STW Technic, LP
Mobile Controllers and Measurement Technologies

Next Generation

Software and Electronic for Heavy Equipment

By Bernd Auer

It's not easy to develop the next generation of a heavy equipment. Giving consideration to all the customer needs and requirements, such as more comfort, better safety and less expensive while at the same time providing a simple "no-worry" package is difficult.

As electronics, software and computer technology enters that once purely mechanical world, modern heavy equipment becomes more like a Boing 777 than a 56 Chevy. Similarly as in the auto industry, electronics continues its triumphal procession. That's easy to believe, because 90% of the innovation is driven by electronic and software.

Without saying, launching a new technology is also sometimes tricky. Electric, electronics and software are oftentimes the reason for machine malfunctions, which doesn't necessarily mean that there are more failures today. Rather it is more likely that it is harder to find and fix these faults. A burst hydraulic hose is simply easier to detect than a corroded connector, which in turn is easier to find than a bug in the depths of software.

Nevertheless, this change of technology can't be stopped. Nobody wants to miss things like servo steering, ABS, ASR, GPS navigation or satellite radio in the car. What is steer-by-wire, remote-radio control, remote maintenance and fleet management on mobile heavy equipment worth? Due to more efficiency, better workflow and more safety they are worth a lot of money.

But how can these improvements be implemented, without having the new technology as the Achilles' heel of the machine?

Standards instead of stand-alone solutions

It's in the nature of technology changes to have many ways of solving technical challenges. Oftentimes, due to the lack of field proven solutions, manufacturers and suppliers favor their own in-house products, which means manufacturer specific closed solutions.
In the 90s, the auto industry began establishing overall standards for programming, operating systems, communication protocols, interfaces, etc. The benefits today are solid field proven components, made cost-effective thanks to the high worldwide quantities.

Standards for electronic and software for mobile heavy equipment

CAN as the standard network to communicate between controllers, displays, sensors, engine control modules, valves, etc. State-of-the-art communication protocols like SAE J1939 or CANopen allow a more or less plug-and-play implementation.

The world wide use of CAN and millions of installations is the behind the availability of the huge number of CAN compatible components at reasonable costs. This means engineers are in the position to choose standardized field proven components. A host of CAN tools help to develop systems fast and easy.

Communication protocols like SAE J1939 or CANopen help the engineers, taking care of bit timing, network management, error management etc. In other words, the communication is an already developed standard, ready to use.

IEC 61131 Tool CoDeSys from 3S
Graphic editors for programming in Sequential Function Chart (SFC), Ladder Diagram (LD), Function Block Diagram (FBD), Continuous Function Chart (CFC, free hand FBD)
Textual editors for programming in Instruction List (IL) and Structured Text (ST)
Full range of standard data types according to IEC61131-3 incl. LREAL with FPU code generation
User defined data types: Arrays, Structures, Enumeration, Alias, Pointer
Comfortable programming with Syntax Colouring, Multiple Undo/Redo, Context sensitive Input Assistance, Context Menus in all editors, Graphic Project Comparison
Library management for creating and managing user defined libraries
Complete offline simulation
Comprehensive Online Functionality: Monitoring, Writing and Forcing of variables and recipes, Debugging of complete projects (Breakpoints, Stepping, Single Cycle, Call Stack), Power Flow, Online Change, Trace Functionality, PLC Browser (command interface to the controller) etc.
OPC-Server, DDE-Server
Communication Gateway for external access and remote maintenance
Hierarchical graphical PLC configuration (Profibus, CANopen, ASi, DeviceNet)
Integrated Visualization (Executable directly in the programming system, in the Windows Runtime, on the Target, via a Web Browser)
Optionally integrated Engineering Interface for connection to Source Code Management Systems, Multi User Operation and general tool interface

Software Engineering

Most manufacturers of electronic controls provide software development tools, which are compatible with IEC 61131-3, the third part of the international standard IEC 61131. It deals with programming languages, and defines two graphical and two textual programming language standards.

- Ladder diagram, graphical
- Function block diagram, graphical
- Structured text, textual
- Instruction list, textual
- Sequential function chart to organize the program control

Telephone +1 (770)242-1002
Telefax +1 (770)242-1006
E-Mail sales@stw-technic.com
Internet www.stw-technic.com

STW-Technic, LP
Mobile Controllers and Measurement Technologies
3000 Northwoods Pkwy. Suite 260
Norcross, GA 30071

As mentioned before, software drives the innovation, and here lies the investment. Proprietary programming interfaces are held hostage by a single company. A standardized programming language assures compatibility with many controller manufacturers, providing backup solutions and second sources.
Another benefit is to have a field proven tool, which is mandatory for safety relevant applications with official registration requirements.

When it comes to official registration there is always the question of, “how field proven are the tools”.
The internationl safety standard IEC 61508 has the following definition of “field proven” software:

- How long is the system field-tested without any changes?
- How many systems are out in the field?
- How diverse are the systems?

Non standard, stand alone programming software for safety relevant applications, with a demand for reliability, are very hard to realize and for this reason too expensive.

Electrical and Environmental Tests

IEC 60204-1	Safety of machinery - electrical equipment of machines
IEC 60529	Degrees of protection provided by enclosures (IP code)
IEC 68-2-1	Environmental testing - Cold
IEC 68-2-2	Environmental testing - Dry heat
IEC 68-2-3	Environmental testing - Damp heat
IEC 68-2-6	Environmental testing - Vibration sinusoidal
IEC 68-2-14	Environmental testing - Change of temperature
IEC 68-2-27	Environmental testing - Shock
IEC 68-2-29	Environmental testing - Bump
IEC 68-2-30	Environmental testing - Damp heat cyclic
IEC 68-2-32	Environmental testing - Free fall
IEC 68-2-52	Environmental testing - Sodium chloride
Life cycle test	Life cycle 52 days operation time with 65°C
Life cycle test	Life cycle, Thermographic with MTBF-calc.

Reliability of a robust controller hardware

Everyone knows what it’s like to buy a PC or digital camera: right after purchasing it’s already out-dated. That’s quite different with controls for mobile machines. The life-time of such machines is up to 15 years, and sometimes longer. During that time the buyer of that machine needs to get back his investment in a sometimes 24/7 operation. The electronics must hold this and spare parts must be available for that period of time. That’s not always easy, and must be considered during the design phase.

95/54/EG 75/322/EWG, ISO 11452-5	EMC Emissions, Immunity Stripline
FCC, 47 CFR	Compliance with FCC Docket 92-152
ISO7637-1, -2	Road vehicles, electrical disturbance by conduction and coupling
IEC/CISPR 25/VDE 0879-2	Limits and methods of measurement of radio disturbance
EN 55011/IEC/CISPR 11	EMC emission (CE conformity)
EN 61000-6-2	EMC immunity (CE conformity
KBA	Certification of Federal Motor Transport Authority (Germany), traffic certificate e1

Reliability here is the keyword. The reliability is the probability, or the rate, that a system can accomplish to defined requirements during a period of time.

$$\text{Re}\,liability = \frac{Total\quad Time - Total\quad Down\quad Time}{Total\quad Time}$$

There are different ratios for reliability, or quality, of the electronic component:

- Malfunction safe operation (robust against operating errors or act beyond control)
- Malfunction related down time (early failure, random failure (MTBF), abrasion failure)

Malfunction safe operation means a failure tolerant system.
For example:

- What happens to the system, if there is for example a short-circuit on the inputs or outputs of the controller due to e.g. a failure in the wire-harness?
- Is the electronic protected against reversal polarity?
- Is EMC an issue?
- What happens through voltage drops?
- Are high or low temperatures a problem?
- Does shock and/or vibration effect the system?

To make a long story short, electronics must go through a substantial testing process to give the peace of mind to put it in a vehicle, in rough environment.

Lifetime system failure rate

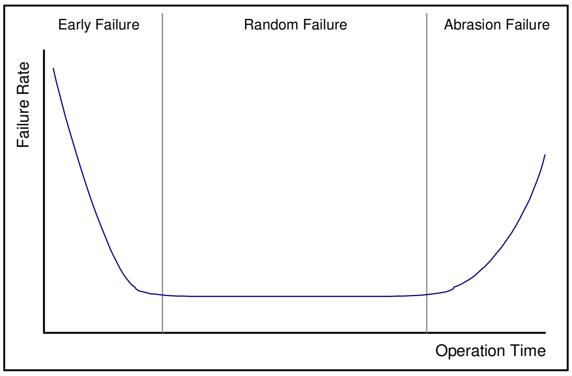
Malfunction over the lifetime of a system can be diagramed in a bathtub curve.

The reason for early failures are most often due to defects in manufacturing and material. Of course the goal is to find such failures before delivery. Modern, state-of-the-art production methods, best test strategies, and a quality management system controlling the whole process are instrumental in doing this.

A relatively constant failure rate (random failure) is only possible during a defined period of time and is reflected through the MTBF (Mean Time Between Failure). The reciprocal value of the MTBF is the failure rate. For example, a MTBF of 10 years is equal to 11.4E-6 failures per hour.

The MTBF is a characteristic of the quality of each single component in the electronics and also the manufacturing. The MTBF must already be considered during the design phase. Because the MTBF is affected by each single component it is directly tied to electronic costs.

The main factors for the abrasion of electronics are the environmental conditions. High temperatures, temperature changes, mechanical shock and vibrations can significantly reduce the lifetime of electronic components.
The right components are critical, but even above this items such as the right spot on the board, housing technology, heat sinking, mechanical damping are the keys which define an experienced electronic manufacturer.
Beside the commercial aspect of reliable electronics there is also the subject of safety engineering, which is worth mentioning here. Without saying, any malfunction must not lead to a dangerous sitiation, neither manufacturing problems, abrasion or a human error.



Functional Safety

As mentioned above, electronic and software drives about 90 % of todays innovations. This is even more important for safety systems, like ABS, ASR, operator assistence systems, load moment indicators and so on.

Accreditation associations, safety organizations, insurance companies, and also the own requirements of single companies or engineers to have state-of-the-art technology are the reasons for more safety on vehicles. And not only those vehicles typically associated with people such as mobile cranes, fire trucks, man lifts, excavators, fork lifts, etc. are taking advantage of this. All manufacturers recognize the need to reduce the risk of major accidents through safety systems and in general through the use of electronics and software for safety related applications.

Functional Safety

DIN V VDE 19250	Principles for safety requirements
DIN V VDE 0801	Principles for computers in safety-related systems
EN 954-1	Safety of machinery - Safety-related parts of control systems
IEC 61508	Functional safety of electronic safety-related systems

But how to determine the risk level in order to plan strategies for the system? The first step is to specify the acceptable risk. Key information are the probability and the severity of an accident. According to the specified risk, there must be defined ways to avoid malfunctions, to detect hard and software failures during runtime and a means to provide safe control of the system when a failure occurs bring the vehicle to a known safe state.

Standards and rules are most often determined through the particular vehicles industry and application. However, an international standard for nearly any kind of safety relevant applications is the IEC 61508. In this paper the safety requirements are diveded into Safety Integrity Levels (SIL), from SIL1, the least safe requirement, to SIL4 the highest level for safety requirements. The Safety Integrity Level, as a result of a risk analysis, defines the system design.

A substantial part of the documentation in IEC 61508 is due to the principle of a lifecycle model, from conceptual design to retirement from the market. This information provides that an early start to design according to the rules of this standard shortens the certification process significantly.

Telephone +1 (770)242-1002
Telefax +1 (770)242-1006
E-Mail sales@stw-technic.com
Internet www.stw-technic.com

STW-Technic, LP
Mobile Controllers and Measurement Technologies
3000 Northwoods Pkwy. Suite 260
Norcross, GA 30071

Outlook

The paradigm shift from a purely mechanical system to a mechatronic system must be accepted first, but the benefits of this step are obvious.

World-wide competition, optimized equipment functionality (much as an assembly line machine), safety aspects and liablity questions are reasons enough.

It is absolutely critical that manufacturers of any kind of on- and off-highway equipment have a good understanding of the technology, which means that they either establish in house their own technology center or rely on a qualified partner to provide the necessary electronic components and design advice.

ESX Family of Controllers

ESX-3XL, freely programmable controller with different extension boards, up to 124 Inputs and outputs
ESX, freely programmable controller with different extension boards, up to 48 inputs and outputs
ESX-LT, freely programmable controller, up to 24 inputs and outputs
ESX-micro, freely programmable controller, up to 10 inputs and outputs
ESX-DIOS/DIOM, CAN-bus addressable I/O modules (CANopen) with 8 (DIOS) or 24 (DIOM) inputs and/or outputs
ESX-C2C, freely programmable data logger and Tele-Service module with CAN, GSM/GPRS