- CAL1 = niedrig
- CAL2 = mittel
- CAL3 = hoch
- CAL4 = sehr hoch

Der Cybersecurity Assurance Level (CAL) wird nicht pauschal für das gesamte Fahrzeug vergeben, sondern für ausgewählte Komponenten (Items). Maßgeblich für die Bestimmung des CAL ist die Risikoanalyse[315] (TARA), bei der Angriffsvektoren, Schadensauswirkungen und Eintrittswahrscheinlichkeiten berücksichtigt werden.

Ein CAL ist nur dann von praktischem Nutzen, wenn er im CSMS durch entsprechende Entwicklungs- und Testaktivitäten konkret umgesetzt wird.

Auch in der funktionalen Sicherheit nach ISO 26262 wird mit dem Automotive Safety Integrity Level (ASIL) ein gestuftes Anforderungsniveau definiert. Wie der CAL in der Cybersecurity legt der ASIL fest, mit welchem Entwicklungs- und Prüfaufwand bestimmte Risiken beherrscht werden sollen.

13.5 UNECE R156 – Softwareaktualisierung im Aftersales

Mit dem Amtsblatt L 82/60 vom 3. März 2021 informiert die EU, dass mit Inkrafttreten zum 22. Januar 2021 die Typgenehmigung um *„Einheitliche Bedingungen für die Genehmigung von Kraftfahrzeugen hinsichtlich der Softwareaktualisierung und des Softwareaktualisierungsmanagementsystems“* (SUMS) ergänzt wird. Für die dazu gültigen Details wird auf die neueste Fassung des UNECE-Statusdokuments ECE/TRANS/WP.29/2020/80 verwiesen, und zwar auf die UNECE R156 mit dem Titel: „Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to software update and software updates management system.“[316]

Die UNECE R156 beschreibt Anforderungen an Fahrzeughersteller hinsichtlich der Installation eines Software Update Management Systems (SUMS). Die Funktion dieses Systems und der damit einhergehenden Prozesse muss gegenüber der Typgenehmigungsbehörde oder einem von der Typgenehmigungsbehörde akkreditierten Prüfinstitut nachgewiesen werden. Es ist sicherzustellen, dass nicht nur die zum Zeitpunkt SOP typgenehmigten Software-Funktionen installiert sind, sondern auch nach Software-Updates, die Typgenehmigung weiterhin gültig ist. Bemerkenswert ist, dass Fahrzeuge mit einem zulässigen Gesamtgewicht kleiner 450 kg und Fahrzeuge der Klasse L, also zwei- und dreirädrige Kraftfahrzeuge, nicht betroffen sind.

Die ISO 24089 beschreibt *Anforderungen und Empfehlungen für das Software-Update-Engineering auf organisatorischer und Projektebene.*

[315] TARA = Threat Analysis and Risk Assessment

[316] Amtsblatt L 82/60, Veröffentlichung der UN ECE R156, https://eur-lex.europa.eu/, 22.1.2021

ISO 24089 wird in der UNECE R156 (Software Updates and Software Updates Management Systems) nicht erwähnt.

Weder die UNECE R156 noch die ISO 24089 spezifizieren, wie ein Software-Update technisch abläuft oder wie ein Software-Update-Management-System aussehen soll. Vielmehr geht es um die Einrichtung von Abläufen und Prozessen zur Entwicklung, Prüfung und Verteilung von Software.

UNECE R156 definiert die RX-Software-Identifikationsnummer. *„RX-Software-Identifikationsnummer" (RXSWIN) bezeichnet eine vom Fahrzeughersteller festgelegte spezielle Identifikationsnummer, die Informationen über die für die Typgenehmigung relevante Software des elektronischen Steuersystems enthält und zu einem für die Typgenehmigung nach Regelung Nr. X maßgeblichen Merkmal des Fahrzeugs gehört.*"

„R" bezieht sich dabei auf eine Regulierung der UNECE, „X" auf die zugehörige Nummer. R79 beispielsweise beschreibt die *„Einheitlichen Bedingungen für die Genehmigung der Fahrzeuge hinsichtlich der Lenkanlage"*. Da die gesamte Lenkanlage eines Fahrzeugs aus mehreren Komponenten besteht und auch eine oder mehrere technische Einrichtungen beinhalten kann, die durch Softwarefunktionen gesteuert werden, ist vom Hersteller ein R79SWIN zu vergeben. Diese Software-Identifikationsnummer ist nicht identisch mit einer Software-Versionsnummer eines Steuergeräts.

Der Fahrzeughersteller vergibt somit die RXSWIN zusätzlich zu seinen proprietären Software-Versionsnummern, um der UNECE R156 gerecht zu werden. Ein Softwareupdate im Aftersales, das keine sicherheitsrelevanten Änderungen und damit keine Anpassung der Typgenehmigung erforderlich macht, führt dazu, dass die RXSWIN unverändert bleibt, während sich eine oder mehrere proprietäre Software-Versionsnummern ändern. In jedem Fall ist der Fahrzeughersteller verantwortlich dafür, dass die Zuordnung von einer oder mehreren proprietären Software-Versionsnummern zu einer RXSWIN verfügbar ist. Die vom Fahrzeughersteller vergebenen RXSWIN müssen dabei nicht zwingend im Fahrzeug gespeichert und abrufbar sein. Eine Abrufbarkeit vom Herstellerportal ist ebenfalls zulässig. Demzufolge kann es erforderlich sein, dass zu installierten Softwareumfängen im Fahrzeug die zugehörigen proprietären Software-Versionsnummern aus dem Fahrzeug ausgelesen und die Zugehörigkeit zur RXSWIN durch Abruf der Zuweisung vom Herstellerportal erfolgen muss.

Zur Sicherstellung der Verkehrssicherheit und der Einhaltung von Emissionsgrenzwerten sind Fahrzeughalter verpflichtet, ihr Fahrzeug regelmäßig zur Hauptuntersuchung (HU) vorzustellen.

Dabei wird auch die Untersuchung des Motormanagement- und Abgasreinigungssystems (UMA)[317] durchgeführt. Je nach Fahrzeugtyp, Datum der Erstzulassung und geltender Abgasnorm wird dabei auch die Übereinstimmung der im Motorsteuergerät gespeicherten abgasrelevanten Softwareidentifikation mit den genehmigten Referenzwerten überprüft.[318]

[317] *Früher:* Abgasuntersuchung AU

[318] § 47a StVZO Anlage VIIIa und VIIIb und EU-Richtlinie 2014/45

Die Prüfung der Software-Integrität ist technisch möglich, aber regulatorisch noch nicht Teil der HU (Stand: 2025).

Abhängig von CSMS- und SUMS-Konformität des Fahrzeugs werden die Prüfungen in der Praxis über die Diagnoseschnittstelle durchgeführt.

Es ist zu erwarten, dass künftig im Rahmen der Hauptuntersuchung auch die Prüfung der RXSWIN, mit der genehmigungspflichtige Softwarestände identifiziert werden können, vom VOG verlangt wird, sowie die Prüfung der Integrität der installierten Softwarestände, etwa durch Abgleich mit signierten Referenzdaten oder mit kryptografischen Nachweisen.

13.6 EU-Richtlinie 2022/2555 (NIS-2)

Die EU-Richtlinie 2022/2555 (NIS-2)[319] verschärft die Cybersecurity-Anforderungen in der Union, erweitert den Anwendungsbereich auf zusätzliche Sektoren und sieht deutlich strengere Kontroll- und Sanktionsmechanismen vor. Ziel ist die EU-weite Harmonisierung und Erhöhung des Schutzniveaus kritischer Infrastrukturen und digitaler Dienste.

NIS-2 stellt selbst keinen Zertifizierungsprozess dar und vergibt selbst auch kein Zertifikat. Betroffene Organisationen müssen nachweisen, eine Sicherheitszertifizierung durchgeführt zu haben. Diese Sicherheitszertifizierung kann erfüllt werden, indem die branchenüblichen Standards, wie die ISO 27001, TISAX® (Abschnitt 13.7) oder der BSI Grundschutz erfüllt sind.

Die Umsetzung der NIS-2-Richtlinien in nationales Recht der EU-Mitgliedsstaaten war auf den 17. Oktober 2024 terminiert. In Deutschland soll deshalb noch im Jahr 2025 das „NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz“ (NIS2UmsuCG) in Kraft treten. Es überführt die EU-Mindeststandards für Cybersecurity der NIS-2-Richtlinie in deutsche Gesetzgebung. NIS-2 und damit auch das NIS2UmsuCG gelten für Unternehmen ab 50 Mitarbeitern oder 10 Millionen Euro Jahresumsatz.

13.7 TISAX

Um den Anforderungen der NIS-2-Richtlinie bzw. des deutschen Umsetzungsgesetzes (NIS2UmsuCG)[320] gerecht zu werden, müssen betroffene Unternehmen geeignete organisatorische und technische Maßnahmen zur Cybersicherheit nachweisen. In der Automobilindustrie hat sich hierfür insbesondere das Prüf- und Austauschverfahren TISAX (Trusted Information Security Assessment Exchange) etabliert. TISAX ist ein unternehmensübergreifendes Verfahren zur Bewertung von Informationssicherheit, das branchenweit anerkannt ist und als Nachweis für ein systematisches Sicherheitsmanagement herangezogen werden kann.

[319] NIS = Netz- und Informationssicherheit, siehe auch https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

[320] Gesetz zur Umsetzung von EU NIS2 und Stärkung der Cybersicherheit

In Deutschland hat sich der VDA mit der Entwicklung eines herstellerübergreifenden Katalogs zur Durchführung von *Assessments zur Informationssicherheit* befasst und das Ergebnis als VDA Information Security Assessment (VDA-ISA)-Katalog[321] als „Branchenstandard" veröffentlicht und empfiehlt „den Unternehmen, die an der Wertschöpfungskette der Automobilindustrie beteiligt sind, Informationssicherheit auf Basis des aktuellen VDA-ISA Katalogs aufzubauen" und entsprechende Assessments durchzuführen, um das TISAX-Zertifikat zu erhalten.[322]

Dieses Zertifikat wird in den Lieferantenbedingungen von verschiedenen Fahrzeugherstellern ab einer bestimmten Unternehmensgröße verlangt.

Anmerkung des Autors: Dies gilt auch für Hochschulen, weshalb aufgrund der Kooperation mit einem großen Fahrzeughersteller für ein Gebäude unseres Instituts eine TISAX-Zertifizierung durchlaufen wurde.

TISAX basiert auf dem VDA-ISA-Katalog, der sich an ISO/IEC 27001 anlehnt.

Ob TISAX allein ausreichend für die NIS-2-Konformität ist, hängt vom Einzelfall und dem Risikoprofil des Unternehmens ab. Das BSI oder zuständige Behörden definieren, was als geeigneter Nachweis gilt (§ 30 NIS2UmsuCG).

13.8 Prozesse in der Werkstatt

13.8.1 Einführende Informationen

Sowohl markengebundene als auch freie Werkstätten sind Unternehmen, in denen prozessgesteuert gearbeitet wird. Die Prozesse bestimmen die Organisationsstruktur. Ein zentraler Funktionsbereich jeder Werkstatt ist die Serviceberatung. Die dort eingesetzten Mitarbeitenden übernehmen die Kommunikation mit dem Kunden und fungieren als Schnittstelle zwischen den Funktionsbereichen. Beispiele für Aufgaben in der Serviceberatung sind:

- Terminvereinbarung
- Beratung
- Fahrzeugannahme mit Symptomerfassung
- Fahrzeugrückgabe
- Rechnungsstellung
- Bearbeitung von Gewährleistungsansprüchen und Garantien

Neben dem Ersatzteilmanagement gehört auch die Instandsetzung zur Aufbau- und Ablauforganisation einer Werkstatt. In der Instandsetzung werden alle Arbeiten am Fahrzeug

[321] VDA ISA Katalog, Version 6.0, https://www.vda.de/de/aktuelles/publikationen/publication/vda-isa-katalog--version-6

[322] VDA: Informationssicherheit in Unternehmen, https://www.vda.de/de/aktuelles/publikationen/publication/empfehlung-informationssicherheit

vom einfachen Servicevorgang (z. B. Ölwechsel, Auffüllen von Betriebsstoffen oder Wechsel der Wischerblätter) bis hin zu umfangreichen Instandsetzungsvorgängen (z. B. Unfallschadeninstandsetzung oder Motorschadenreparatur) durchgeführt. Die Mitarbeitenden in der Instandsetzung benutzen eine Vielzahl an Werkzeugen – vom einfachen Schraubendreher und Maulschlüssel bis hin zu komplexen Messgeräten und Tools für die Diagnose, die ADAS-Kalibration oder die Programmierung von Steuergeräten ist alles dabei und muss fachgerecht eingesetzt werden.

Die Vernetzung der Organisationseinheiten für eine ganzheitliche prozessgesteuerte Abwicklung erfolgt durch Dealer-Management-Systeme (DMS). Um eine möglichst lückenlose Dokumentation der Prozessschritte zu gewährleisten, werden im Instandsetzungsbereich weitere, in der Regel WLAN-basierte Netzwerke eingesetzt, die eine Schnittstelle zum DMS haben.

13.8.2 Datenmanagement in Werkstätten

Workshop-Net, das *„Netzwerk für die digitale Werkstatt ist ein internationaler Branchenstandard der aus dem vormaligen asanetwork hervorgegangen und zu diesem voll kompatibel ist“*.[323]

Das Netzwerk ermöglicht die Datenkommunikation zwischen verschiedenen Werkstattkomponenten, beispielsweise:

- Mess- und Prüfgeräte, wie z. B. ein Partikelzählergerät, Kalibrier- und Justiereinrichtungen zur Fahrwerkeinstelleinrichtung,
- Datenspeicherungssysteme und
- Servicetester und Software-Programmierstationen.

Die European Garage Equipment Association (EGEA) hat sich zum Ziel gesetzt, die Entwicklung des Workshop-Net auf europäische Ebene auszuweiten, um die Interoperabilität von Werkstattkomponenten verschiedener Hersteller zu ermöglichen. Heute hat das Workshop-Net den Status eines Branchenstandards erreicht.

Die gesamte Kommunikation erfolgt im WLAN der Werkstatt. Dazu wird in einer Sterntopologie (Bild 13.3) ein Netzwerkmanager namens „NETMAN“ eingesetzt, der als Kommunikationsserver agiert und jeglichen Datenverkehr über das Netzwerk steuert.

Die Systemstruktur des Netzwerks ist *dienstzentriert*. Das bedeutet, dass alle Teilnehmer sogenannte „Dienste“ anbieten oder nachfragen können. Jeder Teilnehmer ist dabei gleichberechtigt. Im Gegensatz dazu verfügt eine *datenzentrierte* Struktur über eine zentrale Datenbank, auf die die Teilnehmer zugreifen und Daten hinzufügen oder abfragen können. Es ergeben sich diverse Vorteile aus der dienstzentrierten Struktur im Gegensatz zu einer datenzentrierten Struktur. Einfache Systeme können mit weniger Softwareaufwand eingebunden werden, weil kein normierter Datenbankzugriff beachtet werden muss. Gleichzeitig kann das Datenmanagement einzelner Arbeitsplatzrechner bei Anbindung an das System für redundante Datenablage genutzt werden, was in einem datenzentrierten System nicht möglich wäre.

[323] https://workshop-net.net/

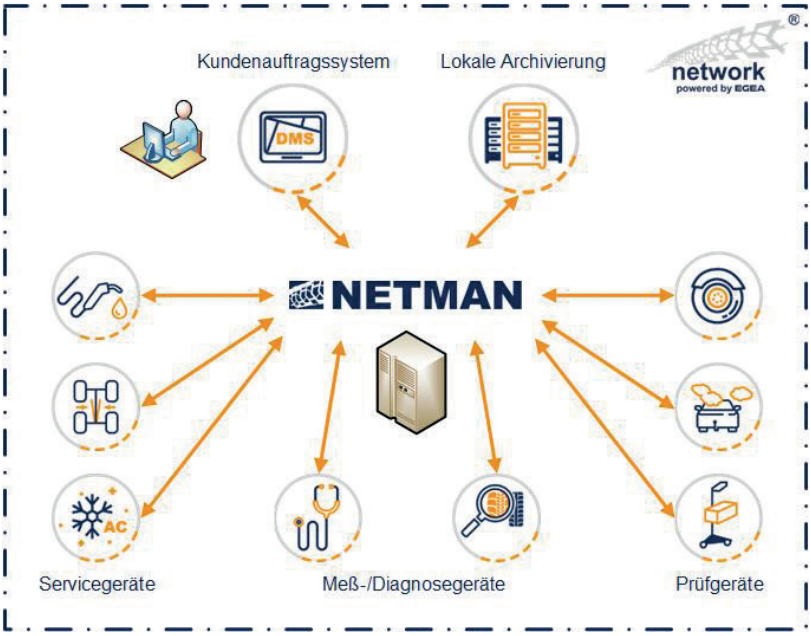

Bild 13.3 Logische Struktur des Workshop-Net (© asanetwork GmbH)

Der modulare Aufbau eines dienstzentrierten Systems ermöglicht die Begrenzung auf die wichtigsten Komponenten und es wird kein zentrales Datenbanksystem benötigt. Darüber hinaus wird eine weitaus bessere Skalierbarkeit erreicht, da eine Erweiterung um zusätzliche Teilnehmer eine direkte Verbesserung der Leistung nach sich zieht. Das Datenbanksystem eines datenzentrierten Systems hingegen muss ggf. erneuert werden, um die gewünschte Leistungsfähigkeit aufrecht zu erhalten. Ein weiterer Vorteil ist die potenzielle Ausfallsicherheit. Während eine datenzentrierte Systemstruktur vollständig auf die Verfügbarkeit der zentralen Datenbank angewiesen ist, können Daten bei einer dienstzentrierten Systemstruktur redundant im Netz verfügbar und dadurch selbst bei Ausfall eines Dienstes immer noch bei einem anderen Dienst abrufbar sein. Zusätzlich können zeitkritische Messungen besser durchgeführt werden, da sich Dienste jederzeit einfach am Netz ab- und wieder anmelden können, wodurch in diesem Fall besonders störende Belastungsspitzen vermieden werden können. Aufgrund der genannten Vorteile hat man sich dazu entschieden, das Workshop-Net dienstzentriert zu gestalten.[324]

13.8.2.1 Dienste im Workshop-Net

Es ist wichtig, die genaue Definition von Diensten im Kontext des Workshop-Net zu erfassen, da diese die Grundlage für die Kommunikation im Netzwerk darstellen. Zusätzlich werden einige wichtige Begriffe und deren Abkürzungen definiert, die bei der Arbeit mit dem Workshop-Net unerlässlich sind. Dabei wird direkter Bezug auf die Dienstdefinition in

[324] *Quelle:* Tech. Dokumentation Workshop-NET, Martin Rothschink, https://workshop-net.net/, S. 7