Nicht verpassen: Neue Regelungen des Kraftfahrtbundesamtes (KBA) zur Cyber-Security im Zuge der Typgenehmigung von Anhängern, Aufbau- und Nutzfahrzeugen

Bekommen Sie Klarheit mit der Cyber-Security-Relevanz-Bewertung nach ISO 21434 der clockworkX GmbH.
Achtung: befristetes Angebot!

Im **Juli 2024**, sowie im **Dezember 2024** treten die UNECE R-155 und UNECE R-156 für alle Fahrzeugtypen in Kraft!
UN Regulation No. 155 - Cyber security and cyber security management system | UNECE
Die UN-Regularien regeln die Cyber-Security- und Software-Update Regularien für Fahrzeugtypen, die ab 2024 mit einem Typzertifikat in den Markt gebracht werden.

Alle Hersteller cyber-security relevanter Fahrzeuge werden dazu verpflichtet ihre technischen Risiken auf Fahrzeugebene zu analysieren und zu bewerten und ein Cyber-Security Management-System (CSMS) aufzubauen.

Eine Nichterfüllung beider Regularien führt zwangsläufig dazu, keine neuen Typzulassungen beim Kraftfahrtbundesamt und anderen Zulassungsbehörden

innerhalb der EU, Asien und Nordamerika mehr erwirken zu können. Dies gilt für Neuentwicklungen, sowie existierende Fahrzeugarchitekturen gleichermaßen.

Wir, helfen Ihnen, diese Regelwerke zu erfüllen, um weiterhin Typzulassungen für Ihre Produkte zu erhalten, sollten Sie elektronische Komponenten in Ihren Anhängern und Fahrzeugen verbaut haben.
Mit unserem Cyber Security Relevanz Check, bekommen Sie innerhalb von zwei Tagen von uns eine klare Aussage in Form eines schriftlichen Berichtes, zu folgenden Punkten:

- Welche Teile Ihrer Fahrzeug– und Integrationsarchitektur cyber-security relevant sind
- Wie ein Umsetzungskonzept inkl. Auditplanung mit unseren Partnern (SGS TÜV Saar, TÜV Süd, TÜV Rheinland, TÜV Austria) aussehen kann
- Welche übergeordneten Strategien Sie einschlagen können, um weiter konform und handlungsfähig im neuen Jahr sein zu können
- Wie Sie Ihre interne Organisation weiterentwickeln müssen (insbesondere Homologation, Entwicklung, After-Sales, Einkauf, Produktion und Management)
- Wie Sie Ihre Lieferanten ansteuern müssen, welche Pflichten Sie als OEM haben und inwiefern eine diesbezügliche organisatorische und technische Lieferantenbewertung Ihrerseits wichtig ist, um konform zu bleiben

Angesichts der zunehmenden Bedrohungen im digitalen Raum, ist es von höchster Dringlichkeit, sich auf die anstehenden Änderungen vorzubereiten.

Um sicherzustellen, dass Ihr Unternehmen den neuen Vorschriften entspricht und Ihre Produkte optimal geschützt sind, bieten wir darüber hinaus **Schulungen und Beratung** an, die wir maßgeschneidert auf Ihre Organisation anpassen werden.

Unsere Experten stehen Ihnen zur Verfügung, um Sie bei der Erstellung und Implementierung des geforderten Cyber-Security-Management-Systems zu unterstützen.

Zögern Sie bitte nicht, uns zu kontaktieren, um mehr über unsere Cyber-Security-Lösungen zu erfahren und sich auf die bevorstehenden Änderungen vorzubereiten.