Technology for the guaranteeing of TFT-based operator and display devices

When it comes to Human-Machine Interfaces, seeing is believing, but errors can occur. RUDOLF GANZ discusses technology for validating displayed control panel information

The Human-Machine Interface (HMI) plays an important role in the railway system. Complex processes are involved in which unexpected situations/circumstances in the context of the system cannot be ruled out. Therefore the operator, as the person who does the final check and with the final possibility for intervention must be able to rely on the system information which is displayed for him and his action must be correctly and reliably interpreted by the system. A monitoring mechanism which is independent of the HMI platform permits the use of standard computer units with TFT and touch screens even for HMIs with safety relevant information.

Specification for the Human-Machine Interface for transmission of safety relevant information

Task formulation for modern HMIs with safety requirements

Within the context of a hazard analysis for rail vehicles as well as for electronic signal boxes, it must be checked whether modern safety relevant TFT display and operator systems must be incorporated in safety consideration and compliance procedures, even though for financial reasons, many of these units today are realised with PC (or comparable) hard- and software components. These are becoming more and more powerful and allow among other things for good ergonomic design of the HMI. They are, however, moving away from the basic requirement for simplicity in safety relevant equipment due to constantly increasing complexity.

Also, the effect of potential errors associated with the multilayered and collaborative structures within such an information entry or display function is difficult to determine. New multicore processors with features such as 'hyper threading' and 'speculative design', which furthermore document long errata sheets of current and often as yet unrectified errors, are barely controllable in the context of safety verification. Approaches for the realisation of HMIs for safety relevant information on the basis of standard PC components alone should therefore be critically viewed, even when they adhere to appropriate requirements within a normative development process and/or if there is direct integration of testing mechanisms within such a platform.

A monitoring mechanism independent of the platform is advantageous in order to avoid such a complex and extensive consideration, which might need to be repeated with every project-specific variation or with every hardware change of PC components possibly only available short-term, and yet at the same time to be able to benefit from more powerful computer units. This should consist of simpler components with long-term availability and should be generic or independent of projects.

Definition of specifications

The starting point is the definition of safety requirements, for example:

'Information which, with reference to an HMI display (in the context of a hazard and risk analysis) has been classified as safety relevant should not be displayed with false or out-of-date information content for a longer time period than the permitted error exposition time T_{off}, depending on the required safety level without the error being revealed and a safety reaction being activated.

It must be guaranteed that corruption during the transmission of information, introduced into the system by the user through the conscious selection of a control element of a display or control panel, must be identifiable without any doubt by the addressee of the information.'

The independent display monitoring

The architecture of the IconTrust® monitoring system is introduced, which has proven to be both advantageous as well as effective with regard to the above requirements. The concept is based on a sensor unit which analyses the result of image generation of the operator and display device – i.e. the signals going to the TFT panel – and converts them into a form which is possible to check for correctness using the simplest computer technology. This is schematically illustrated in *figure 1.*

It is assumed that a reliable data source from a safety perspective is available, such as a safe SPS, EVC,... This transmits data values to the displaying HMI computer which contains among other things, safety relevant values concerning the display. From the pixel data stream, prepared for display by the HMI computer, a sensor unit captures the sections (rectangular areas of the screen as line and column sections) characteristic for the display of safety relevant information and allocates the data a kind of check sum during the updating of a page. This check sum is then adjusted in real time with the specific reference check sums for the particular display in the design phase (plausibility test) and compared with the expected check sum for the current value of the input variable (verification test). Depending on the application, the comparison result can now be used for activating a user-defined safety reaction.

In the monitoring system design various architectures are possible. As shown in

Figure 1: Sensor for analysis of displayed image data and external testing (IconTrust® Generic)

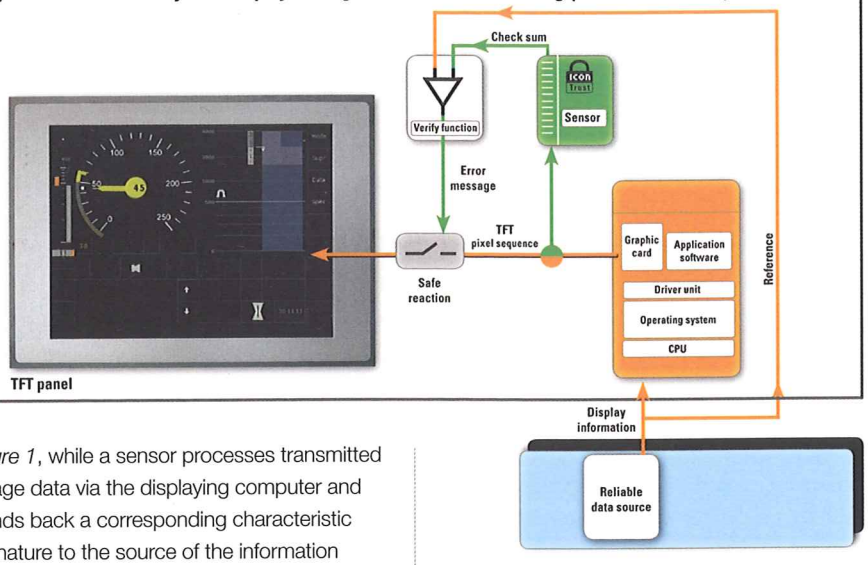


figure 1, while a sensor processes transmitted image data via the displaying computer and sends back a corresponding characteristic signature to the source of the information for comparison, the comparison takes place directly within the HMI/panel PC according to *figure 2*. For this, the corresponding reference information must be transmitted to the comparing element (for example, two-channel microcontroller). The advantage of this in the second variant is that the safety reaction can be directly carried out, where applicable, through an interruption in the data stream or pigmentation, whereas during the redirecting of the check sums to the source, these must trigger the reaction where applicable (e.g. warning light). On the other hand, error identification is in this case, directly tied to the information source.

This process results in the following advantages, among others:

- The images are processed with the refresh rate of the TFT. A projected error tolerance allows the acceptance of even single image influencing interference where appropriate (e.g. EMC), so as not to significantly impair availability.
- The monitoring operates fully independently of the displaying HMI computer. However, it alone guarantees the complete error exposition of all inherently potential error sources for the displaying computer. Standard components in hard and software can therefore be used on the PC side without a reduction in performance. Variations due to project specifications and component obsolescence have no influence on the safety case of the monitoring function.
- A variation in non-safety relevant display contents has no effect at all on the test function; a variation in safety relevant display elements must be updated solely in the configuration of actualisation of the reference check sums.

Whether a variation analysis might be required must be agreed with the licensing authority in a particular case, the scope of which is however very limited depending on the system.

Consequently, considerable cost savings result throughout the life cycle of an HMI system equipped with the IconTrust® sensor:

- At the design stage generic verification of the monitoring mechanism can be resorted to, thereby limiting the verification procedure to compliance with conditions of use.
- During project / product adaptation updated verification is not required; all that might be required is verification of the correct adaptation of configuration data.

The extension to safe entries

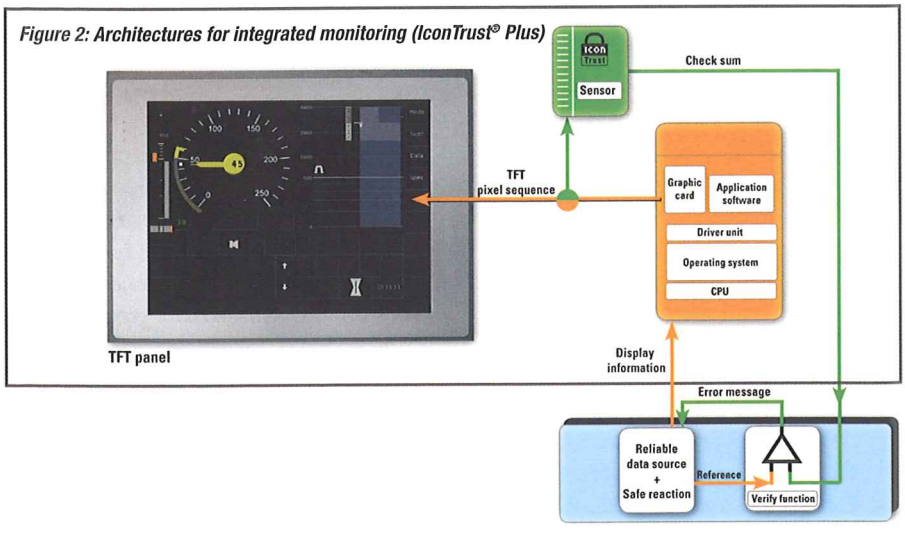
The most recent and major extension of the patented IconTrust® technology is SelectTrust. So far IconTrust® is used for ensuring that what is supposed to be shown on a TFT screen, in fact, is shown on that screen. But due to the variability in the selection of the monitored display area with SelectTrust the selection is driven by touch screen signals. The operator touches the screen in the proximity of the graphic element which he intends to select. Then, SelectTrust positions a monitoring area of IconTrust® right in that area. Consequently, the generated fingerprint finally corresponds to the selections of the data entry of the operator.

This characteristic information is generated independently of any processing element of the PC. The PC could simultaneously compute the touch event via touch controller, driver software operating system, and so on..., hereby assigning the coordinates of the finger contact to a virtually active area of information content. It is clear that this computation is potentially faulty. By comparing now the results of the two independent paths any error may be disclosed.

Different procedural variations of the use of this basic principle such as data entry with multiple (sequential) entry events, modification of the graphic elements shifting them in different position which demand that the operator is following what is shown on the screen when selecting and so on ..., may be used to increase reliability or safety of the procedure

With SelectTrust, as an extension of IconTrust®, it is possible – illustrated schematically in *figure 3* – to create and transmit information in addition to and independently of the touch screen, thereby permitting the addressee to check the transmitted information and to identify errors, where applicable. The chosen graphical element, selected by the operator, is independently selected in parallel by the display monitoring process; an allocated check sum

Figure 2: Architectures for integrated monitoring (IconTrust® Plus)



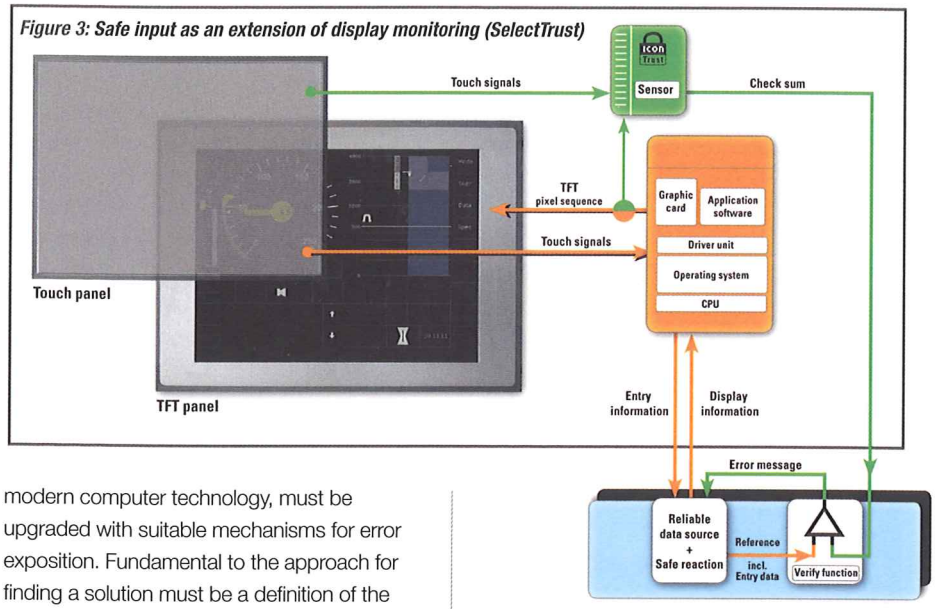
is generated corresponding to the selected graphical element and sent to the addressee. User selection is realised using a separate touch controller or additionally through a second touch unit or separate display of one touch panel.

The determined position is however not transmitted to the PC but to the display monitoring sensor in IconTrust® which then, corresponding to the next screen refresh cycle, allocates a check sum generator to one of the rectangular monitoring areas which then transmits this on a separate channel. In this way, the recipient of the input information receives on the one hand, the value transmitted through the HMI PC, and on the other hand, he also receives a check sum to which he can allocate a definite value by means of the reference tables. By comparing these, the reliability of the information can be guaranteed accordingly.

Conclusion

Display and operator systems which are used for the input and output of safety relevant information and which were realised using modern computer technology, must be upgraded with suitable mechanisms for error exposition. Fundamental to the approach for finding a solution must be a definition of the safety requirements which is as thorough and minimalistic as possible while also being appropriate. The solution of a monitoring system fully decoupled from the display and operating function has shown itself to be particularly cost effective, especially when considered over the complete life cycle of the HMI product. ■■

Figure 3: Safe input as an extension of display monitoring (SelectTrust)



For further information, please contact
Dr. Rudolf Ganz, managaing director:
DEUTA-Werke GmbH
Email: rudolf.ganz@deuta.de
Web: www.deuta.com; www.icontrust.com