Grant Thornton
Bharat

Automobile

Cyber security

Service

Auto Bytes

Automotive cyber security regulations and compliance

January 2021

Introduction

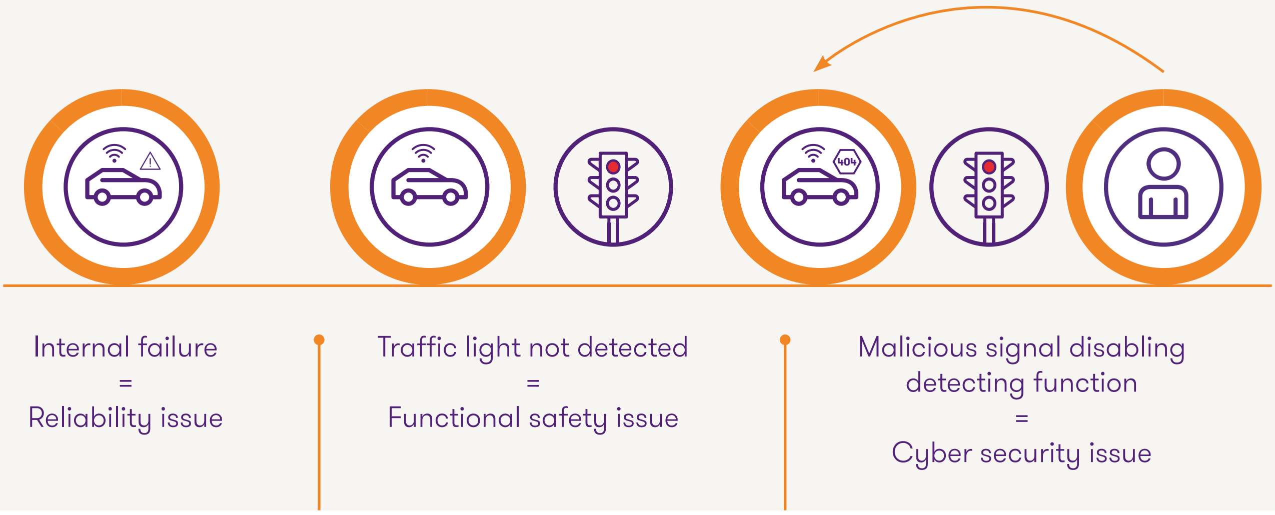
In today's time, as the automotive sector is seeing a paradigm shift through large transformation initiatives such as adoption of digital technologies, connected vehicles, transition to cloud, there has been a growing concern over the risks associated over the cyber realm. Need for cyber dominates the priorities of the sector as it adapts to a post-COVID 19 world.

The automobile sector is investing in software innovations to enhance consumer experience and improvise modern vehicles. These innovations are cashing largely on the digitalisation of in-vehicle systems, extending it to the back end and propagating softwares to pack modern technologies in today's vehicles. The demand for vehicle-to-vehicle (V2V) connectivity technology and incorporation of Internet of Things (IoT) has increased the number of cloud-based applications and advanced technology in new forms of mobility, including connected and autonomous vehicles.

In the coming three years, about 1.2 billion motorised vehicles are likely to have connected features wherein the demand for connected and autonomous vehicles will grow more than five times to USD 212 billion by 2027. The average vehicle today contains up to 150 electronic control units (ECUs) and about 100 million lines of software code. With every line of code, the cyber risk to the connected vehicles increases. The number is projected to reach 300 million lines of code by 2030.

This emergence of autonomous vehicle technology is a key trend raising demand for advanced features; however, this is also resulting in cyber threats. As Original Equipment Manufacturers (OEMs) deal with this one-of-a-kind threat, the challenge has become severe in the post-COVID world.

The representation below illustrates the differences between reliability, functional safety and cyber security issues



Internal failure
=
Reliability issue

Traffic light not detected
=
Functional safety issue

Malicious signal disabling detecting function
=
Cyber security issue

The looming cyber threats specifically in terms of data confidentiality and protection have posed pressure on the automobile sector. The cyber security automotive regulations provide a need to develop solutions with required cyber measures in vehicles. Some of the measures include hardware and software vulnerability discovery, reverse engineering, cyber forensics and specialised tools and facilities. This will help industry and government analyse how to integrate security and technology. Moreover, effective compliance programmes are likely to ensure minimal cyber threats.

In the automotive cyber market, cloud security is growing at a CAGR of 29.4%, thereby representing a great revenue generation opportunity for OEMs. According to Data Security Council of India (DSCI), the Indian cyber security services industry is expected to grow to USD 7.6 billion in 2022. Moreover, with the influence of the World Forum for Harmonization of Vehicle Regulations (WP.29) which is a worldwide regulatory forum within the institutional framework of the UN Economic Commission for Europe (UNECE)- the UNECE WP.29 regulation on cyber security and software updates displays a broad adoption of the regulation across the world. Interfaces and communications are considered as key elements for evaluating the cyber security of a system. The analysis of such high-level system threat in a specific context commonly referred to as a threat modelling and is documented in the automotive sector through a model called threat analysis and risk assessment.

Mitigation is a challenge that requires:

- Development environment access control
- Technology tools
- Informed operator responsiveness

The WP.29* regulations

The automotive regulations require OEMs & relevant third parties to implement measures in areas related to:

- Managing vehicle cyber risks
- Securing vehicles by design to mitigate risks along the value chain
- Detecting and responding to security incidents across vehicle fleet
- Providing secure software updates and ensuring vehicle safety is not compromised
- Data protection and privacy of customers

Risk assessment standards

The International Organization for Standardization/Society of Automotive Engineers (ISO/SAE)** standards provide enough common ground to allow the automobile sector to produce consistent cyber security practices for the development of the next generation of connected vehicles.

In addition, to WP.29 regulation, the ISO is developing automotive cyber security standards. The ISO/SAE* 21434 standard establishes 'cyber security by design' throughout the entire lifecycle of the vehicle.

It provides the model for developing a risk assessment system and specifies details on processes and work products.

*The WP.29 regulation defines the automotive cyber security requirements to approve vehicles based on type (cars, vans, trucks and buses) and the certificate of compliance for the Cyber Security Management System (CSMS)

**ISO/SAE standard 21434 hopes to establish clear technical and procedural requirements for each stage of the vehicle's life cycle

Our view

Automotive technology has raised concerns about the cyber threats to connected vehicles and induced the sector to rethink of cyber security risks along the entire value chain.

The rise in electric vehicles, IoT, connected vehicles and the seamlessness of the technology within, has resulted in a surge in cyber risks across the ecosystem. A collaborative approach may be required to overcome the investments in time, money and broader organisational changes. The reality is that cybercrimes could generate millions in losses to the automotive sector. Paving way to new approaches of cyber security applied to the automobile sector, which must be flexible and adaptive along the production chain and the lifetime of CAVs. It is imperative that the auto players focus on cyber threats while the systems are being designed to ensure security by design. They should also keep a close eye on the evolving cyber threats to ensure systems are updated more frequently.

There is a need to make the integration of cyber security practices as practical and easy as possible for automotive stakeholders. Hence, OEMs need to engage with the cyber community, working together with government, private-sector firms, standards organisations, academia, research and testing facilities, to face the cyber challenges and deepen the knowledge of automotive cyber security technologies and best practices. The automotive sector players will also need to enhance their in-house cyber capabilities in order to ensure the systems are resilient and also supports the end consumer with ongoing security monitoring giving them an added trust and confidence.

Given the scale of challenges ahead, the industry is likely to experience a considerable disruption in the coming years, as OEMs support their own cyber security capabilities and new players enter the value chain with dedicated cyber security offerings cyber security is a constant race between attackers and defenders, and for the automobile industry.

Key consideration for overall cyber assurance

01 SOC 1 /2 attestation

02 ISO 27001 Certification assistance and compliance

03 Data privacy & protection

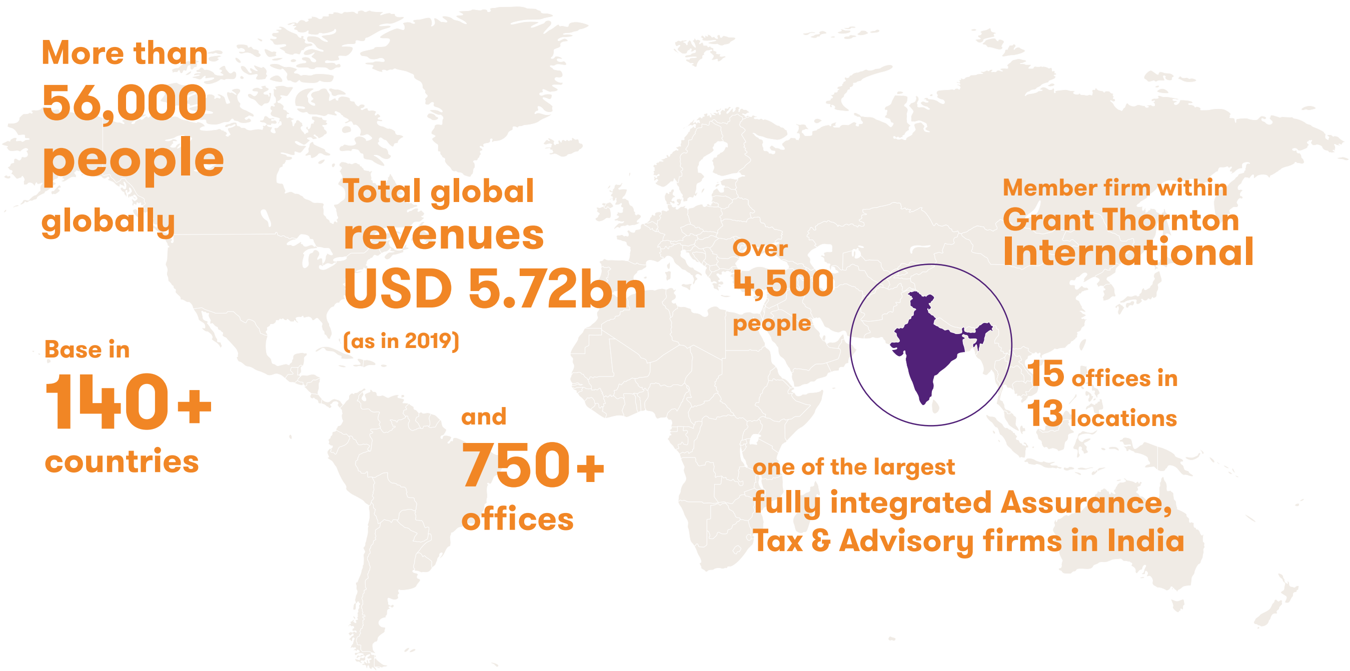
04 Connected vehicle technology risk assessment

05 Application security (IT & OT)

06 Supply chain third party risk assessment

Sources: Data Security council of India
UNECE
Mckinsey Report on Mastering the challenge
Bureau of Indian Standards

About Grant Thornton



More than **56,000 people** globally

Total global revenues **USD 5.72bn** (as in 2019)

Over **4,500** people

Member firm within **Grant Thornton International**

Base in **140+** countries

and **750+** offices

15 offices in **13** locations

one of the largest **fully integrated Assurance, Tax & Advisory firms in India**

6 compelling reasons to consider Grant Thornton

01 A truly global organisation

02 Proven global credentials

03 A single global audit approach

04 A different way of doing business

05 Deep expertise in non-audit services

06 Strong local expertise

To get in touch with our Risk and Cyber experts, contact:

Saket Mehra
Partner and Automotive Sector leader
Grant Thornton Bharat
E: Saket.Mehra@IN.GT.COM

Akshay Garkel
Partner, Cyber
Grant Thornton Bharat
E: Akshay.Garkel@IN.GT.COM

Rohit Das
Director, Cyber
Grant Thornton Bharat
E: Rohit.Das@IN.GT.COM

Priyanka Mehra
Manager, Risk
Grant Thornton Bharat
E: Priyanka.Mehra@IN.GT.COM

Contact us

To know more, please visit www.grantthornton.in or contact any of our offices as mentioned below:

NEW DELHI
National Office,
Outer Circle, L 41,
Connaught Circus,
New Delhi - 110001
T +91 11 4278 7070

NEW DELHI
6th Floor, Worldmark 2,
Aerocity,
New Delhi - 110037
T +91 11 4952 7400

AHMEDABAD
7th Floor, Heritage Chambers,
Nr Azad Society,
Nehru Nagar,
Ahmedabad - 380015

BENGALURU
5th Floor, 65/2, Block A,
Bagmane Tridib, Bagmane
Tech Park, CV Raman Nagar,
Bengaluru - 560093
T+91 80 4243 0700

CHANDIGARH
B-406A, 4th Floor,
L&T Elante Office Building,
Industrial Area Phase I,
Chandigarh - 160002
T +91 172 4338 000

CHENNAI
7th Floor, Prestige Polygon,
471, Anna Salai, Teynampet,
Chennai - 600018
T +91 44 4294 0000

DEHRADUN
Suite No 2211, 2nd Floor,
Building 2000, Michigan Avenue,
Doon Express Business Park,
Subhash Nagar,
Dehradun - 248002
T +91 135 2646 500

GURGAON
21st Floor, DLF Square,
Jacaranda Marg,
DLF Phase II,
Gurgaon - 122002
T +91 124 462 8000

HYDERABAD
7th Floor, Block III,
White House,
Kundan Bagh, Begumpet,
Hyderabad - 500016
T +91 40 6630 8200

KOCHI
6th Floor, Modayil Centre Point,
Warriam Road Junction,
MG Road
Kochi - 682016
T +91 484 406 4541

KOLKATA
10C Hungerford Street,
5th Floor,
Kolkata - 700017
T +91 33 4050 8000

MUMBAI
11th Floor, Tower II,
One International Center,
SB Marg Prabhadevi (W),
Mumbai - 400013
T +91 22 6626 2600

MUMBAI
Kaledonia, 1st Floor, C Wing,
(Opposite J&J Office),
Sahar Road, Andheri East,
Mumbai - 400 069

NOIDA
Plot No 19A, 2nd Floor,
Sector - 16A,
Noida - 201301
T +91 120 485 5900

PUNE
3rd Floor, Unit No 309-312,
West Wing, Nyati Unitree,
Nagar Road, Yerwada
Pune - 411006
T +91 20 6744 8800

For more information or for any queries, write to us at contact@in.gt.com

Follow us @GrantThorntonIN

"Grant Thornton Bharat" means Grant Thornton Advisory Private Limited, the sole member firm of Grant Thornton International Limited (UK) in India, and those legal entities which are its related parties as defined by the Companies Act, 2013, including Grant Thornton Bharat LLP.

Grant Thornton Bharat LLP, formerly Grant Thornton India LLP, is registered with limited liability with identity number AAA-7677 and has its registered office at L-41 Connaught Circus, New Delhi, 110001.

References to Grant Thornton are to Grant Thornton International Ltd. (Grant Thornton International) or its member firms. Grant Thornton International and the member firms are not a worldwide partnership. Services are delivered independently by the member firms.