Hello Car

Future-proofing industries through interconnection ecosystems – the digital car as a model

By Ivo Ivanov, CEO of DE-CIX International

Industries worldwide are entering into a new era of digitalization, everywhere, for everything, making performance, resilience, and security in network connections business-critical. An increasing number of enterprises from segments like healthcare, finance, retail, logistics, and automotive have been discovering the benefits of connecting with their digital value chain via an Internet Exchange, reports Ivo Ivanov, CEO of DE-CIX International.

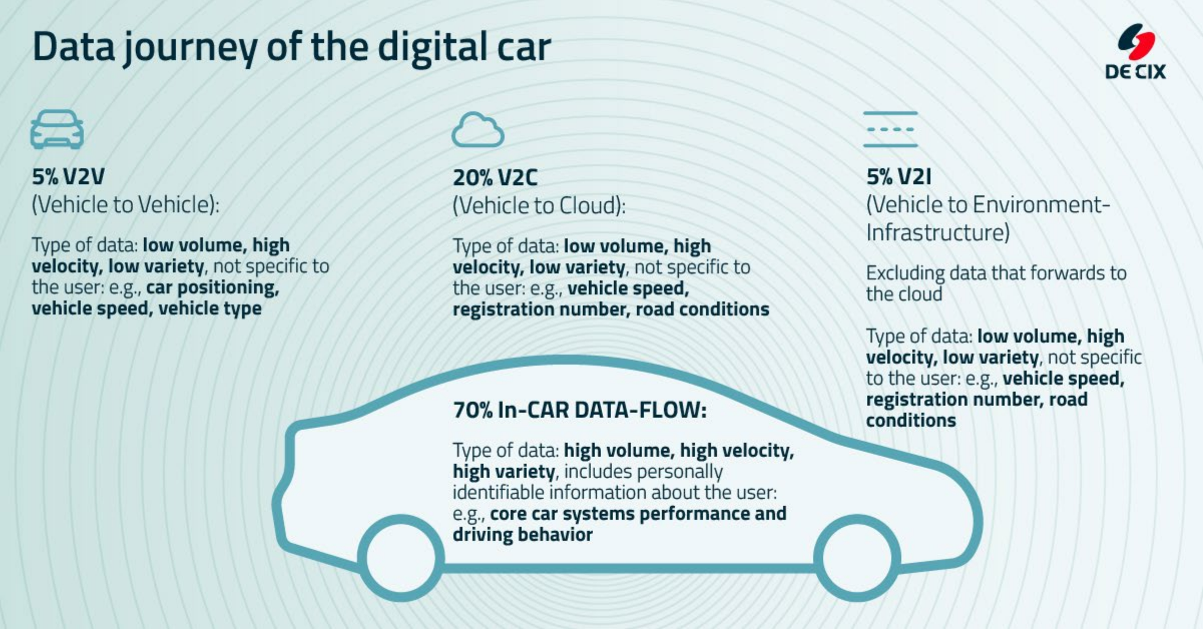
In the digital world, performance, resilience, and security in network connections are business-critical. Enterprises need the fastest reaction times and the highest resilience, which together improve the performance and the reliability of applications and services. Furthermore, in the increasingly complex world of digital business – where companies exchange data with one another for the provision of digital services and applications across national borders and regulatory regions, in a platform economy – it is crucial to reduce the complexity of the relationships and ensure that partners comply with policy and legal requirements. Finally, the highest level of security on the data transmission and the network is indispensable. To guarantee great performance and the highest level of security possible, enterprises from all verticals require that their network is directly and redundantly connected to the required application and content networks. Doing this via a highly secure, high-performance Internet Exchange (IX) means that the demand for resilience, security, and fast reaction times can be fulfilled in a simplified manner and – backed by Service Level Agreements (SLAs) – guaranteed.

While Internet Exchanges have traditionally been seen as locations where telecommunications companies (carriers), Internet service providers, content networks, and content delivery networks interconnect to exchange data, we are now seeing an increasing number of participants joining from other industry segments, like healthcare, finance, retail, logistics, and of course, automotive.

As an early adopter, the automotive industry has already started reaping the benefits of interconnection over IXs. This is because the digital car is a prime example of a digital product – one where the manufacturers simply cannot afford to cut corners on the performance, resilience, or security of their networks. The efficacy and the privacy of their connections to other networks to exchange data are paramount to the provisioning of the many services and features that make the digital car what it is, and any lapses will impact strongly and immediately on the reputation of the car brand.

Joining the platform economy

At the same time, industries worldwide are entering into a new era of digitalization; everywhere, for everything, and for everyone. This requires rethinking and restructuring business models. Digital business models based on the platform economy are now offering distinct competitive advantages for globally acting enterprises, which take them beyond the capabilities of traditional industrial setups. New players are now presenting a clear competitive challenge – for example, in the area of autonomous driving and car applications – to the traditional automotive sector. Therefore, car manufacturers are needing to shore up their space in the platform economy and interconnect with their suppliers, service providers, and customers in new and optimized ways in order to control the data journey of their cars.



Data journey of the digital car

DE CIX

5% V2V
(Vehicle to Vehicle):

Type of data: **low volume, high velocity, low variety**, not specific to the user: e.g., **car positioning, vehicle speed, vehicle type**

20% V2C
(Vehicle to Cloud):

Type of data: **low volume, high velocity, low variety**, not specific to the user: e.g., **vehicle speed, registration number, road conditions**

5% V2I
(Vehicle to Environment-Infrastructure)

Excluding data that forwards to the cloud

Type of data: **low volume, high velocity, low variety**, not specific to the user: e.g., **vehicle speed, registration number, road conditions**

70% In-CAR DATA-FLOW:

Type of data: **high volume, high velocity, high variety**, includes personally identifiable information about the user: e.g., **core car systems performance and driving behavior**

Figure 1: From maintenance data to navigation and infotainment: The data journey of the digital car involves many different kinds of data that need to be sent to or received from a range of service providers and suppliers.

By choosing an IX platform that already has an established and vibrant ecosystem of diverse kinds of networks, a car manufacturer can position itself right on the spot, where the digital economy is already playing out and where the future is being molded. The chances are high that the networks the car maker needs to interconnect with are already participating in these ecosystems. An IX enables direct interconnection between these parties, using the very efficient principle of one-to-many or many-to-many, and aggregating the traffic instead of using multiple bilaterals. Beyond this, if the automotive manufacturer creates its own closed and secure private ecosystem within the existing IX environment, the geographical distance to the other networks – and thus the reaction time (latency) – is minimized, resilience is ensured, and the car maker is rewarded with a substantial boost in the security of its networks, and, therefore, of its data. This can be further enhanced by additional security solutions provided by the Internet Exchange operator. The result is that the automotive manufacturer can have the best of all worlds when it comes to connectivity – high-performance, reliable, and secure interconnection to enhance and protect their digital products and to satisfy and protect their customers.

Creating interconnection ecosystems for industries – the digital car as a model

The digital car is a digital ecosystem entailing a huge variety of types of data. This includes data relating to physical safety and the physical conditions on the road, data for improving traffic management, data on the status and maintenance of the car, data on the provisioning of infotainment and entertainment and other services according to personalized preferences, and the list goes on.

We see three overriding challenges that car makers are confronted with in dealing with the exchange of these many different types of data with many different partners and service providers. Firstly, there is the provision of services and features smoothly and with fast reaction times (this is dependent on the performance and reliability of the connectivity to other networks). Secondly, there is the fulfillment of compliance requirements for multiple regions around the globe where the car may be sold or driven (leading to high levels of legal and regulatory complexity, increasing exponentially with the number of networks and service providers involved). Finally, there is the security of the network in order to ensure that neither the identity of the driver nor that of the car itself can be abused and that the car is protected from hijacking or any form of unauthorized manipulation.

Previously, the approach for automotive manufacturers was a best-effort solution involving Multiprotocol Label Switching (MPLS) and IP transit (upstream), with no end-to-end control of the traffic flows between the car and the networks wanting to deliver data to or receive data from the car. This solution creates a range of challenges for the networks: The more intermediates between two networks, the higher the latency, the greater the risk of performance and security issues, and the more complex compliance becomes – because if you do not control the data value chain, you cannot control any of this.

But at the same time, there's also no need to go throwing the baby out with the bath water or reinventing the wheel: Existing MPLS and IP transit solutions can be enriched and complemented with interconnection services via an Internet Exchange, offering additional redundancy along with capitalizing on the ecosystem around the IX to ensure the optimization of performance and resilience, as well as increasing security.

With the central challenges – performance/reliability, complexity/compliance, and security – in mind, it is clear that choosing the best interconnection solution is crucial to the long-term market positioning of the car manufacturer.

How connectivity issues can impact brand reputation

Let's look firstly at performance and reliability. Whether a chauffeured businessperson is attending video conferences on the road, a salesperson needs to be well connected to business applications when underway on business; whether a harried car owner is further delayed by the slow reaction of their car door to their mobile phone key, or the children in the back seat want to stream games or videos on a long drive, even – in the not-too-distant future – that the car itself becomes the complete fifth screen; all of these scenarios (and the many more digital services that automotive manufacturers are dreaming up for the comfort and delight of their customers and passengers) require a very strong, reliable, and high-performance connectivity infrastructure behind them. If the connectivity performance is poor and digital services cannot be consumed as expected, the responsibility for such failings will land squarely on the shoulders of the car maker, with the accusation that their digital products are not properly connected.

Interconnecting with partners via an Internet Exchange enables aggregation in an improved latency to the location of the car, and therefore with improved stability and reaction times. Because at an IX, automotive networks are enabled to meet in the most direct and shortest way with all the data suppliers and buyers that are currently important to them – as well as those that in the future are likely to become important. With a direct interconnect, coupled with a closed user group (CUG) specifically designed for enterprise interconnection, the connection on the network side can be ideally optimized, reducing latency to the other provider networks and data centers involved and significantly improving the performance of digital services and applications within the digital car.

The automotive manufacturer as custodian of personal privacy

Secondly, the topic of compliance, in particular with – but not limited to – data protection, has become a serious headache for many a car maker. There is just so much sensitive data in a digital car. The sensor system in the closed environment of the digital car has the capacity to ascertain information about the driver’s state of health, emotional state, concentration capacity, behavior behind the wheel, even the driver’s state of inebriation – in a nutshell, the fundamental character and physical condition of this person. But beyond this, with the aid of artificial intelligence, the car’s sensors can pick up other insights into the behavior of not only the driver but also passengers: the location of the vehicle, destinations of travel and any stopovers, the identity of passengers, the identity of communication partners, and so on. This is highly sensitive information, which concerns the core of our fundamental rights. Thus, the digital car – and, as a result, the car maker – becomes the custodian of personal privacy.

Alongside this is the need to protect the intellectual property of the car manufacturer in the sharing of data with partners along the data value chain. As a result, clear contractual relationships and agreements between business partners are a necessary, but increasingly complex, undertaking.

Controlling compliance through connecting individually to each partner network and forging individual bilateral relationships – as has been done in the past in the automotive industry – is not a future-oriented approach for the digital car. Such a solution does not scale well to larger ecosystems involving a greater number of players wishing to interconnect intelligently. Bearing in mind the hundreds – potentially thousands – of organizations around the world delivering data to and/or receiving data generated by the digital car, the result of this approach is literally thousands of bilateral interconnections and relationships – something that nobody can efficiently manage.

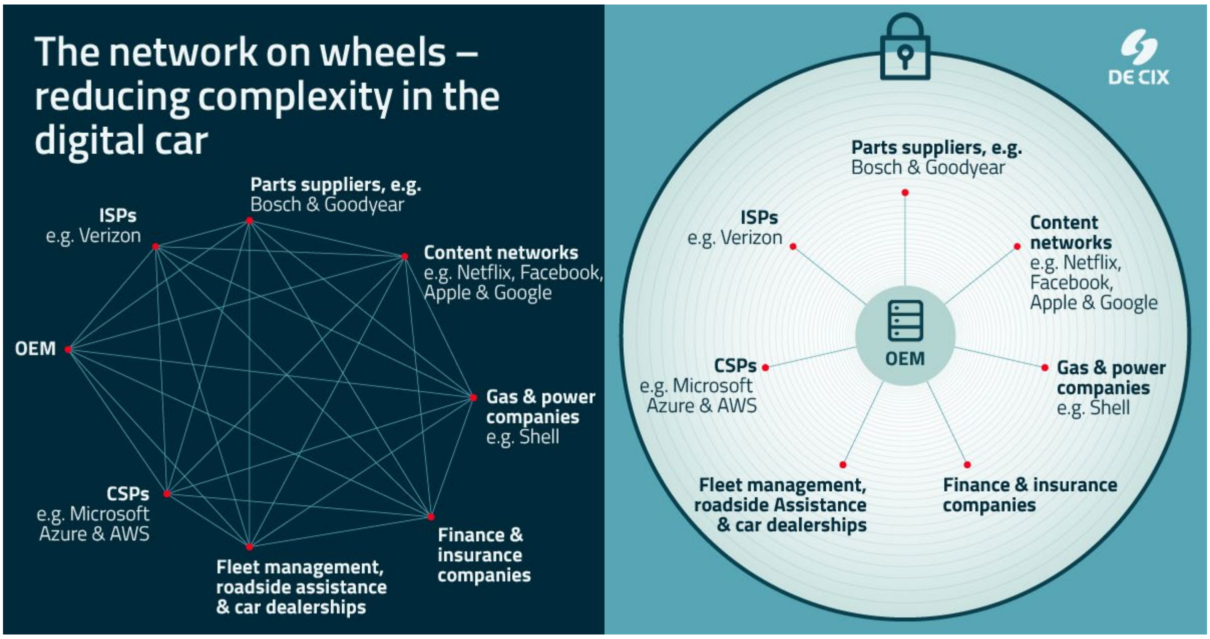

The network on wheels – reducing complexity in the digital car
ISPs e.g. Verizon
Parts suppliers, e.g. Bosch & Goodyear
Content networks e.g. Netflix, Facebook, Apple & Google
OEM
Gas & power companies e.g. Shell
CSPs e.g. Microsoft Azure & AWS
Finance & insurance companies
Fleet management, roadside assistance & car dealerships
DE CIX
Parts suppliers, e.g. Bosch & Goodyear
ISPs e.g. Verizon
Content networks e.g. Netflix, Facebook, Apple & Google
CSPs e.g. Microsoft Azure & AWS
OEM
Gas & power companies e.g. Shell
Fleet management, roadside Assistance & car dealerships
Finance & insurance companies

Figure 2: The complexity of controlling the compliance of many partners can be overcome by creating a secure and private closed user group, with the OEM’s compliance policies a prerequisite for participation by partner networks.

Overcoming the complexity of global compliance needs

There’s another way to deal with this challenge: If an Internet Exchange operator provides the automotive manufacturer with a closed, secure, and private interconnection environment in the form of a closed user group (CUG) in which policies for compliance requirements are enabled, then fulfillment of these policies can function as a prerequisite for all the participants of the group, and this can be efficiently controlled. This can even be undertaken per market, per regulatory region, even at a federal or state level.

Multiple adjacent CUGs can be owned and operated by the car maker to take care of conflicting regulations while always maintaining its own company policies. For example, a manufacturer could set up three separate CUGs in the digital hub Frankfurt (capitalizing on the proximity of the dense ecosystem of networks there), with one corresponding to EU law, one to UK law, and a third according to the compliance requirements in the USA. Equally, a set of adjacent CUGs could be set up on an IX platform in any of the world's strong digital hubs – like New York to serve the North American regulatory environment, Madrid to serve Southern Europe, and Mumbai to serve the Indian subcontinent. By locating the CUG within the region it serves, getting closer to the ground where the car is on the road, performance and reliability can clearly also be optimized.

While the topic of sensitive data paints a particularly vivid picture of the compliance issue, compliance is not only about data protection. There are countries with different regulatory requirements for cloud concentration risk mediation plans, others with different security requirements as to data transmission, data reception, and data sharing. There are industry-specific regulations for individual sectors, such as the automotive and finance industries. All this could then be implemented according to the needs of the enterprise that owns the CUG.

Mitigating the risk of malicious third parties lurking under the cover of anonymity

The issue of security is even more critical. One of the most highly charged threat scenarios for the digital car is the potential theft of the identity of the driver (that a crime could be committed in the guise of an innocent car owner) or of the car itself as an IoT device (that the car could be hijacked, manipulated technically, or in the worst case even weaponized). What can be done to mitigate this risk? The approach of the closed environment offered by a CUG, being very direct and close to the action, means that security can be substantially improved. This is possible, firstly, because of the direct interconnection of the networks. The fewer intermediary transporters there are between the automotive network and the network of the legitimate data supplier/recipient, the fewer possibilities there are for anonymous third parties to lurk in the shadows. The reason for this is anchored in the logic of direct interconnection, also known as "peering". By peering at an IX – and especially within a closed and private environment on the IX platform – it is possible to know exactly which network is sending traffic and which is receiving it, therefore disallowing anonymity among the networks or any lack of transparency as to the traffic source and destination.

In contrast, this is not possible with IP transit, the traditional approach to automotive connectivity. With IP transit, the car manufacturer's only option is to place its traffic into the hands of a transit provider, who, in turn, announces the packet requests back to the global Internet – to a variety of recipients and senders that the car maker does not and cannot know. The risk entailed in this anonymity is that criminals can hide behind it.

Connecting partners – the digital car of the future is a network on wheels

If, instead, data is sent to an automotive manufacturer network via a secure closed user group on an IX platform, then the manufacturer knows exactly which network has sent it. This network is known, the connection having been checked using BGP and Layer 2 validation instruments, meaning that the risk of hijack or a DDoS attack originating from this network is much lower – because this network cannot hide or mask its identity.

On top of this, if the Internet Exchange operator is able to provide additional security mechanisms to reduce the danger of route hijacks, to prevent IP hijacking, and to protect networks from DDoS attacks, then the digital car and its ecosystem are well protected against the most significant risks of the Wild West of the open Internet. In this way, the already secure filtering logic of a closed peering user group is further enhanced through additional security tools specifically developed to protect networks.

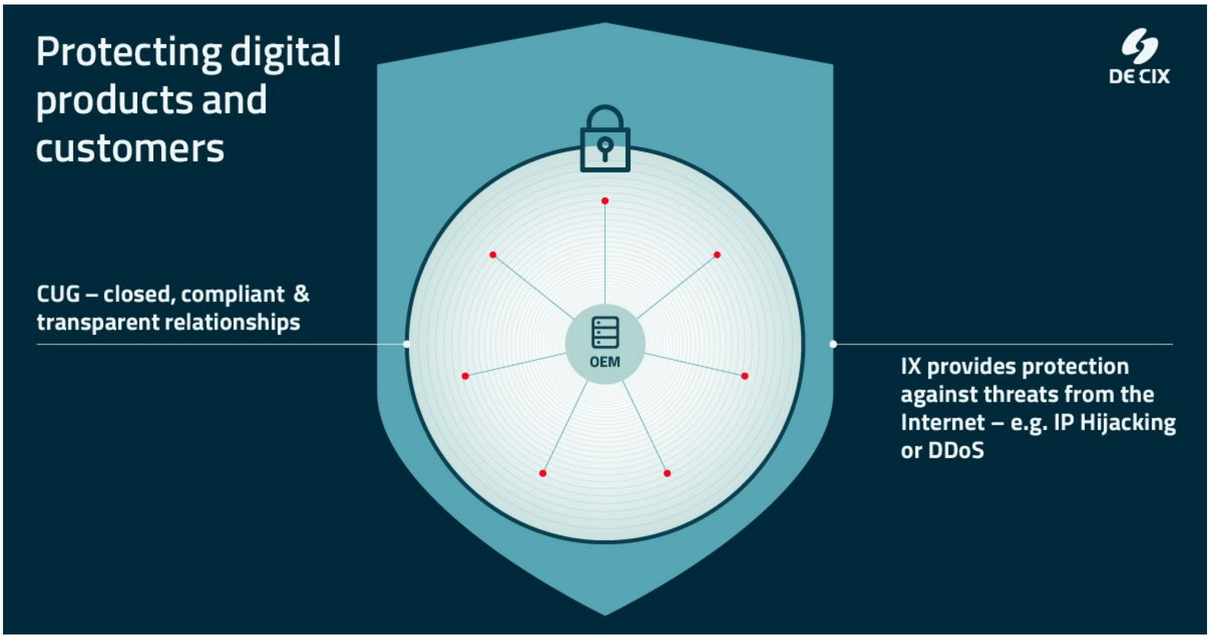

Protecting digital products and customers
DE CIX
CUG – closed, compliant & transparent relationships
OEM
IX provides protection against threats from the Internet – e.g. IP Hijacking or DDoS

Figure 3: Multiple layers of security: The secure ecosystem of the closed user group can be further protected by additional security services provided by the Internet Exchange operator.

As we have seen, many of the challenges faced by car manufacturers in implementing connectivity for the digital car can be solved using the logic of secure interconnection within a vibrant digital ecosystem, via an Internet Exchange like DE-CIX – home to the largest neutral ecosystems in the world. Directly interconnecting with partners, using the very efficient principle of one-to-many or many-to-many and controlling for compliance, we see one clean environment – a secure, private, and simplified platform – where the automotive network can interconnect with all the participants in the data value chain. Locating this exclusive, closed environment within a secure, resilient, neutral, and high-performance Internet Exchange means that the participants can interact in a single protected and highly efficient environment. In this way, automotive manufacturers can prepare for the bright future of the digital car, the network on wheels.

This same logic – of interconnection with partners for a smooth and safe data journey – applies just as well to other transport sectors, like airlines and logistics suppliers. But it also applies to all industries entering the platform economy – banks, e-health system operators, the hospitality sector, e-manufacturing with its global supply chains, and many more in future. Closed, secure, and private interconnection environments offer everyone the chance to grow and develop their digital business models with security and resilience baked in.