Mensch-Maschine-Schnittstellen

Bedien- und Anzeigegeräte mit TFT-Technologie

Dr. Rudolf Ganz, Deuta-Werke GmbH, Geschäftsführer, Bergisch Gladbach

Die Mensch-Maschine-Schnittstelle oder auch Human-Machine-Interface (HMI) spielt für den Bahnbetrieb eine wichtige Rolle. Da es sich um komplexe Prozesse handelt, bei denen auch unerwartete Situationen/Zustände im Systemkontext nicht ausgeschlossen werden können, muss der Mensch als letzte Prüfinstanz und Eingriffsmöglichkeit sich auf die ihm dargestellten Informationen des Systems verlassen können und sein Eingriff vom System verlässlich und korrekt interpretiert werden. Ein von der HMI-Plattform unabhängiger Überwachungsmechanismus erlaubt die Verwendung von üblichen Rechnereinheiten mit Flachbildschirm (TFT) und Touchscreen selbst für HMI mit sicherheitsrelevanter Information.

Im Rahmen einer Gefährdungsanalyse muss geprüft werden, ob moderne sicherheitsrelevante TFT-Anzeige- und Bediensysteme in die Sicherheitsbetrachtung bzw. -nachweisführung sowohl für Bahnfahrzeuge als auch für elektronische Stellwerke mit einbezogen werden müssen. Heute werden viele dieser Einheiten aus wirtschaftlichen Gründen zumeist mit PCs (oder vergleichbaren) Hard- und Softwarekomponenten realisiert. Diese Rechnereinheiten werden zwar immer leistungsfähiger und erlauben unter anderem eine gute ergonomische Gestaltung des HMI, entfernen sich jedoch aufgrund der damit verbundenen ständig wachsenden Komplexität von der fundamentalen Forderung nach Einfachheit für sicherheitsrelevante Einrichtungen.

Anforderungen

So ist die Auswirkung potenzieller Fehler innerhalb der vielschichtigen und kollaborierenden Strukturen einer solchen Einheit auf die korrekte Erfüllung der Anzeige- beziehungsweise Eingabefunktion von Informationen nur schwer erfassbar. Neue Multi-Core Prozessoren mit Merkmalen wie zum Beispiel „Hyper Threading", „spekulativer Ausführung", die zudem über lange Errata-Listen aktuelle, oft nicht behobene Fehler dokumentieren, sind im Rahmen einer Sicherheitsnachweisführung kaum beherrschbar.

Ansätze zur Realisierung von HMI für sicherheitsrelevante Informationen allein auf der Basis von Standard-PC-Komponenten sind selbst bei Einhaltung entsprechender normativen Vorgaben an einen Entwicklungsprozess oder/und bei der direkten Integration von Prüfmechanismen innerhalb einer solchen Plattform kritisch zu betrachten.

Um den Aufwand einer solch umfangreichen Betrachtung zu vermeiden, die ggf. mit jeder projektspezifischen Änderung bzw. bei jeder Hardwareänderung der teils nur kurzzeitig verfügbaren PC-Komponenten wiederholt werden muss und dennoch die Vorzüge einer leistungsfähigen Rechnereinheit nutzen zu können, ist ein von der Plattform unabhängiger Überwachungsmechanismus zweckmäßig. Dieser sollte aus einfacheren Komponenten mit Langzeitverfügbarkeit und weitgehend projektunabhängig bzw. generisch sein.

Anforderungsdefinition

Für eine sichere Anzeige- bzw. Bedienfunktion sollten (beispielhaft) folgende Bedingungen erfüllt werden:

- Eine Information, die im Bezug auf die Anzeige auf einem HMI (im Rahmen einer Gefährdungs- und Risikoanalyse) als sicherheitsrelevant klassifiziert wurde, darf dort nicht über einen Zeitraum länger als die zulässige Fehleroffenbarungszeit T_{off} (abhängig vom erforderlichen Sicherheitsniveau), mit falschem oder veraltetem Informationsgehalt angezeigt werden, ohne dass der Fehler offenbart wird und eine sicherheitsgerichtete Reaktion ausgelöst wird.
- Es muss sichergestellt sein, dass Verfälschungen bei der Übermittlung von Informationen, welche durch bewusste

Selektion eines Bedienelementes eines Anzeige- und Bediengerätes durch einen Menschen in das System eingebracht werden, beim Adressaten der Information zweifelsfrei erkennbar sind.

Unabhängige Anzeigeüberwachung

Die obigen Anforderungen werden durch den IconTrust®-Überwachungsmechanismus in vollem Umfang erfüllt. Das Prinzip von IconTrust® basiert auf einer Sensoreinheit, die das Ergebnis der Bildgenerierung des Bedien- und Anzeigegerätes – also die Signale vom PC zum TFT-Panel – analysiert und in eine Form überführt, in der es durch einfachste Rechentechnik auf Korrektheit überprüft werden kann (Abbildung 1).

Dabei wird angenommen, dass eine Quelle von verlässlichen Daten, im sicherheitstechnischen Sinne, vorhanden ist, wie beispielsweise der sichere Fahrzeugrechner EVC, der Stellwerksrechner, usw. Diese Datenquelle übermittelt Datenwerte an den darstellenden Rechner (PC), die unter anderem sicherheitsrelevante Größen hinsichtlich der Anzeige beinhalten. Dieser PC erstellt daraus die Graphikinformationen und sendet einen entsprechenden Pixeldatenstrom zum TFT-Panel. Aus diesem erfasst nun eine Sensoreinheit die für die Anzeige von sicherheitsrelevanten Informationen genutzten Abschnitte (rechteckige Bildschirmbereiche als Zeilen- und Spaltenabschnitte) und weist den Daten während jeder TFT-Aktualisierung eine Art Prüfsumme zu. Diese Prüfsumme wird dann in Echtzeit mit den für die bestimmte Darstellung in der Projektierungsphase bestimmten Referenzprüfsummen abgeglichen (Plausibilitätsprüfung) und mit der für den aktuellen Wert der Eingangsgröße erwarteten Prüfsumme verglichen (Prüfung auf Korrektheit). Das Vergleichsergebnis kann nun je nach Anwendung zur Auslösung einer beliebigen, sicherheitsgerichteten Reaktion genutzt werden.

Im Systemdesign der Überwachung verschiedene Architekturen möglich. Während, wie in Abbildung 1 gezeigt, ein Sensor die durch den anzeigenden Rechner übermittelten Bilddaten verarbeitet und eine entsprechend charakteristische Signatur an die Quelle der Information zum Vergleich zurück sendet, so findet der Vergleich nach Abbildung 2 innerhalb des HMI/Panel-PC direkt statt. Hierzu müssen die entsprechenden Referenzinformationen an den Vergleicher (zum Beispiel zweikanaliger Mikrocontroller) übermittelt werden. Vorteil in der zweiten Variante ist, dass die sicherheitsgerichtete Reaktion ggf. durch ein Unterbrechen des Datenstroms oder eine Einfärbung direkt durchgeführt werden kann, wohingegen bei dem Rückspielen der Prüfsummen zur Quelle diese die Reaktion im Bedarfsfall auslösen muss (zum Beispiel Warnlampe). Die Fehlererkennung ist jedoch in diesem Fall direkt an die Informationsquelle angebunden.

Mit dem Verfahren ergeben sich nun unter anderem die folgenden Vorteile:

- Es werden die Bilder mit der Bildwiederholfrequenz des TFT verarbeitet. Eine projektierte Fehlertoleranz ermöglicht die Akzeptanz von ggf. nur Einzelbilder beeinflussenden Störungen zum Erhalt der Verfügbarkeit.
- Die Überwachung arbeitet völlig unabhängig vom PC, sie stellt jedoch die vollständige Fehleroffenbarung aller dem PC inhärenten potenziellen Fehlerquellen im Bezug auf die Darstellung sicher. Daher können auf der PC-Seite

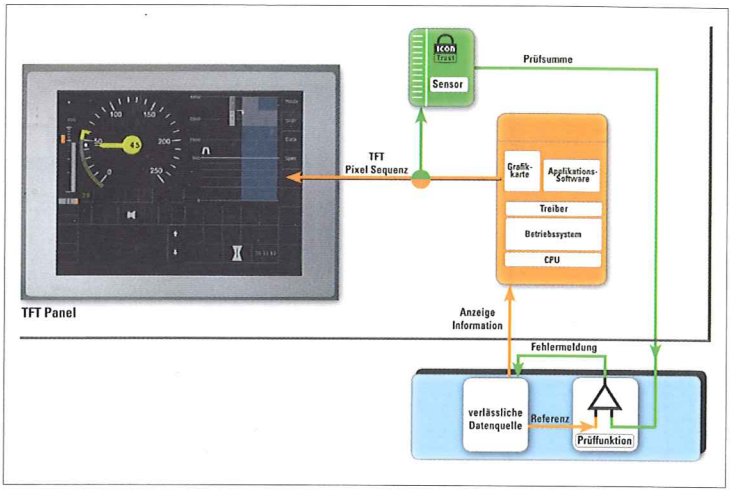

Abbildung 1: Sensor zur Analyse der Bilddaten (IconTrust® Generic)

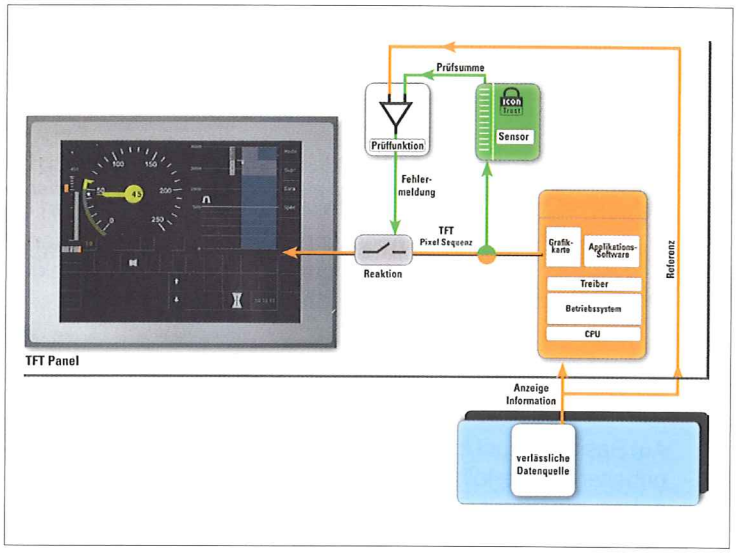

Abbildung 2: Architekturen zur integrierten Überwachung (IconTrust® Plus)

Standardkomponenten in Hard- und Software ohne Einschränkung der Leistung genutzt werden. Änderungen aufgrund von Projektanforderungen und Bauteileobsoleszenz haben keinen Einfluss auf die Sicherheitsnachweise der Überwachungsfunktion.

- Eine Änderung von nicht sicherheitsrelevanten Darstellungsinhalten hat keinerlei Auswirkung auf die Prüffunktion; die Änderung von sicherheitsrelevanten Anzeigeelementen muss ausschließlich in der Konfiguration als Aktualisierung der Referenzprüfsummen nachgeführt werden. Ob ggf. eine Änderungsanalyse erforderlich wird, ist im konkreten Fall mit der Zulassungsbehörde abzustimmen, deren Umfang ist jedoch systembedingt sehr begrenzt.

Somit ergeben sich über den Lebenszyklus eines solchen mit dem IconTrust®-Sensor ausgestatteten HMI-Systems erhebliche Kosteneinsparungen:

- Bei der Ersterstellung kann auf die generischen Nachweise des Überwachungsmechanismus zurückgegriffen und referenziert werden, so dass sich die Nachweisführung auf die Einhaltung der Anwendungsbedingungen beschränkt.

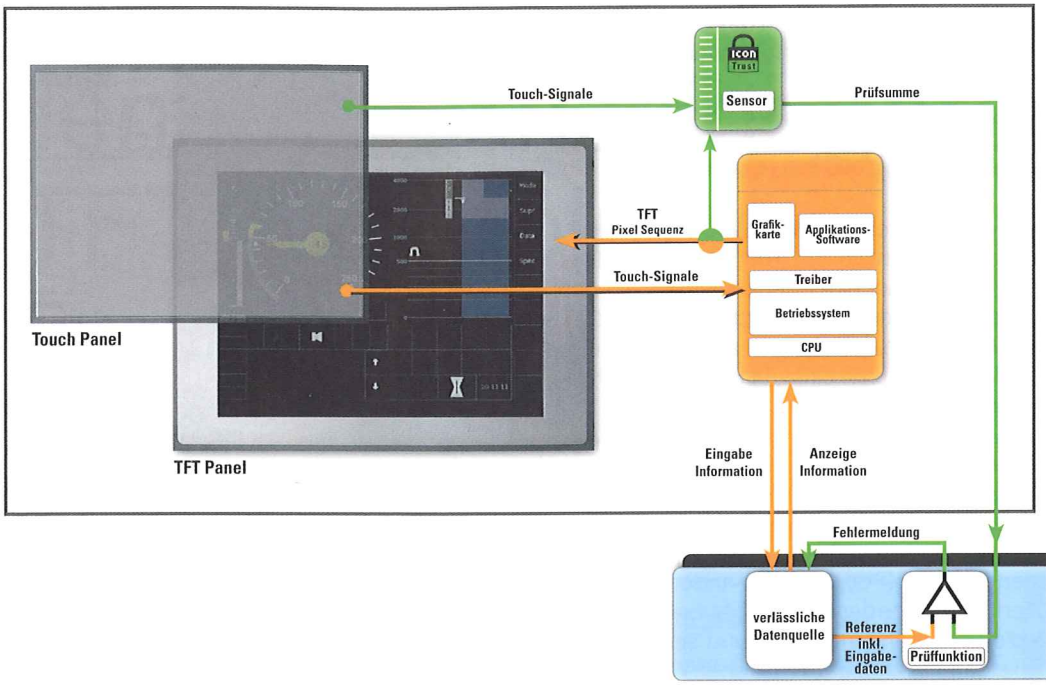

Abbildung 3: Sicherung von Eingaben als Erweiterung der Anzeigeüberwachung (SelectTrust)

- Bei Projekt-/Produktanpassungen ist ggf. kein aktualisierter Nachweis erforderlich, bzw. nur der Nachweis der korrekten Adaption der Konfigurationsdaten.

Erweiterung zur gesicherten Eingabe

Auf Basis der zur Überwachung von angezeigten Informationsgehalten vorgestellten Technik lassen sich auch Bedienereingaben eines mit Touchfolie ausgestatteten HMI absichern. Dazu sei zunächst nochmals auf die oben formulierte Sicherheitsanforderung verwiesen. Der Bediener wählt bewusst ein Bedienelement aus. Dazu sucht er das Element auf der Anzeige (zum Beispiel eine dort dargestellte Taste) und berührt an der entsprechenden Stelle die Displayfront respektive den Touchscreen, was dann standardmäßig ein Touchevent mit den Koordinaten des Berührpunktes an die Verarbeitung durch Treiber, Betriebssystem und Applikationssoftware auslöst. Mit der Verarbeitung wird anhand der Koordinaten eine Zuordnung zu einem Inhalt vorgenommen. Dieser wird dann an den geeigneten Adressaten der Information als Eingabewert weitergeleitet. Auf diesem Weg könnten jedoch all die Verfälschungen durch die auch bereits für die Anzeigefunktion relevanten Quellen entstehen, so dass eine nur auf diese Weise übermittelte Information nicht als verlässlich zu bewerten wäre.

Mit SelectTrust, als einer Erweiterung von IconTrust®, kann jedoch zusätzlich und unabhängig vom Touchscreen eine Information erzeugt und übermittelt werden, die es dem Adressaten erlaubt, die übermittelte Information zu überprüfen und ggf. Fehler festzustellen (Abbildung 3).

Dabei wird das durch den Selektionsprozess des Bedieners ausgewählte grafische Element parallel durch das Anzeigeüberwachungsverfahren unabhängig selektiert, eine entsprechende dem selektierten grafischen Element zugeordnete Prüfsumme generiert und an den Adressaten gesendet. Die Selektion durch den Bediener wird dabei ggf. über einen separaten Touchcontroller oder zusätzlich durch eine zweite Toucheinheit bzw. separate Auslese des einen Touchpanel realisiert. Die ermittelte Position wird jedoch nicht dem PC, sondern dem Anzeigeüberwachungssensor in IconTrust® übermittelt, der dann entsprechend für den nächsten Aktualisierungszyklus des Bildschirms einen der rechteckigen Überwachungsbereiche einem Prüfsummengenerator von IconTrust® zuordnet, der diese dann auf einem separaten Kanal übermittelt. Somit erhält der Empfänger der Eingabeinformation einerseits den durch den HMI-PC ermittelten Wert, andererseits jedoch auch eine Prüfsumme, die er einem eindeutigen Wert anhand von Referenztabellen zuordnen kann. Durch deren Vergleich kann die Verlässlichkeit der Information entsprechend gesichert werden.

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. Grundlage eines Lösungsansatzes muss dabei eine sorgfältige und möglichst minimalistische, wenngleich angemessene Definition der Sicherheitsanforderungen sein. Als technische Lösung für die Erfüllung dieser Anforderungen erweist sich eine von der Darstellungs- und Bedienfunktion vollständig entkoppelte Überwachung IconTrust® als besonders kosteneffektiv, insbesondere bei der Betrachtung des kompletten Lebenszyklus des HMI-Produktes. ■