03.22
V+T Verkehr und Technik
75. Jahrgang
März 2022
Seite 77 – 112
www.VTdigital.de
Organ für den Öffentlichen Personennahverkehr (ÖPNV)
Verkehrstechnik · Verkehrswirtschaft · Verkehrspolitik

Auszug aus der
Verkehr und Technik

Ausgabe März 2022

SÖNKE BRANDT | WALTER SIEGERT | DANA SCHIFFER

Safety Aspekte von COTS-Monitoren

Sichere Anzeige und Eingabe auf Standard-Monitoren bis SIL3

Ausgangslage – Sicherheit heißt „da kann ich mich drauf verlassen" – Sichere Terminals nicht nur auf der Schiene – Sicherheit für Standardmonitore mit einer Auflösung in 1920 × 1080 (Full HD) – Fazit

Dipl.-Inf. Sönke Brandt, *Entwicklung eingebettete Systeme,* **Walter Siegert,** *Programmmanager Industrie, und* **Dana Schiffer,** *Marketing, alle DEUTA-WERKE GmbH, Bergisch Gladbach*

1. Ausgangslage

Jeder Computernutzer kennt die Situation: Der Bildschirm des PCs ist plötzlich eingefroren. Mit einiger Zeitverzögerung prüfen wir den Treiber der Grafikkarte, den Arbeitsspeicher, Hard- und Software oder starten das Betriebssystem neu. Was im privaten Umfeld nur ein ärgerliches zeitraubendes Unterfangen ist, kann in sicherheitsrelevanten oder kostenintensiven Arbeitsumgebungen die

Gefährdung von Menschenleben, Produktionsfehler und Produktschäden bedeuten.

Dennoch wird in Stellwerken, Leitwarten oder Kontrollzentren, in denen Überwachungen, Notfallmaßnahmen oder Kommandooperationen durchgeführt werden, häufig auf Standard-PC-Technologie mit Monitoren und Computermäusen, so genannten „Commercial of the Shelf" (COTS) Komponenten, gesetzt. Dabei muss der Nutzer jedoch verschiedene potentielle Fehlerquellen wie z. B. CPU, Datenspeicherstellen (Hard- und Software), Speicher, Grafikcontroller und Grafikspeicher, Betriebssystem oder Grafik-Softwarebibliotheken berücksichtigen, die zu fehlenden, veralteten oder verfälschten Informationen auf dem TFT führen können. Die Komplexität der Rechentechnik erschwert die Analyse und Aufdeckung möglicher Fehlermodi. Ein Blick in den Windows Support-Bereich genügt, um festzustellen, dass gerade dann, wenn mehrere Monitore angeschlossen werden, immer wieder ein oder mehrere Monitore einfrieren, was in Leitwarten und Kontrollzentren verheerende Auswirkungen haben kann (Bild 1).

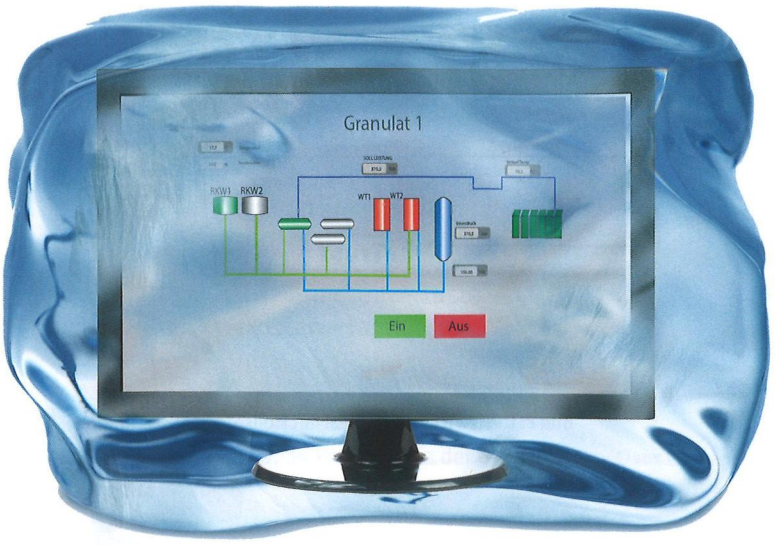

Bild 1: **Der eingefrorene Bildschirm**

2. Sicherheit heißt „da kann ich mich drauf verlassen"

Für die Entwicklung eines sicherheitsrelevanten Mensch-Maschine-Systems bedeutet dies z. B., dass zu jeder Zeit, egal in welcher Anlagensituation, sichergestellt sein muss, dass dem Bediener nur korrekte und aktuelle Daten angezeigt werden, auf Basis derer er seine Bedienentscheidungen trifft. Verschärfend wirkt, dass trotz gestiegener Integrationsanforderungen die Komplexität der Bediensysteme minimiert werden muss, um dem zunehmenden Kostendruck auf den Entwicklungs-, Qualifizierungs-, Fertigungs- und Wartungsaufwand sowie den Produktpreis entgegenzukommen. Für die Sicherung eines Anzeigesystems stehen viele Lösungen zur Verfügung, beginnend von einer kostenintensiven mehrkanaligen Auslegung der Visualisierung bis zu einer kostengünstigen einkanaligen Variante mit elektronischer Sicherungsbeschaltung. Nach diesem Grundprinzip wurde die DEUTA-Sicherheitstechnologie IconTrust® entwickelt.

DEUTA entwickelte mit der Trust-Technologie eine Überwachungseinrichtung, die im HMI-Gerät den Signalfluss der Visualisierung zum TFT-Display und das TFT-Display selbst überwacht. Die Entscheidung, ob innerhalb konfigurierbarer Überwachungsbereiche eine Information korrekt dargestellt oder bedient werden kann, wird abgeleitet aus einem Soll-Ist-Vergleich der Prozesswert-Darstellung mit einem Referenzwert.

3. Sichere Terminals nicht nur auf der Schiene

Initiiert wurde der Bedarf nach einer sicheren Anzeige- und Eingabetechnologie durch die Schienenfahrzeugindustrie. Im Rahmen der Baseline 3 und ihren „Sicherheitsanforderungen für die technische Interoperabilität von ETCS Level 1 und 2" steht die verbindliche Spezifikation des Driver Maschine Interface (DMI) als SIL-Komponente im Fokus.

Denn im Führerstand der Fahrzeuge lösen elektronische Anzeige- und Steuerelemente herkömmliche mechanische Geräte und Einzelkomponenten ab. Die modernen Bedienterminals im Führerstand von Zügen werden mit leistungsfähiger moderner PC- bzw. ARM-Standardtechnik aufgebaut, da dies Kostenvorteile bietet und eine ergonomische Gestaltung erlaubt. Dies ist insbesondere wegen der Flexibilität der Anzeigesoftware von Vorteil, die sich schnell für die verschiedenen spezifischen Länder- und Kundenprojektanforderungen anpassen lässt, was zu einer ständig wachsenden Variantenanzahl unterschiedlicher Informations- und Steuerungsdarstellungen in den Zügen führt, die es sicher zu beherrschen gilt.

Doch auch hier gilt „Safety First". Die jeweiligen Gefahrensituationen wurden mit einer zulässigen Gefährdungsrate in so genannten THR (Tolerable hazard rates) gegliedert und mit Sicherheitsleveln versehen. Die Gefahrensituationen reichen von der fehlerhaften Quittierung einer Zwangsbremsung bis zur fehlerhaften Darstellung der Fahrzeuggeschwindigkeit.

4. Sicherheit für Standardmonitore mit einer Auflösung in 1920 × 1080 (Full HD)

Die Sicherheitstechnologie IconTrust® wird bereits seit rund 10 Jahren weltweit erfolgreich in den Führerstand-

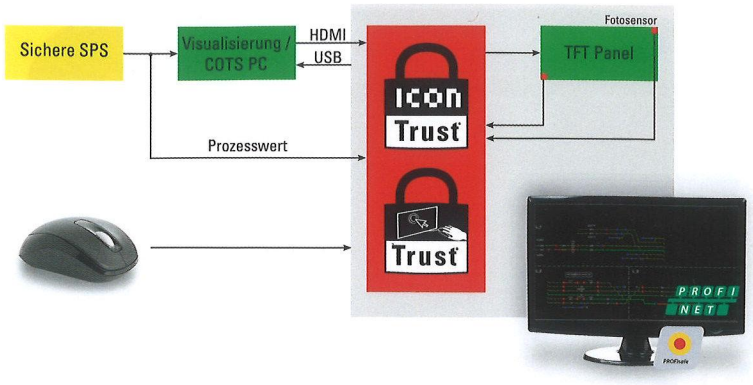

Bild 2: **D-ViewTrust®-Terminal mit MouseTrust®**

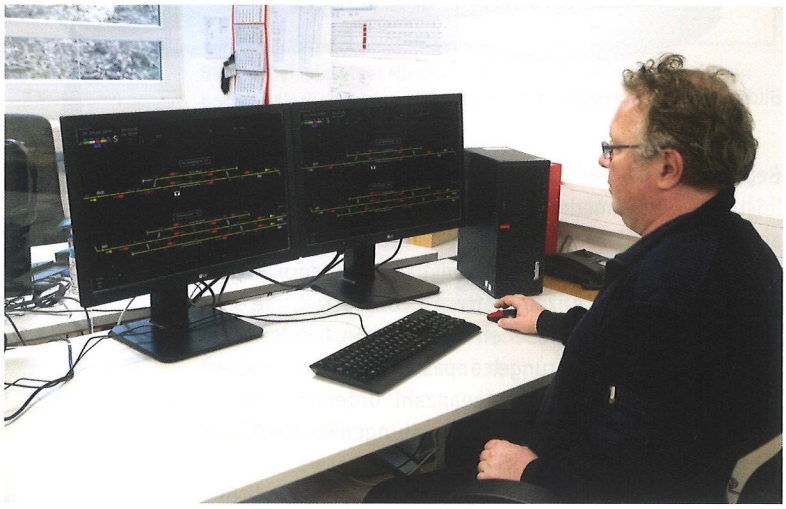

Bild 3: **Ein sicherer Arbeitsplatz – Standard-Monitore mit PROFINET/ PROFIsafe Ausrüstung**

displays von Schienenfahrzeugen eingesetzt. Nun sind diese Sicherheitstechnologien auch in Standardmonitoren mit einer Auflösung von 1920 × 1080 (Full HD) verfügbar. Ob Kontrollzentren, Produktionsstätten oder Leitstellen – überall, wo Informationen sicher angezeigt werden müssen, finden die D-ViewTrust® Monitore mit IconTrust® Technologie Anwendung. Bei Displaygrößen von 17"–24" bieten D-ViewTrust® Monitore ausreichend Fläche, um sicherheitsrelevante Informationen übersichtlich darzustellen – Anzeige auf Bildschirm und Eingabe per Maus bis SIL3.

Grundlage der patentierten Überwachungstechnologie IconTrust® sind ein FPGA-basierter Sensor und ein sicherer Computer. Der zweikanalige Sensor ermittelt aus den darzustellenden Bildinformationen entsprechende Safety-Codes, die der zweikanalig aufgebaute Embedded-Rechner mit den zulässigen Codes vergleicht. Diese Codes sind Fingerabdrücken ähnlich. Bei einem Teach-in werden Referenzwerte für alle Anzeigewerte generiert und im Embedded-Rechner zusammen mit dem korrespondierenden Prozesswert abgelegt. Somit kennt das Überwachungssystem gewissermaßen alle erlaubten Prozessdaten. Im Betrieb übermittelt die sichere SPS dem Bedienpanel die aktuellen Anzeigewerte. Das Bedienpanel generiert die Darstellung, IconTrust® greift mit den FPGAs den Datenstrom zu den TFT-Multiplexern ab und generiert daraus einen weiteren Code. Die Controller vergleichen, ob dieser Code in der Referenztabelle enthalten ist und dem Nominalwert der sicheren SPS entspricht. Falls nicht, erfolgen eine sicherheitsgerichtete Reaktion, die dem Bediener die Nicht-Verfügbarkeit der Anzeige offenbart, und eine Alarm-Meldung an die sichere SPS (Bild 2).

IconTrust® bündelt die Sicherheitsfunktionen für Darstellung und Eingabe: Mit IconTrust® sind die Aktualität und Korrektheit der angezeigten Daten sichergestellt – die eigentliche Applikation zur Darstellung der Informationen, die auf unsicherer COTS-Technik beruhen kann, muss nicht einem Nachweisverfahren unterworfen werden. Dabei kann IconTrust® eine Vielzahl anwendungsspezifisch konfigurierter Bereiche gleichzeitig und unabhängig kontrollieren und bei Abweichung eine entsprechende kundenspezifisch vordefinierte sicherheitsgerichtete Reaktion auslösen.

IconTrust® leitet die Datensätze als Fingerabdruck der aktuell angezeigten Informationen ab. Damit können in mehreren Bildschirmbereichen prinzipiell alle Arten von separat dargestellten Informationen als Graphik, Symbol, Zeigerinstrument, Text oder Farbcodierung unabhängig und exklusiv überwacht werden.

Durch den einfachen, kompakten und autarken Aufbau sind die Anzeige-Komponenten rund um die Sicherungstechnologie IconTrust® von den üblichen Nachqualifizierungen bei Produkt- oder Prozessmodifikationen, z. B. auf Grund begrenzter Bauteilverfügbarkeit der Hardware oder einer Anpassungen der Software, nicht betroffen. Die verwendeten Bauteile für IconTrust® sind im Hause DEUTA-WERKE GmbH vertraglich gesichert langzeitverfügbar und die eingesetzte Schaltungslogik ist ohne Softwareänderung kunden- und anforderungsspezifisch adaptierbar.

5. Fazit

Die vollständige und durchgehende technische Überwachung eines Bedienarbeitsplatzes ist mit der vorhandenen Sicherheitstechnologie IconTrust® auch bei COTS-Komponenten einfach möglich und hat weitere Vorteile: Es werden nicht nur sicherheitsrelevante Anzeige- und Eingabebereiche sicher überwacht. Darüber hinaus wird der Bediener entlastet, weil er nicht in die Überwachung der Monitor-Anzeige eingebunden ist (Bild 3). ■

DEUTA-WERKE

DEUTA-WERKE ist ein Pionier der nachgewiesenen, sicheren Darstellung und sicheren Eingabe auf TFT-Terminals. DEUTA liefert hochverfügbare, redundante Multifunktions-Terminals mit gutachterlichem Sicherheitsnachweis für die SIL 3-Darstellung und SIL 2-Eingabe. DEUTA Trust Technologie ermöglicht die Verwendung generischer Plattformen mit modernsten Prozessoren für performante Darstellungen und somit das höchste Maß an Ergonomie und Gestaltungsfreiraum ohne Einschränkung an die Sicherheit. Der Anwender behält die freie Wahl des Betriebssystems und der Grafik-Tools sowie die Möglichkeit für Upgrades von Legacy-Softwarelösungen.
DEUTA gilt als Marktführer für sichere Terminals mit einer Anzeigensicherheit bis SIL3 und einer Eingabesicherheit bis SIL2.