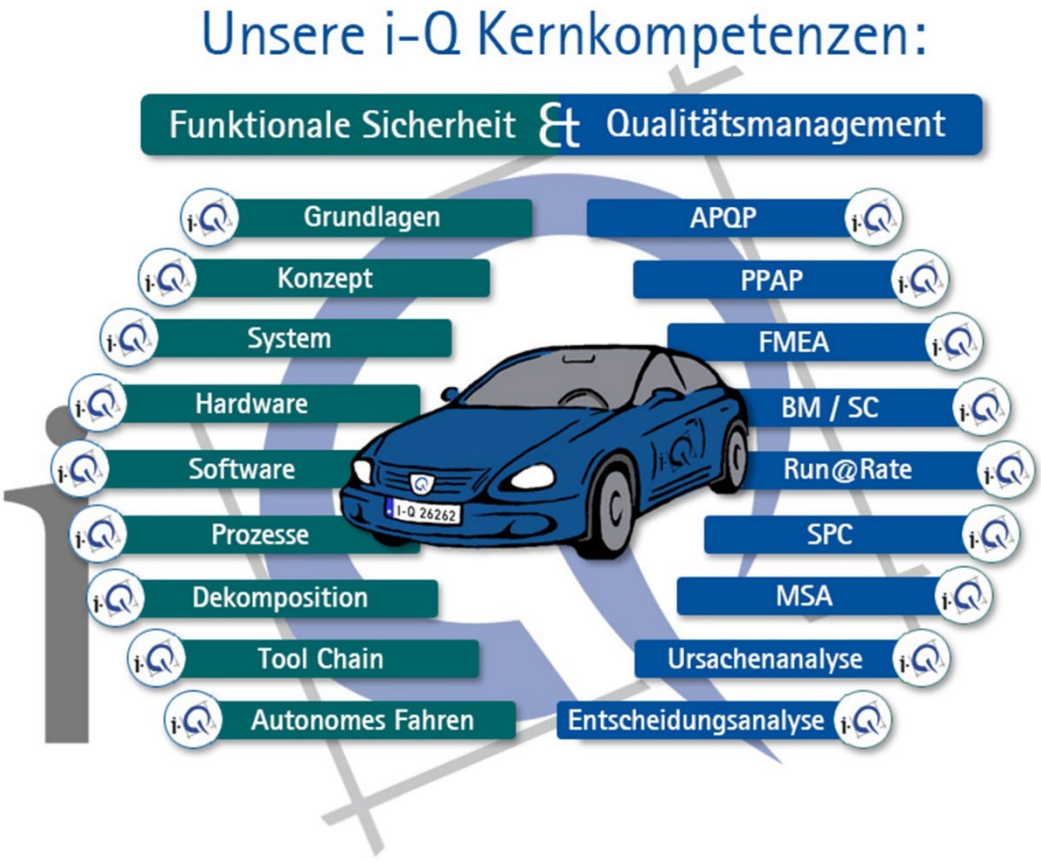
Schacht & Kollegen
Qualitätskonstruktion GmbH

i-Q Schacht & Kollegen Qualitätskonstruktion GmbH

C bei autonomen Fahrzeugen

Was müsste sich bei ISO 26262 ändern?



www.i-Q.de

Qualitätskonstruktion – FuSi – QM – Beratung – Umsetzung

1. Die Controllability bei autonom fahrenden Fahrzeugen

Bei der Erstellung der HARA innerhalb der ISO 26262 werden drei Summanden bestimmt. Die Severity (S0 bis S3), die Exposure (E0 bis E4) und die Controllability (C0 bis C3). Daraus ergibt sich dann durch aufsummieren der Summanden die ASIL-Klassifizierung. Wenn die Zahlen zusammen 10 ergeben, dann haben wir einen ASIL D.

Bei der Controllability gehen zurzeit die Beschreibungen davon aus, dass hauptsächlich der Fahrer des Fahrzeugs die Beherrschbarkeit der Situation besonders stark beeinflussen kann. Aber im Falle, dass das Fahrzeug automatisiert (SAE Level 1 bis 3) oder sogar autonom (SAE Level 4 und 5) unterwegs ist, entfallen immer mehr die Einflussmöglichkeiten des Fahrers, so dass es nach dieser Bewertung ein autonomes Fahrzeug (in den allermeisten Fällen) grundsätzlich mit einer C3 gewertet werden müsste.

Aber das kann ja so nicht ganz stimmen, denn autonom fahrende Fahrzeuge sollten ja grundsätzlich sicherer sein als von Menschen gesteuerte Fahrzeuge.

Jetzt steht allerdings auch ein ganz wichtiger Hinweis in der aktuellen Norm. Die Bewertung innerhalb der HARA hat ohne die zu Hilfenahme von schon geplanten oder sogar installierten Sicherheitsmaßnahmen zu erfolgen. Das gilt allerdings immer nur für das aktuell betrachtete System. Andere, unabhängige Systeme dürfen allerdings durchaus zur Risikominimierung herangezogen werden. Siehe dazu ISO 26262-3:2018, 6.4.1 Einleitung der Gefahrenanalyse und Risikobewertung (Text der Norm, siehe Anhang).

Das würde also für ein autonom fahrendes Fahrzeug bedeuten, dass zum Beispiel bei der Bewertung eines Kamerasystems zwar keine Maßnahmen innerhalb des Kamerasystem berücksichtig werden dürfen, aber durchaus Systeme wie LIDAR, RADAR, Ultraschall oder auch Infrarot zur Minimierung der Gefahrenbeurteilung herangezogen werden können. Dabei muss natürlich sehr genau betrachtet werden, welche Aufgaben des Kamerasystems tatsächlich von anderen Sensoren adäquat übernommen werden können.

Aber die redundanten Systeme könnten sich ja dann zum Beispiel bei der Beherrschbarkeit der Situation bemerkbar machen.

Daher müssen wir uns meiner Meinung nach ersthafte Gedanken machen, wie wir solche Szenarien in die Bewertung von HARAs für autonom fahrende Fahrzeuge aufnehmen können. Denn zurzeit sehe ich einfach viele verschieden Versuche auf die Situation zu reagieren. Und die wenigsten davon halte ich für wirklich zielführend.

Ich versuche es mal mit einem Beispiel: Ich möchte gerne mein Auto autonom in meine Garage einparken. Dazu muss ich jetzt mein Kamerasystem betrachten, das mir Informationen gibt, so dass ich auch tatsächlich zwischen den seitlichen (baulichen) Begrenzungen in die Garage reinpasse und mir nicht die Spiegel abfahre und / oder den Lack zerkratze.

Jetzt habe ich vielleicht noch weitere Sensoren an Bord. Gehen wir mal von Ultraschall und LIDAR aus.

Der Ultraschallsensor ist dabei sicherlich mit Vorsicht zu genießen, denn er wird (ähnlich wie heute bei der Einparkhilfe) zwar sagen, dass da etwas ist, aber ob er so genau ist, dass er zwischen dem Fahrweg und der restlichen Umgebung unterscheiden kann, wage ich ernsthaft zu bezweifeln. Sehr wahrscheinlich wäre dann spätestens 10cm vor der seitlichen Garagenwand Schluss, weil der Ultraschallsensor sein Veto einlegt.

Bei unserem LIDAR-System könnte das schon anders aussehen. Das System sollte eigentlich den freien Ausschnitt der Garagen-Silhouette erkennen und bei groben Fehlern des Kamerasystems unterstützend eingreifen können. Und genau DAS sollte sich dann in der Bewertung der Controllability niederschlagen und zu einer besseren Gesamteinstufung bei der ASIL-Klassifizierung führen.

Natürlich bin ich jetzt kein absoluter Spezialist für diese ganzen angesprochenen Systeme. Es soll ja auch nur ein Beispiel sein. Aber ich würde mich natürlich sehr über hilfreiche, fachliche Kommentare sowohl zum Thema ISO 26262 als auch zu den von mir erwähnten Systemen freuen.

Jörg Schacht (geschäftsführender Gesellschafter, i-Q Schacht & Kollegen Qualitätskonstruktion GmbH)

2. Anhang mit Normenverweisen

2.1 Englisch

6.4.1 Initiation of the hazard analysis and risk assessment

6.4.1.1 The hazard analysis and risk assessment shall be based on the item definition.

6.4.1.2 The item without internal safety mechanisms shall be evaluated during the hazard analysis and risk assessment, i.e. safety mechanisms intended to be implemented or that have already been implemented in predecessor items shall not be considered in the hazard analysis and risk assessment.

NOTE 1 In the evaluation of an item, available and sufficiently independent external measures can be beneficial.

EXAMPLE Electronic stability control can mitigate the effect of failures in chassis systems by increasing the controllability for the driver if it is shown to be available and independent from the item under evaluation.

NOTE 2 Safety mechanisms of the item that are intended to be implemented or that have already been implemented are incorporated as part of the functional safety concept.

2.2 Deutsch

6.4.1 Einleitung der Gefahrenanalyse und Risikobewertung

6.4.1.1 Die Gefährdungsanalyse und Risikobeurteilung basiert auf der Definition des Systems.

6.4.1.2 Das System ohne interne Sicherheitsmechanismen ist bei der Gefahrenanalyse und Risikobeurteilung zu bewerten, d.h. Sicherheitsmechanismen, die implementiert werden sollen oder bereits in Vorgänger-Systemen implementiert wurden, werden bei der Gefahrenanalyse und Risikobeurteilung nicht berücksichtigt.

ANMERKUNG 1 Bei der Bewertung eines Systems können verfügbare und ausreichend unabhängige externe Maßnahmen von Vorteil sein.

BEISPIEL Die elektronische Stabilitätskontrolle kann die Auswirkungen von Fehlern in Fahrgestellsystemen mildern, indem sie die Beherrschbarkeit für den Fahrer erhöht, wenn sie nachweislich verfügbar und unabhängig von dem zu bewertenden System ist.

ANMERKUNG 2 Sicherheitsmechanismen des Systems, die implementiert werden sollen oder bereits implementiert wurden, sind als Teil des Konzepts der funktionalen Sicherheit integriert.