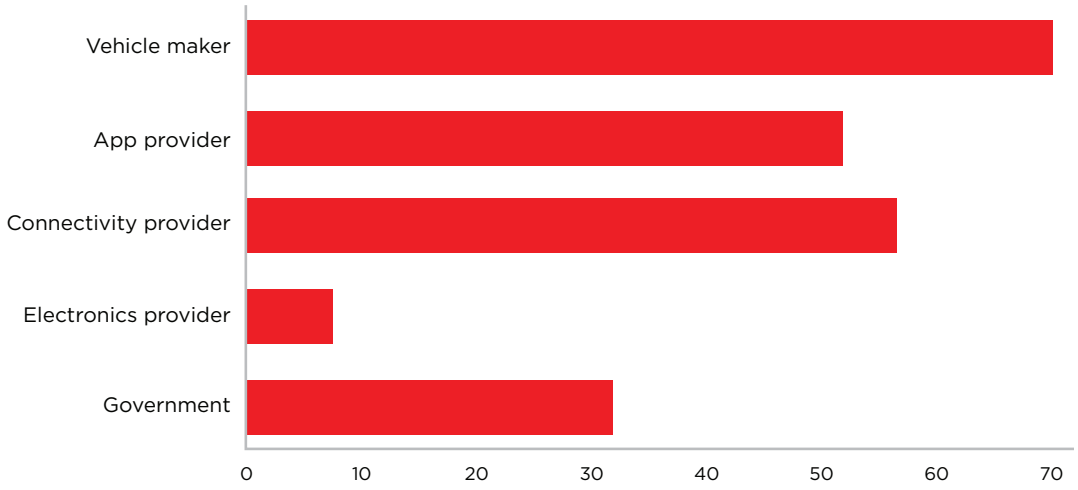
Realistic timeframe for security

In spite of the current opinion that security is insufficient to enable autonomous driving, respondents feel issues can be addressed in the relatively near future. We asked them how long they think it will take to create an acceptably secure connected car environment.

A highly positive 4.2% felt this environment could be achieved in less than 12 months, while the majority of respondents (53.7%) thought an acceptably secure environment could be created in one to three years. The pessimists accounted for 43.1% of respondents who stated that it will take more than five years to create an acceptably secure environment.

However, once development has been undertaken there was a consensus among 77.4% of respondents that security will be trusted enough to enable autonomous vehicles to take off. Less than a quarter of respondents (22.6%) felt that security will not become trusted enough for the technology to take off. There are other issues to consider here, including consumer unfamiliarity with autonomous driving so it may be the case that security concerns ultimately prove not to be the most significant barrier for autonomous driving to overcome.

Who will be responsible for the data privacy aspect of telemetry data?



A final element of connected car security we explored was which type of organisation will be responsible for the data privacy aspect of telemetry data. Vehicle makers were chosen by the largest segment of our respondents (31.9%) as the organisations responsible for data privacy, followed by connectivity providers, which were chosen by 25.9% of respondents. Application providers were the organisations chosen as responsible for data privacy by 23.6% of our survey base while governments were selected by 14.8% of respondents.

Electronics makers were selected by just 3.7% of respondents, suggesting that this group are not yet perceived as data gatherers or storers to the extent that application and connectivity providers are.

Sponsored by:

Volkswagen

IN-CAR SERVICES

Sponsor's Comment: Volkswagen

"Stay connected with Volkswagen Car-Net

New, practical services and useful apps: this is the world of Car-Net. For individual navigation services or connecting your vehicle to your smartphone: You'll find all the options offered by the apps and services from Volkswagen.

App-Connect – three innovative technologies that allow you to bring smartphone apps on to your infotainment system's touchscreen: MirrorLink(R), Apple CarPlay™ and Android Auto™.

With the "Guide & Inform" Services you will be better informed while driving. For example get news that you are really interested in, search for POIs or keep an eye on the real time traffic situation.

"Security & Service" offers you mobile access to important vehicle functions and combines security with transparency for even more comfort. Whether for Service Scheduling, Automatic Accident Notification, Breakdown Call or the Online Anti-Theft Alarm, get support for every situation with all the key information you need."

To begin this section of the survey we focused in on the technologies that are transforming what can be done in connected cars. First, we asked our respondents where they see predictive intelligence transforming connected cars. We asked them to choose from a list of functionality that would be enabled by predictive intelligence. The most popular response was for vehicle maintenance which was chosen by 76.3% of respondents, this was followed by using predictive intelligence for avoiding traffic jams, which was selected by 74.9% of respondents.

Location-based services were the next most frequently selected capability, chosen by 64.6% of respondents. This was followed by applying predictive intelligence for navigation based on user behaviour, which was selected by 62.8% of respondents.

Less popular was using predictive analytics for upselling content and applications, which was selected by 29.3% of respondents, suggesting privacy concerns among respondents.

We then asked what respondents see as the most exciting, new innovative IoT initiative in connected car research and development. Autonomous driving was the most popular category and was selected by 31.3% of respondents. It was closely followed by smart cities/smart highways, which were selected by 28% of respondents. After this the relative share of respondents selecting each initiative started to tail off. 18.7% selected advanced driver assistance systems, 11.7% chose smart mobility services and just over 6% chose in-car services.

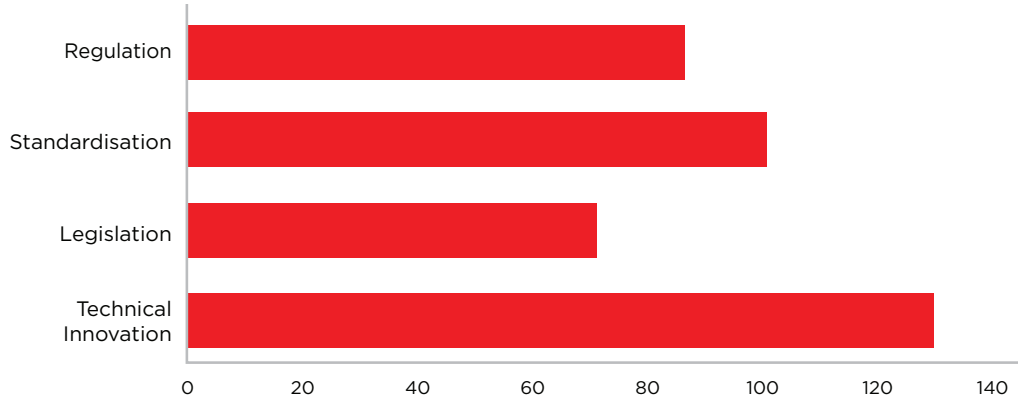
Next we addressed how closely hardware vendors will work with smartphone applications to serve consumers' desires. We asked respondents how they see hardware vendors working with smartphone applications to achieve greater innovation given that users want to control entertainment and other features using voice commands.

There was overwhelming response indicating a strong expectation that the two will collaborate with greater intensity. 49% of respondents agreed that hardware vendors will work very closely with smartphone applications to achieve innovation, while 48.1% thought the two would work together somewhat. Just 2.8% of respondents thought the two would not work together to achieve innovation.

With huge fear in the industry about connected cars taking driver awareness away from the road we asked respondents how automation and connectivity can still ensure safety. Respondents were asked to choose between regulation, standardisation, legislation and technical innovation as means to ensure safety.

The majority (61.6%) of respondents said they thought technical innovation would be the enabler of ensuring connected car safety. 47.9% felt that standardisation would be the enabler, while 41.2% thought it would be regulation and 33.6% legislation. This indicates that technical solutions are still expected to address the concerns of the market and only partial reliance is being placed on regulators, legislators and standards initiatives.

There is huge fear in the industry about connected cars taking driver awareness away from the road. How can we ensure the automation and connectivity provided will support safety?



With this in mind, we then asked respondents about their views on open source software and collaboration. We asked whether they see open source software and collaboration with hundreds of companies working together being seamlessly adopted in connected car innovation over more traditional, proprietary code developed by each car maker.

Unsurprisingly, most responses (53%) said there will be a blend of open source and proprietary activity but among those who thought the market will split along either/or lines, 26.8% felt that open source and extensive collaboration will happen and 20.2% said OEMs and car makers' proprietary code means connected cars will never be fully collaborative, open source environments.

One of the main motivations for manufacturers to develop the next generation of intelligent vehicles further is the hope of creating a transport system with zero accidents, zero fatalities and zero emissions. That's a lofty and distant goal but manufacturer research suggests autonomous vehicles will be safer than those operated by humans. With this in mind, we asked our respondents how safe they think it is to put their lives in the hands of an autonomous vehicle that make all the driver's decisions for them.

The message that autonomous cars can be safer than traditional non-connected cars is well understood and the majority (54%) of our respondents said that this would be the case. Another large group of respondents – 30.5% – didn't see autonomous vehicles being safer but thought they would present roughly the same level of risk as traditional non-connected cars.

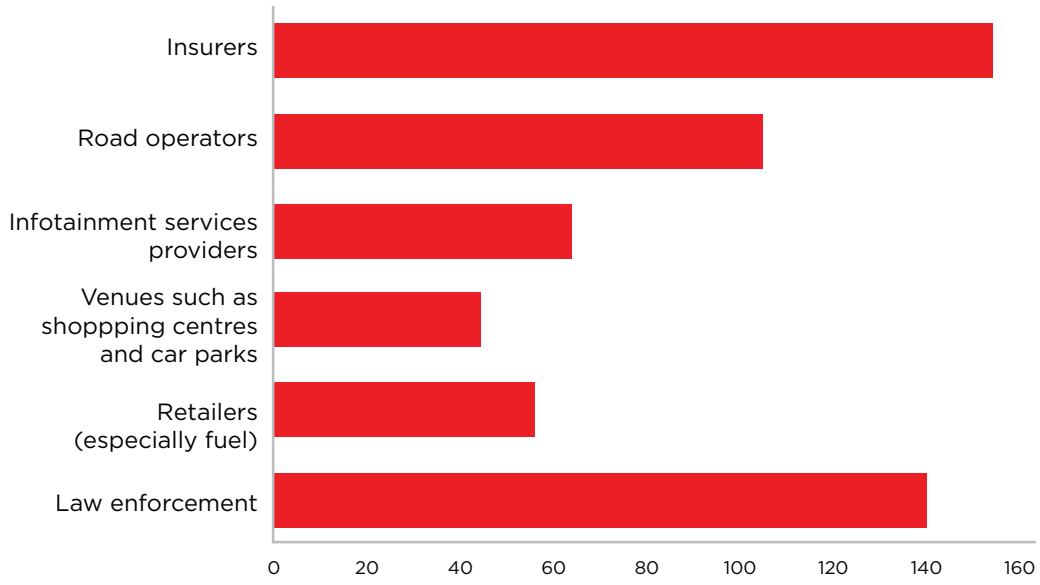
Perhaps considering the immaturity of autonomous driving, standards and technologies, 15.5% of respondents said they felt that autonomous cars would be more dangerous than traditional non-connected cars.

The findings of this question reveal a strong understanding of the benefits of autonomous cars for road safety but reveal some concerns, many of which may evaporate as people become more familiar with the concept and reality of autonomous vehicles.

As connected cars and autonomous vehicles in particular begin to be deployed they will start to collect vast volumes of data about drivers. This data can range from information such as if you drive with no seatbelt or you broke the speed limit, to knowing where you drove to, when you drive and what entertainment or other in-car services you used. This is highly valuable information for many organisations, from insurers to car makers to retailers, road operators and providers of roadside services such as fuel, hotels and restaurants.

The car maker will have access to much of the data from in-car systems and will use it to feed research and development and improve maintenance efficiency. Other organisation would strongly like to access vehicle-related data so we asked our respondents to identify other organisations, except car makers, will have access to this data.

Connected cars can collect vast amounts of data about drivers, such as if you broke the speed limit or if your seatbelt was unbuckled. Who else besides the automakers will have access to this information?



Insurers were selected by the largest number of respondents (75.9%), who clearly identified the business case for insurers to know more about their customers and the advantages to customers in reduced premiums of sharing such data. Next most popular was law enforcement, which was selected by almost 70% of respondents. In many markets, this will require new legislation and it is unclear the extent to which sharing such data will become mandatory.

Next most widely selected were road operators, which were chosen by 51.7% of respondents, who identified that vehicle data is useful for planning road improvements, managing traffic flows and understanding likely peak time traffic loads.

Just under one third of respondents (31.5%) identified providers of infotainment services as being a group who would have access to such data. These organisations will know what services drivers buy and use it for upsell, cross sell and customer experience management.

Retailers, for fuel in particular, were selected by 27.6% of respondents, demonstrating that connected car data is of huge value for planning store locations, understanding buying habits and preferences and marketing effectively to drivers of connected vehicles.

This was emphasised by 21.7% of respondents which selected venues such as shopping centres and car parks which could extract similar insights and value from connected car data.

Finally, we asked our respondents whether they thought these petabytes of individual connected car data would be sold with the user's consent. Encouragingly, the majority (61.7%) said this would not happen, demonstrating that organisations are becoming mature about how they respect users' privacy and looking to get user opt-in for data sharing.

However, the remaining 38.3% felt the data would be sold without the users' consent, creating distrust among drivers. In many markets such activity will be illegal but it remains a concern in many consumers minds that needs to be clearly addressed so greater levels of trust can be created.

Sponsor's Comment: Gemalto

CLOSING SUMMARY

This survey shows a transportation industry at the precipice of transformation, changing the way we drive and interact with our environment.

The survey findings indicate tremendous growth for the entire ecosystem with the greatest monetization potential for carmakers, MNOs and service providers. Results also indicate that expanding connectivity and emerging 5G and NB-IoT technologies are key to growth. In addition, data privacy and solid identity management are high on the list of requirements to earn consumer trust in connected cars. Ubiquity of service, adequate bandwidth, security, and the ability to manage technology for the long life of vehicles are thus essential for reliable and trustworthy connected cars.

The timeline to next gen smart cars and autonomous driving will rely heavily on enabling technologies. These include mature technologies such as telematics and navigation, emerging solutions such as insurance telematics, predictive intelligence designed to eliminate accidents and traffic delays, as well as evolving solutions like advanced IoT platforms, security solutions and secure over the air platforms that allow updates and lifecycle management.

As connected cars converge with smart cities and new mobility schemes, V2V and V2I connectivity becomes imperative. Developing and funding infrastructures will depend on cooperation from the entire ecosystem as well as emerging standards, harmonized frameworks and both open source and proprietary code.

The Mobile World Live survey provides important insight on the forces and technologies shaping the evolving transportation landscape. We hope it serves all IoT stakeholders in developing successful strategies to Connect, Secure and Monetize™ our world of new mobility, through solid Identity Management.

MOBILE WORLD LIVE

Produced by the mobile industry for the mobile industry, Mobile World Live is the leading multimedia resource that keeps mobile professionals on top of the news and issues shaping the market. It offers daily breaking news from around the globe. Exclusive video interviews with business leaders and event reports provide comprehensive insight into the latest developments and key issues. All enhanced by incisive analysis from our team of expert commentators. Our responsive website design ensures the best reading experience on any device so readers can keep up-to-date wherever they are.

We also publish five regular eNewsletters to keep the mobile industry up-to-speed: The Mobile World Live Daily, plus weekly newsletters on Mobile Apps, Asia, Mobile Devices and Mobile Money. What's more, Mobile World Live produces webinars, the Show Daily publications for all GSMA events and Mobile World Live TV – the award-winning broadcast service of Mobile World Congress and exclusive home to all GSMA event keynote presentations.

Find out more www.mobileworldlive.com

THANKS TO ALL OUR SPONSORS FOR THEIR SUPPORT OF THIS REPORT

gemalto
security to be free

European Global Navigation Satellite Systems Agency

CISCO

INTERDIGITAL

f5

Volkswagen