Redundant und sicher – Anforderungen an ein modernes DMI im ETCS

Die Mensch-Maschine-Schnittstelle in einem ETCS-Umfeld besteht heute im Wesentlichen aus Displays. Es gibt zwei Grundformen der Driver Machine Interfaces (DMI): Die Ausführung als Touchscreen und als Tastaturgerät.

Dana Schiffer
Marketing DEUTA-WERKE
Dana.schiffer@deuta.de

▶ Die UIC-Norm 612-0x bestimmt die Oberfläche des DMIs. Sie beschreibt, wo und wie die Tasten beschriftet sind. Es gibt ein Layout für das Touch-Gerät und ein Layout für das Tastatur-Gerät. In beiden Fällen ist ein 10,4 Zoll TFT-Display mit einer Auflösung von 640 x 480 Pixeln der definierte Standard. Die Vorgaben sind sehr detailliert und bis auf Pixelebene genau.

Auch wenn ein Display den Anforderungen der Spezifikation genügt und alle Anforderungen eingehalten werden, steht der Zug still, wenn das Display ausfällt. Um dies zu vermeiden werden Redundanzen aufgebaut. Eine einfache Lösung besteht darin, zwei Geräte in den Führertisch einzubauen, die das Gleiche tun. Fällt ein Gerät aus und das zweite Display ist aktiv, kann der Zug weiterfahren. Was diese Lösung vor allem benötigt, ist Platz. Da in den Zügen oft die nationalen Zugsicherungssysteme und ETCS verbaut sind, ist der Platz in den europäischen Führerständen meist sehr begrenzt. Eine Lösung mit zwei Displays ist daher kaum zu realisieren.

Die DEUTA-Lösung basiert auf zwei kleinen 8-Zoll-Displays, die, anders als üblich, hochkant nebeneinander angebracht sind. Die zwei Displays zeigen eine gemeinsame grafische Oberfläche – die sich an den Vorgaben der UIC-Spezifikation orientiert, so dass die Darstellungsform auf jeden Fall den Anforderungen entspricht. Die beiden Displays gemeinsam zeigen also dasselbe Bild wie ein übliches 10,4 Zoll TFT-Display. Diese Lösung bietet ein volles Redundanzprinzip, das heißt jedes Display ist eine völlig separate, eigenständige Einheit. Die beiden Displays kommunizieren miteinander und erkennen, wenn eine Einheit einen Fehler hat. Es gibt keine Zentraleinheit im Hintergrund, die die beiden TFT-Panels ansteuert.

Praktisch bedeutet dies: Beide Einheiten laufen immer und zeigen unterschiedliche Informationen. Fällt ein Display aus, erkennt das zweite Display, ob dadurch ein sicherheitsrelevanter Teil betroffen ist, z.B. der Tachometer. In diesem Fall übernimmt das zweite Display die Darstellung der sicherheitsrelevanten Anzeige, es entfallen dafür die nicht zwingend erforderlichen Anzeigen.

Zwei redundante Displays erzeugen eine Gesamtoberfläche von 10,4 Zoll

SICHERHEIT FÜR BASELINE 3

Im Rahmen von ETCS-Baseline 3 und ihren Sicherheitsanforderungen für die technische Interoperabilität, steht zusätzlich die verbindliche Spezifikation des Driver Machine Interfaces als SIL-Komponente im Fokus.

Wie man in dem nachstehenden Auszug aus Subset 091 Vers. 3.3.0 sehen kann, liegt der Schwerpunkt besonders auf manuellen Fehlbedienungen, bei denen menschliches Versagen eine Fehlerursache haben könnte. Dabei kann die Fehlerursache auch in der unbemerkten Anzeige und Eingabe falscher Daten liegen, die der Fahrzeugführer im Regelbetrieb nicht in Echtzeit überprüfen kann.

Anzeige- und Eingabeverhalten des DMI sind im Subset-091 streng normiert. Die Responsezeit nach der Eingabe und die Darstellung der grafischen Objekte sind auf 20 ms limitiert. Die Wahrscheinlichkeit eines Eingabefehlers von Fahrzeugdaten und Parametern muss für den Fahrer minimiert werden. Und auch hier gibt es wieder einen zeitlichen Richtwert: Innerhalb von 60 Sekunden muss das DMI für die Dateneingabe aus dem Standby-Modus bereit stehen. Dabei muss jederzeit sichergestellt werden, dass der Triebfahrzeugführer seine Arbeit zügig und fehlerfrei ausüben kann, ohne die Komplexi-

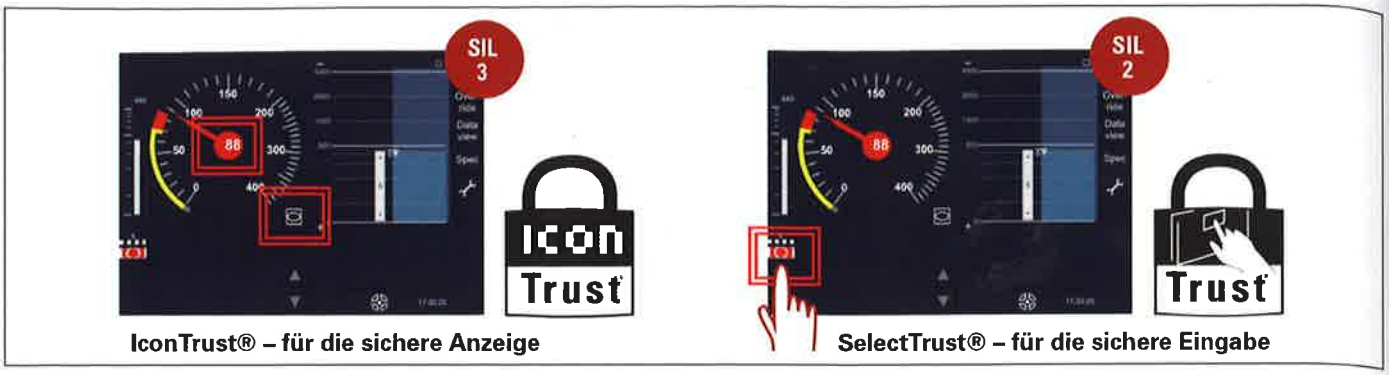
	Gefahrensituation	Zulässige Gefährdungsrate (Fehler pro Stunde)	SIL gemäß EN 50129:2003
MMI-1a	Fehlerhafte Bestätigung eines ETCS-Mode-Wechsels zu einem weniger sicheren ETCS-Mode	4.0*10-6	1
MMI-1d	Fehlerhafte Bestätigung einer ETCS-Level-Transition	2.0*10-6	1
MMI-1g	Fehlerhafte Anforderung des ETCS- Modes SH	8.0*10-7	2
MMI-2a.1	Fehlerhafte Darstellung der Fahrzeuggeschwindigkeit	7.4*10-7	2
MMI-2b	Fehlerhafte Darstellung des ETCS-Modes	1.0*10-6	1
MMI-6	Fehlerhafte Bestätigung der Funktion „Virtual Balise Cover"	4.0*10-7	2
MMI-6	Fehlerhafte Darstellung der Funktion „Virtual Balise Cover"	3.0*10-6	1
DMI-03e	Fehlerhafte Darstellung einer Fixed-Text-Message	2.0*10-6	1
DMI-04h	Fehlerhafte Quittierung einer Zwangsbremsung	2.0*10-7	2
DMI-04j	Fehlerhafte Anforderung einer ETCS-Isolation	2.0*10-7	2

Safety Requirements – Auszug aus Subset-091 – Ausgabe 3.3.0

tät des Gesamtsystems unnötig zu erhöhen. Jede Meldung auf dem DMI muss in kürzester Zeit gelesen und verstanden werden.

Was muss für eine sichere Anzeige und Toucheingabe beachtet werden?

- → Fehler und Obsoleszenzen in modernen komplexen Rechnerkernen, Caches, Grafikeinheiten etc. müssen beherrscht werden.
- → Fehler in Betriebssystemen und komplexer Software sollen bewertet und mit großem Aufwand geprüft und dokumentiert werden. Bei Änderungen sind aufwendige Nachprüfungen und Auswirkungsanalysen notwendig.
- → Die Position der Touch-Eingabe muss sicher erfasst werden: Die Eingabeeinheit muss diagnostiziert werden. Wenn nicht alle Fehlerzustände diagnostiziert werden können und eine höhere Sicherheitsstufe benötigt wird, muss die Positionserfassung redundant erfolgen.
- → Der projektspezifische Begutachtungsaufwand (Zeit und Geld) sollte so gering wie möglich sein.
- → Die sichere Darstellung an der Eingabeposition ist erforderlich. Es soll sichergestellt sein, dass die Darstellung zu der ausgelösten Eingabefunktion passt. »



IconTrust® – für die sichere Anzeige

SelectTrust® – für die sichere Eingabe

Daher ist für eine sichere Eingabe auch immer eine sichere Anzeige notwendig.

→ Bei Bediensystemen ist die Eingabesicherheit abhängig von der Sicherheitsfunktion:
- Sicheres Starten eines Aktors, der eine Gefährdung erzeugen kann
- Sicheres Stoppen / sicheres Loslassen

Die in dem Subset-091 geforderte Überwachung der sicheren Anzeige- und Eingabebereiche werden in DEUTA-DMIS mit den patentierten Sicherheitstechnologien IconTrust® und SelectTrust® überwacht. DEUTA hat sich mit diesen patentierten Sicherheitseinrichtungen bewusst für eine flexible Lösung entschieden, die auf Applikationsänderungen schnell angepasst werden kann. Denn sicherheitsrelevante Änderungen und Neukonfigurationen der Überwachungsbereiche können projektspezifisch konfiguriert und für die Begutachtung vorbereitet werden.

IconTrust® überwacht dedizierte Bereiche auf dem TFT-Panel und unterscheidet dabei zwischen gültigen und ungültigen Informationen. IconTrust® verwendet einen sicheren Rechner, wie den EVC (European Vital Computer), um die sicheren Daten an den Panel-PC zu vermitteln. Dort werden die Daten verarbeitet und angezeigt. IconTrust® überwacht die dargestellten Bildbereiche auf dem TFT-Display und sendet die Bestätigungen zurück an den sicheren Rechner. Der Vergleich erfolgt in dem sicheren Rechner z. B. im EVC.

SelectTrust® ist eine Technologie, die eine nachweislich sichere manuelle Eingabe von Informationen über einen Touchscreen oder Softkey ermöglicht. Die Eingabeposition und die Darstellung an dieser Position werden mit SelectTrust® überprüft. Nur bei Korrektheit wird eine funktional sichere Eingabeaktion an einen sicheren Rechner weitergegeben. Für den Bediener ist SelectTrust® unsichtbar: Er wählt auf dem TFT-Display ein angezeigtes graphisches Bedienelement aus und berührt es. SelectTrust® selektiert mittels IconTrust® das gedrückte Bedienelement, ordnet eine Signatur zu und sendet eine funktionale sichere Eingabeaktion an einen sicheren Rechner. Die Verlässlichkeit der Eingabeaktion ist dadurch gesichert. SelectTrust® und IconTrust überwachen alle sicherheitsrelevanten Bereiche.

Beide Überwachungssysteme arbeiten vollständig entkoppelt von der Darstellungs- und Bedienfunktion.

Die Endanwender können existierende Applikationssoftware mit dem IconTrust®/SelectTrust®-Konzept weiter verwenden. Beide Technologien arbeiten unabhängig von Betriebssystemen, Programmiertools, Programmiersprache und Bibliotheken. Es gibt keine Beschränkung auf zertifizierte Softwaretools oder stark reglementierte Kodierregeln. Das Konfigurationstool IVEN bietet eine Vorschau der konfigurierten Überwachungsbereiche und prüft die Konfiguration auf Konsistenz. Dabei zeichnet IVEN alle Prozesswerte mit dem korrespondierenden Bildschirmfoto auf, überträgt die Konfiguration in das IconTrust-Modul und generiert automatisch einen PDF-Validationsbericht, der direkt für die Begutachtung verwendet werden kann.

FAZIT

Anzeige- und Bediensysteme, die für sicherheitsrelevante Informationsein- und -ausgabe genutzt werden, und auf Basis moderner Rechentechnik realisiert wurden, müssen durch geeignete Fehleroffenbarungsmechanismen ergänzt werden um den neuesten ETCS-Spezifikationen zu entsprechen. Grundlage eines Lösungsansatzes muss dabei eine sorgfältige und möglichst minimalistische, wenngleich angemessene Definition der Sicherheitsanforderungen sein. Als Lösung erweist sich eine von der Darstellungs- und Bedienfunktion vollständig entkoppelte Überwachung als besonders kosteneffektiv, insbesondere bei Betrachtung über den kompletten Lebenszyklus des DMI-Produktes.

Generell kostet ein SIL 3 DMI der neuesten Generation nicht mehr als ein SIL1-Terminal. Für die gesamtwirtschaftliche Betrachtung sind nicht nur die Anschaffungskosten des DMI, sondern die Zukunftssicherheit und die Folgekosten zu berücksichtigen. Bei einem modernen, kostenoptimierten DMI-Konzept beeinflussen sich Änderungen der Softwareapplikation und der DMI-Hardware nicht gegenseitig. Der Vorteil liegt auf der Hand: Unabhängig von den Hardware-Abkündigungen im Laufe eines DMI-Lebenszyklus, behält die Sicherheitsbegutachtung ihre Gültigkeit. ◄

▶ SUMMARY

Redundant and safe – What the ETCS requires of a modern DMI

Display and operating systems that are used for the input and output of safety-relevant information and are implemented on the basis of modern computer technology must have fault-disclosure mechanisms added to then if they are to comply with the latest ETCS specifications. Solutions must thus be based on a careful definition of the safety requirements, which at the same time ought also to be to-the-point and as minimal in scope as possible. One solution to emerge as particularly cost-effective is for monitoring to be completely decoupled from the display and operating function, especially if the entire life cycle of the DMI product is taken into consideration.