VIRTUELLE BEDIENTABLEAUS

Die Industrie wünscht sich eine sichere virtuelle Alternative zu bislang genutzten Hardware-Bedientableaus, denn diese gelten als unflexibel und statisch. Aber wie werden auf einem TFT-Bedientableau sicherheitsrelevante Anzeigen und Eingaben umgesetzt? Schließlich müssen sicherheitskritische Faktoren und Fehlfunktionen ausgeschlossen werden.

TEXT: Walter Siegert, Deuta Werke **BILD:** Deuta Werke

Grundsätzlich sind virtuelle Bedientableaus nichts Neues: Wir bedienen sie täglich, wenn wir ein Ticket für die Straßenbahn kaufen oder am Bankautomaten Geld abheben und natürlich haben sie einen festen Platz in der Industrie. In sicherheitsrelevanten Bereichen können Bedienfehler auf einem TFT-Bedientableau jedoch Menschenleben kosten. Hier ist die sichere Anzeige und Bedienung der Mensch-Maschine-Schnittstelle die Voraussetzung für den Schutz der Umwelt.

Bislang stand weltweit keine Technologie zur Verfügung, die aus einem Standard-TFT ein Bedientableau mit sicherer Eingabe- und Anzeige-Technik machte. Initiiert wurde der Bedarf nach einer sicheren Anzeige- und Eingabetechnologie von der Schienenfahrzeugindustrie. In den Führerräumen der Bahnfahrzeuge lösen elektronische Anzeige- und Steuerelemente herkömmliche mechanische Geräte und Einzelkomponenten ab. Der Führerraum von Zügen wird mit PC- oder ARM-Standardtechnik aufgebaut, da dies Kostenvorteile bietet und eine ergonomische Gestaltung erlaubt. Insbesondere die Flexibilität der Anzeigesoftware, die sich schnell für die verschiedenen spezifischen Kunden-, Länder- oder Projektanforderungen anpassen lässt, führt zu einer zunehmenden Variantenanzahl unterschiedlicher Informations- und Steuerungsdarstellungen in den Zügen, die es technisch sicher zu beherrschen gilt. Ähnliches gilt für mechanische Bedientableaus, die in Industrieanwendungen nur für jeweils eine Anwendung konzipiert sind.

Am Anfang stand die Eisenbahn

Blindes Vertrauen in die Technik ist bei sicherheitsrelevanten Anwendungen in jedem Industriebereich unangebracht. Die Vertrauenskette, die sich letztlich bis hin zum Bedienpersonal erstreckt, beginnt in der frühen Phase der Produktkonzeption. Bei der Betrachtung der PC-/ARM-Technik von Anzeigegeräten fiel deren Fehlerpotenzial auf; so kann zum Beispiel eine fehlerhafte technische Datenübertragung oder eine Datenkorruption im Grafikspeicher vorliegen oder ein Fehler in der grafischen Steuerung des Displays, in der Visualisierungssoftware, im Betriebssystem, im Treiber des TFT-Signals oder im Mikroprozessor selber. Für eine Anzeige oder Toucheingabe mit Safety- beziehungsweise Performance-Level gilt es einiges zu beachten. Zu beachten:

- Fehler und Obsoleszenzen in modernen komplexen Rechnerkernen, Caches, Grafikeinheiten und Ähnliche müssen beherrscht werden.
- Fehler in Betriebssystemen und komplexer Software müssen bewertet, 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. 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 und sicheres Loslassen)

Sichere Bedienung virtueller Bedientableaus

Als Antwort auf diese Fragen entwickelte Deuta die Sicherheitsfunktionen IconTrust und SelectTrust um Darstellungs-

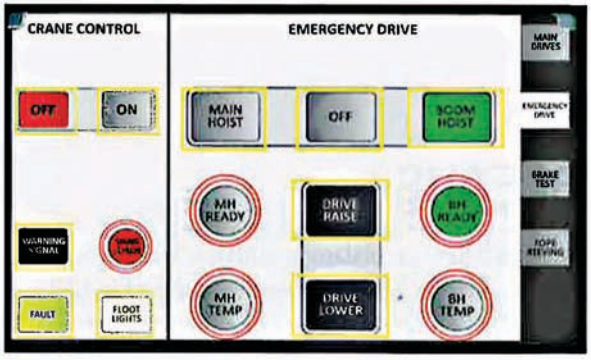

Abbildung 1: Bei diesem virtuellen Bedientableau stehen die roten Markierungen für die sichere Anzeige und die gelben für die sichere Eingabe.

und Bestätigungsfehler des unsicheren PC-Systems in einzelnen Funktionen zu detektieren. Beide Überwachungssysteme arbeiten vollständig entkoppelt von der Darstellungs- und Bedienfunktion. Die Endanwender können existierende Applikationssoftware mit dem IconTrust/SelectTrust-Konzept weiter verwenden. Die Technologien arbeiten unabhängig von Betriebssystemen, Programmiertools, Programmiersprache und Bibliotheken. Es gibt keine Beschränkung auf zertifizierte Softwaretools oder stark reglementierte Kodierregeln.

Funktionsweise der sicheren Eingabe

Speziell für virtuelle Bedientableaus bietet IconTrust eine Technologie für die sichere Anzeige bis PL-e oder SIL-3. Die SelectTrust-Technologie ermöglicht eine Touch-Eingabe mit dem Performance Level PL-d oder SIL-2. In einer Verarbeitungskette von der Berührung eines grafischen Elements auf einem Touchscreen, über die Zuordnung eines entsprechenden Informationsgehalts aus den ermittelten Koordinaten, bis zur Übermittlung der Information an beispielsweise einen Steuerungsrechner, können verschiedene Fehler auftreten. Aufgrund des komplexen Verarbeitungsprozesses ist es nicht immer möglich diese Fehler zu offenbaren, was aber eine zwingende Voraussetzung für die Eingabe von sicherheitsrelevanten Informationen am Touchscreen ist.

Damit der sichere Rechner eine, auf klassichem Wege erstellte Information überprüfen und mögliche Fehler feststellen kann, erstellt SelectTrust parallel eine Referenzinformation die, vom klassischen Toucheventhandling des HMI unabhängig ist und direkt aus dem angezeigten Bilddatenstrom generiert wird.

Dabei wird über das Anzeigeüberwachungsverfahren IconTrust, den selektierten grafischen Elementen direkt eine Signatur zugeordnet und eine entsprechende Prüfsumme generiert. Diese Prüfsumme repräsentiert den Inhalt des durch den Bediener ausgewählten grafischen Elements eindeutig.

Korrekte Touch-Eingaben gewährleisten

Neben der „klassischen" Behandlung von Touchevents innerhalb komplexer HMI-Strukturen generiert SelectTrust direkt aus den angezeigten Bilddatenstroms eine vom ersten Informationspfad unabhängige, Referenzinformation. Anhand dieser zweiten Information kann der sichere Rechner die Korrektheit des ersten Informationpfads überprüfen.

Die patentierte SelectTrust Technik erlaubt die Ein- und Ausgaben sicherheitsrelevanter und nicht sicherheitsrelevanter Informationen innerhalb derselben HMI-Einheit zu realisieren. Damit ermöglicht es die Nutzung von leistungsfähiger Standard PC-/ARM-Technologie und deren Vorteilen. Somit erhält die sichere Steuerung die durch den HMI-Rechner ermittelte Information und zusätzlich die von SelectTrust generierte Signatur.

Trust-Technologien sorgen für korrekte Daten

Die beiden Trust-Technologien IconTrust und SelectTrust stellen die Aktualität und Korrektheit der angezeigten Daten sicher, ohne dass die eigentliche Applikation zur Darstellung der Informationen, die auf unsicherer TFT-Technik beruhen kann, einem Nachweisverfahren unterworfen werden muss. Aufgrund dieser Unabhängigkeit ist der Einsatz eines der Systeme auch in anderen Industriebereichen als virtuelle Bedientableaus vorstellbar. Der Sicherheitsnachweis mit SIL-Zulassung für die IconTrust-Technologie ist unabhängig vom Visualisierungssystem, den Software-Entwicklungswerkzeugen sowie der Hardwarekonfiguration. Es ist sogar möglich, existierende Applikationssoftwaremodule wiederzuverwenden und existierende Anlagen zum SIL-Equipment nachzurüsten. ☐