

ccc
Kontakt

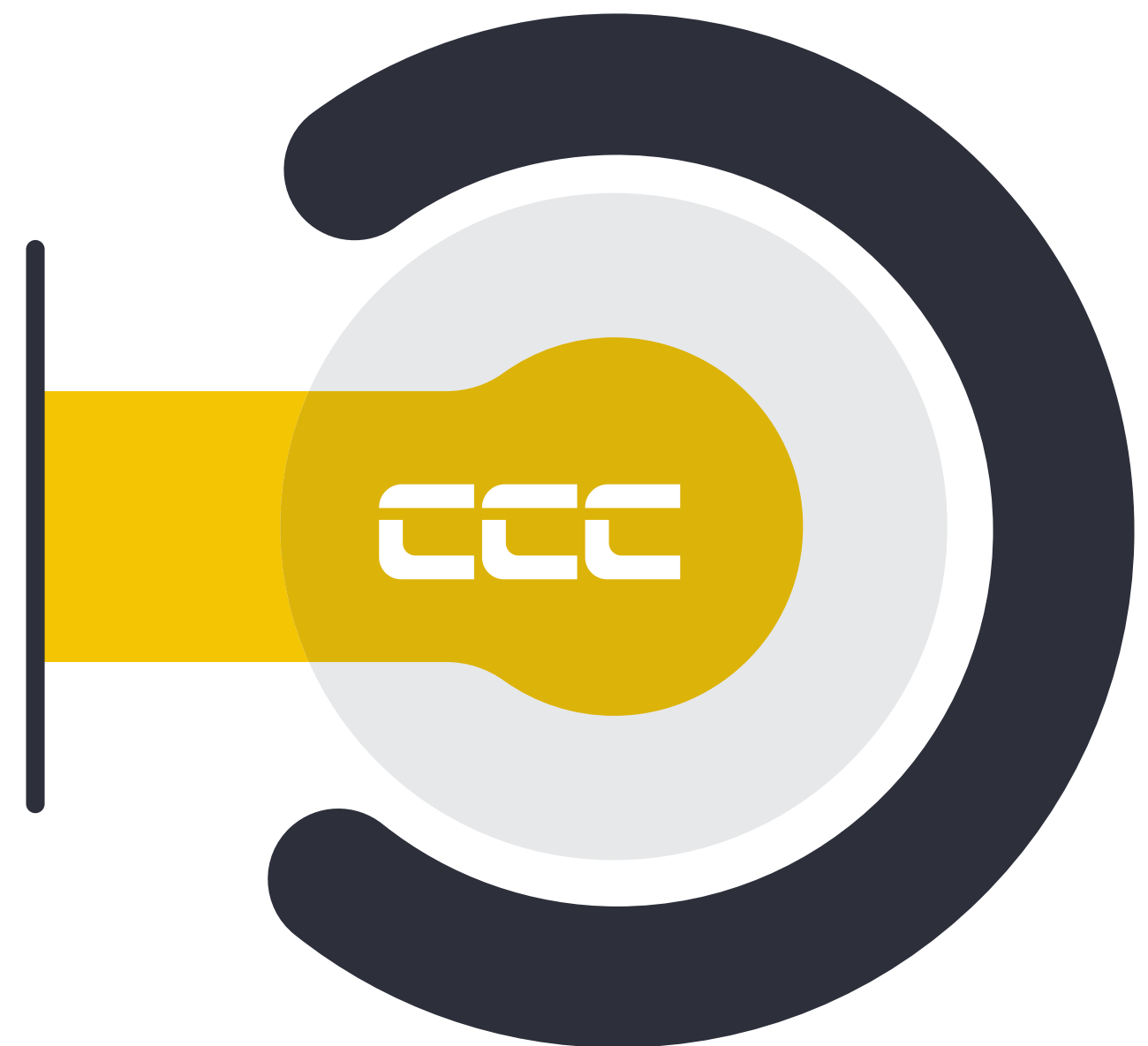
Weststraße 4
57392 Schmallenberg

P : 02972 96396-01

M : 0173 8253824

E : b.richter@cybercomplete.de

w : www.cybercomplete.de



CYBERSICHERHEIT
Automotive CSMS/SUMS

Unser Unternehmen

Das Team der Cyber Complete GmbH versteht die Informationssicherheit als ganzheitlichen Ansatz und eine der wichtigsten Säulen in heutigen Unternehmen. In der Industrie- und Wirtschaftswelt des 21. Jahrhunderts ist inzwischen eine Vernetzung und Globalisierung gegeben, die eine Cybersicherheit für Unternehmen, Konzerne und Privatpersonen unabdingbar macht und eine Grundvoraussetzung für ein erfolgreiches Wirken ist. Täglich erfolgen aus allen Winkeln des Globus unzählige Hackerangriffe und Versuche, in die Systeme von Firmen einzudringen – die Tendenz ist weiter steigend. Auch politische Institutionen und ganze Regierungen sind von diesen Entwicklungen betroffen, besonders wenn es dabei um sensible und besonders schützenswerte Inhalte und Daten geht.



Inhaltsverzeichnis

Was sind CSMS/SUMS?	04
Ziele	05
Anforderungen CSMS	06
Anforderungen SUMS	07
Hersteller und Zulieferer	08
CSMS/SUMS Unterstützung	09
Blick in die Zukunft	10 - 11

Was sind CSMS/SUMS?

CSMS (Cybersecurity Management Systeme) und SUMS (Software-Update-Management-Systeme) sind Bezeichnungen für UN-Regelungen und enthalten Anforderungen an Hersteller und Dienste, die systemgesteuerte Fahrzeuge bzw. embedded-Systems-Komponenten für solche Fahrzeuge herstellen.

Eine angemessene Erfüllung dieser Vorschriften werden verlangt für Typgenehmigung aller Neufahrzeuge und sind seit Juli 2024 verbindlich.



Ziele

- Identifizierung möglicher Angriffsvektoren und Minimierung der Risikofaktoren im Fahrzeug
- Sicherstellung von Systemen und Steuerelementen der Fahrzeuge, damit diese zukünftig nicht von kriminellen Gruppen oder Cyberkriminellen ausgenutzt werden können
- Langfristiger Schutz und Gewährleistung von Kompatibilität durch kontinuierliche Softwarepflege und regelmäßige Risikobewertungen

Zusammengefasst:

In der Entwicklung, bei der Produktion und während des gesamten Lebenslaufs bis zur Verschrottung muss die Sicherheit der internen Systeme des Fahrzeugs gegeben sein.

Anforderungen

CSMS

Das Einrichten eines CSMS zielt darauf ab, die Cybersicherheit von Fahrzeugen und deren Systeme zu gewährleisten. Die Hauptziele sind:

1. Schutz vor Cyberangriffen: Sicherung der Integrität des Fahrzeugs
2. Sichere Entwicklung von Fahrzeugsoftware: Festlegung von Anforderungen für die sichere Entwicklung und Integration von Fahrzeugsoftware und -systemen
3. Risikomanagement: Einführung eines Risikomanagements, das die potenziellen Bedrohungen für Fahrzeug-IT-Systeme identifiziert und abmildert

4. Transparenz und Nachvollziehbarkeit: Dokumentation der im Fahrzeug implementierten Cybersicherheitsmaßnahmen für Transparenz und Verantwortlichkeit gegenüber Behörden und Verbrauchern
5. Vorbereitung auf künftige Bedrohungen: Bewertung und Anpassung von Sicherheitsmaßnahmen zum Schutz von Fahrzeugen auf zukünftige Angriffe

Anforderungen

SUMS

Ein SUMS legt die Anforderungen für die Verwaltung von Software-Updates in Fahrzeugen fest. Die Hauptziele umfassen:

1. Software-Update-Management: Sichere und fehlerfreie Installation von Software-Updates sowie Schutz vor Manipulation
2. Fahrzeugsysteme Aktualität: Kontinuierliche Verbesserung von Fahrzeug und Systemen durch Sicherheitsupdates und neue Features

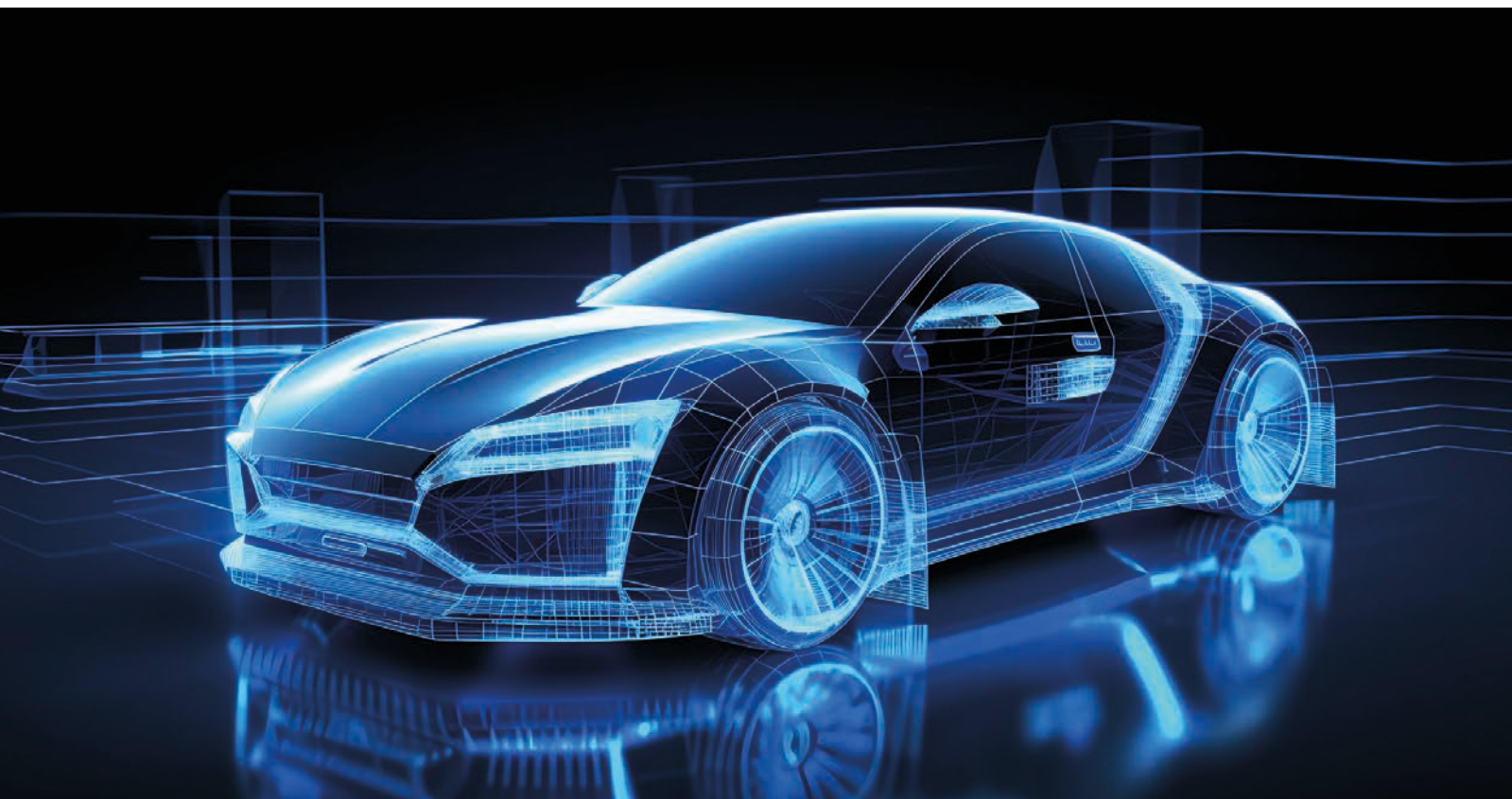
3. Transparente Update-Prozesse: Optimierte und nachvollziehbare Prozesse für Verwaltung und Durchführung von Software-Updates
4. Kompatibilität und Sicherheit: Softwareupdates beeinträchtigen nicht die Funktion und produzieren keine Sicherheitslücken
5. Langfristige Unterstützung: Regelmäßige Bereitstellung von Software zur Beseitigung von Schwachstellen sowie Verbesserung der Leistung



Zulieferer: Betroffen oder nicht?

Explizit werden nur die Fahrzeughersteller selbst verpflichtet, jedoch muss die Sicherheit der Systeme über die gesamte Lieferkette gewährleistet werden. Schlussfolgernd besteht ein Interesse, dass auch Zulieferer diese Vorgaben erfüllen. Zulieferer, die Softwaregesteuerte Steuerelemente oder

Softwaregesteuerte/bidirektional gesteuerte Sensoren herstellen/einbauen sind mit großer Wahrscheinlichkeit davon betroffen und müssen die Anforderungen erfüllen. Jedoch ist es empfohlen, das von einer sicheren Quelle prüfen zu lassen.



CSMS/SUMS Unterstützung

Der Anforderungskatalog für CSMS und SUMS ist sehr umfangreich und detailliert, um alle potenziell möglichen technischen Szenarien abzubilden. Die Implementierung von SUMS/CSMS erfordert dazu viel technisches Wissen über die eigenen Produkte und Komponenten.

Es wird von uns dringend empfohlen, sich bei diesem Projekt professionelle Unterstützung und Begleitung heranzuziehen.



Blick in die Zukunft

Die Zukunft der Automobilbranche wird von einer Reihe von Trends und Entwicklungen geprägt sein, die auf die ständig wachsenden und sich verändernden Bedrohungen von digitalisierten und vernetzten Fahrzeugen reagieren. Hier sind einige Schlüsselaspekte der zukünftigen Cybersicherheit in der Automobilbranche.

● Security by Design

Dieser Entwicklungsansatz muss in die bestehenden Prozesse implementiert und bei allen Mitarbeitern verfestigt werden. In Zukunft wird es ohne diesen Ansatz nicht gehen, da nachträgliche Änderungen sonst immense Kosten verursachen würden.

● IoT in Produktion und Verbau

Mit der zunehmenden Verbreitung von Internet of Things (IoT)-Geräten werden Sicherheitslösungen notwendig, die diese Geräte absichern und sie vor Missbrauch schützen.

● Update-Sicherheit und Over-the-Air-Updates

Die Sicherheit des Update-Prozesses muss zu jeder Zeit vorhanden sein und darf nur unter vorgegebenen, nicht umgehbaren Rahmenbedingungen durchgeführt werden. Nur dadurch kann die Verkehrssicherheit und der Schutz des Menschen sichergestellt werden.

● Künstliche Intelligenz und maschinelles Lernen

Durch die immer ausgefeilteren Angriffsmethoden ist das Implementieren von KI und maschinellem Lernen eine absolute Notwendigkeit, um Angriffsmuster frühzeitig zu erkennen und entsprechende Maßnahmen ergreifen zu können.

● Sicherheit für kritische Infrastrukturen

Die Sicherheit von kritischen Infrastrukturen wie Energieversorgung und Verkehrssystemen wird eine wachsende Priorität darstellen, da Angriffe auf diese Systeme erhebliche Auswirkungen auf die Gesellschaft haben könnten.

● Autonomes Fahren

In der Zukunft wird Autonomes Fahren eine immer größere Rolle spielen. Die Kommunikation von Sensoren in Fahrzeugen und Bauteilen gegen Angriffe zu schützen wird ein immer größerer Teil von Entwicklung und Produktion.



Die Zukunft der Automobilbranche wird von einer Reihe von Trends und Entwicklungen geprägt sein, die auf die ständig wachsenden und sich verändernden Bedrohungen von digitalisierten und vernetzten Fahrzeugen reagieren.