

# In Vehicle Safety and Cyber Security Model

Gururaj Basavaraj  
Cyber Security Design Engineer

**Abstract:** Cyber security is a standard defining requirements and providing guidelines for achieving security related functionality incorporated into E/E systems installed in road vehicles, Cyber security is becoming a critical parameter for consumer and manufacturers as cyber security helps to eliminate vehicle recalls through Over The Air programming(OTA), OTA has got number of potential vulnerabilities without proper security, The vulnerable factors motivated L&T TS to design and develop In Vehicle Safety and Cyber security Framework (“I.V.V.C,S,”) that solves these complex challenges, helping automotive manufacturers reduce the cost and time required for automotive standard whereas accelerating innovation in their safety-intensive products the organizations are creating dedicated cyber security safety teams at different organization levels to achieve secure products, which is adding additional 20% to 50% effort/cost based on the features that need be supported.

**Keywords—** “I.V.V.C,S,”, OTA, Secure Algorithm, “I.V.S.C,S,,” Crypto.

## I. INTRODUCTION

In vehicle safety and Cyber security model addresses the vulnerabilities of the critical functional components. The objective of the “I.V.S.C.S.” is to provide freedom from unacceptable threats and risks that can damage the vehicle by hacking. The increasing complexity of systems way beyond the vehicle itself Ensuring reliable design and verification of the components used in these systems, including compliance with industry standards on Risk Management and quality, is critical for success in this highly competitive market for all Tier 1 Manufacturers and Service providers to meet Automotive OEM expectations.

## II. APPROACH TO CONCEPT

### A. History

The modern cars are coming up with more connected features along with internet to other cars this is expected to increase in future.

This is creating an environment where security is going to be critical topic that needs to be addressed.

At L&T Technology Services, we have a Cyber Security experts working on customer projects with security and safety requirements on the following activities:

- Secure model life cycle design
- Secure model Design and development.
- Manage all development artifacts and processes in a single data model.
- Secure service layer development and integration

### B. Evolution

At L&T technology services, we have come up with an approach to incorporate the “I.V.S.C,S,,” model in the existing system and software development life cycle process.

The idea behind this process is to incorporate the “I.V.S.C,S,,” model which will create a secure platform that the products standards are getting increased.

### C. Future

The expected functional change in the automotive industry is that the vehicle recalls should be completely reduced that paves way for advanced technologies for automotive domain. “I.V.S.C,S,,” is proprietary of L&T technology services and its customers, we are confident that we can contribute much more in coming days.

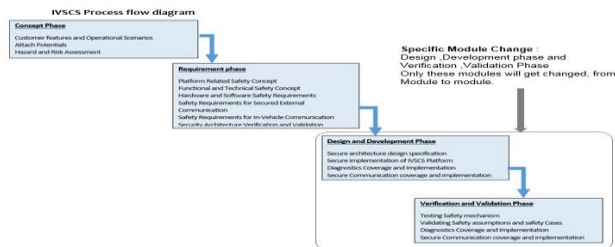
## III. METHODOLOGY

at L&T technology services we adhere to the new methodology along with existing Design and Software development life cycle

- All the challenges of security loop holes are mitigated in the process of design and development.
- Independent Plug and Play Feature for Secured Layered Services, with generic Interfaces of the Functionality.
- Independent Module functionality, Replaceable modules irrespective of Functionality.

- Manage all development artifacts and processes in a single data model, from security requirements to test results, security risks and mitigations
- Manage end-to-end traceability of these assets and can show that every security requirement has been validated and every risk has been mitigated
- Ensure strict change management procedures are followed across all lifecycle artifacts
- Automated framework defines the process along with different activities that need to be carried out during the entire product development cycle.

- Secure message communication
- Secure bootloader
- Secure Flashing methodology
- Provision of security disability
- Safety on Over the Air programming.
- Safety for connected vehicles through In-vehicle communication.



**Fig: "I.V.S.C,S.," Process flow diagram**

#### IV. "I.V.S.C,S.," SECURE DESIGN

"I.V.S.C,S.," has many unique features that enable the faster and easier compliance of achieving Security Safety Cryptographic Methods as compared to other Secure methodologies.

**A. Eminence of the "I.V.S.C,S.," Design:** The Layered Security Architecture is captured in a single data model, from requirements to test results, models, and risks and mitigations. This Overcomes the Traditional methods.

**B. Independent Interference:** The architectural framework defined in "I.V.S.C,S.," allows configuration Authenticated communication of separate External Communication, In-vehicle communication mechanisms for different components. Therefore, the incorrect execution of the non-safety relevant software components cannot interfere with functioning of the safety software components. This is difficult to achieve without layered concept.

**C. Rights and Secure management:** Functionalities provided will help to create trusted framework, signing the software digitally with the authorized certificate.

- Hardware/Software based security peripheral

#### **Advantages of secure design:**

Model designed and developed to condense the data access or manipulation of data from external entity to avoid Financial loss and malfunction of safety critical functionality. "I.V.S.C,S.," components can be replaced with the different kind of security component with which it can support on different framework and its functionality.

#### V. "I.V.S.C,S.," MODEL INTEGRATION FOR OCCUPANT CLASSIFICATION

##### A. Possible effects without "I.V.S.C,S.," model integrate

- Sensitive car data (vehicle speed, motor characteristic data) is exploitable.
- Passengers personal data along with GPS data are exposed to outer world.

##### B. Applied methodology through "I.V.S.C,S.,"

Integrating hardware based security mechanism, OEM can choose the hardware based secure mechanism as per the need, L&T technology services "I.V.S.C,S.," model team has the capability to develop multiplatform security cryptographic library based on customer need.

##### C. Outcome of the methodology

Achieving Security services through confidentiality, Integrity, non-repudiation and authentication. Concept of secure flashing without any data backup only with digital signature capability. Component wise unlock functionality are provided for individual competencies degradation which helps to achieve more stringent security layer.

To support hardware based security mechanism the necessary supported algorithms and hardware will be taken by supported vendors as the secure algorithms should have been approved by their geographical cryptographic standard society.

**VI. “I.V.S.C,S,,” MODEL INTEGRATION FOR CRASH SENSING**

- A. Possible effects without “I.V.S.C,S,,” model integrate
- Internal basic logic for security reprogramming, for performing SW updates vehicles should be recalled.
  - Sensitive car data with respect to air bag deployment event data, power train signal data is exploitable.

B. Applied methodology through “I.V.S.C,S,,” Integrating software based security mechanism, L&T technology services “I.V.S.C,S,,” model team has developed the software based secure bootloader cryptographic algorithm with the help of third party for secure algorithm based on customer need. Over the Air programming capabilities with complicated secure design over security later.

C. Outcome of the methodology  
No need of vehicle recall, 100% operational reprogramming concept from anywhere to the vehicle. concept of secure flashing along with data backup, signature verification capability, so that unauthenticated data will not be flashed or data will not be provided to unauthenticated or received.

To support software based security mechanism the necessary supported algorithms is developed by L&T technology services and integrated to achieve secure bootloader and over the air programming proficiency.

**VII. BENEFITS TO TIER-1 & OEM (ORIGINAL EQUIPMENT MANUFACTURER)**

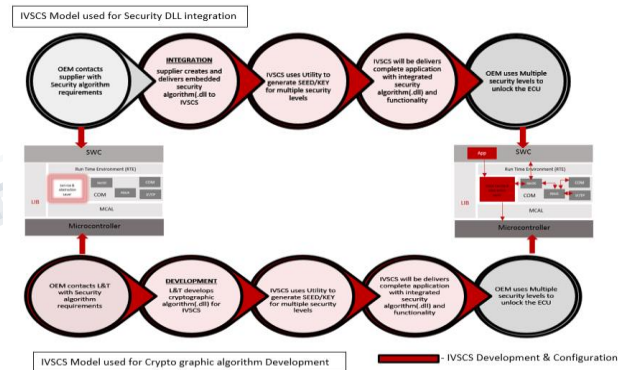
- ❑ Reduces the Vehicle recalls avoiding failures which gives huge benefit in terms of cost.
- ❑ Module specific Secure External communication protocols.
- ❑ Reduces Time and Cost performing Penetration Tests on Intrusion detection mechanism and Firewalls.
- ❑ Achieves In-Vehicle Communication with Encryption and Message Authentication.
- ❑ Develops Secure Platforms for Flashing, maintaining IVSCS Crypto Library

**VIII. APPLICATION OF “I.V.S.C, S,,” ON MULTIPLE PLATFORMS**

Certain OEMs wants to integrate the cryptographic Algorithm/DLLs from third parties and few OEMs wants L&T technology services to develop cryptographic algorithms based on cryptographic standard.

“I.V.S.C,S,,” can be used for any kind of environment like AUTOSAR or non Autosar

- ❑ Standardized interfaces with reusable Independent modules.
- ❑ Development of Safety Critical Vehicle Modules such as Safety Systems, Steering Systems, Advanced Brake Systems, Battery Management Systems, Body Control Modules etc.
- ❑ Developing Secure Message Authentication for Each module along with In-Vehicle and External Communication independent of platform related Software.



*Fig: “I.V.S.C,S,,” use case*

**IX. BENEFITS OF THE L&T TECHNOLOGY SERVICES THROUGH “I.V.S.C, S,,” METHODOLOGY**

By incorporating the Security standards in the existing system and software development life cycle process; we can achieve the following key benefits:

- Released the product faster in time to market to compete with emerging market.

- Reduced Safety Product Development Cycle Time by a quarter.
- Reduced Time is because of existing Design and configuration
- Provides 99.999% Reliable product with SAE J3061, ISO26262 Compliance.

### **CONCLUSION**

Cyber security is an efficient feature that is going to be an integral part of upcoming electronic control units in future. Would like to thank management of automotive L&T technology services.

### **REFERENCES**

[1] Ram Chillarege, Jeffrey M. VoasY Reliability of Embedded and Cyber-Physical Systems. [https:// www. nist. gov /publications/reliability-embedded-and-cyber-physical-systems](https://www.nist.gov/publications/reliability-embedded-and-cyber-physical-systems)

[2] Wolf SSL [https:// www. wolfssl .com /license /fips/?gclid=EAIaIQobChMI85fT7JHI2gIVxA0rCh0EqAHCEAAYASAAEgLzOvD\\_BwE](https://www.wolfssl.com/license/fips/?gclid=EAIaIQobChMI85fT7JHI2gIVxA0rCh0EqAHCEAAYASAAEgLzOvD_BwE)

