System and Software Design for a modern Grape Harvester Fulfilling State of the Art Functional Safety Requirements

Erik Lautner (Hydac International GmbH)

The article presents an overview of the complex system design as well as of the interactive functionality of the drive and control system of a modern self-driven grape harvester machine.
A modular design for hard and software was developed to fulfill the extensive functional and operator requirements. This approach also complies with the legal requirements of functional safety according to the 2006/42/EC Machinery Directive and the standard "Safety of machinery – safety related parts of control systems" EN ISO 13849-1:2008.

With the new grape harvesting machine model „ERO-Grapeliner Series 6000" (see **Figure 1**) a bunch of innovative machine functions and unique technical machine characteristics could be realized. The effort for the machine assembly and the end-of-line commissioning could be reduced. Additionally the diagnostic and service capabilities were improved.

Figure 1: Grapeliner Series 6000

The redesign process did incorporate the electric/electronic machine control, the hydraulic drive system as well as the application software. To be able to fulfill state of the art control systems safety requirements, it is necessary to look at the system with its different modules in its entirety.
The development process included all necessary steps to comply with the increased safety requirements according to the Machinery Directive 2006/42/EC [1].

Harvesting Process and Machine Functionality

A self-driven grape harvester harvests the grapes by shaking the grape-vines.
To realize this, the grape harvester drives over the rows using the double shaker drive to shake the grapes off of the grape-vine.
The separated grapes fall on the shingle conveyor and slide sideways onto the big conveyor belt. In the course of the conveying residue leaves will be removed by three fan drive systems. Fehler! Verweisquelle konnte nicht gefunden werden. shows a clear model of the harvesting process subsystems.
The destemmer, which is available as an option, separates the grapes in the next stage of the harvesting process from their stems.
After passing the final transverse conveyor the grapes will end up in the grape bin. They can be unloaded sequentially out of the bin onto a truck or continuously by using an additional conveyor belt.

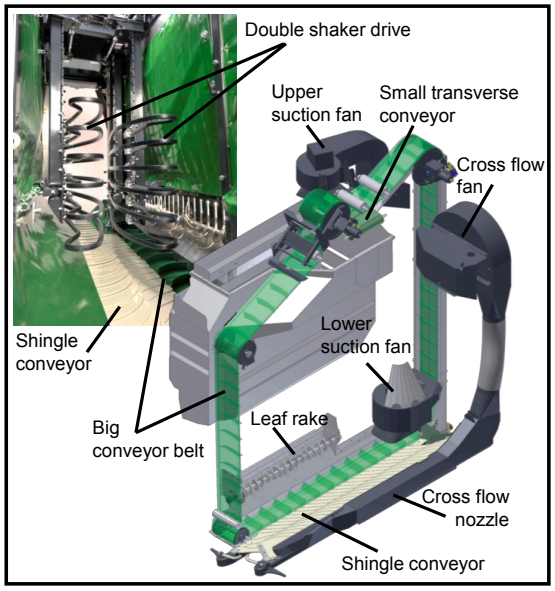

Figure 1: Harvesting process model

Grape Harvester Machine Parameters

The new “Grapeliner Series 6000” (see **Figure 2**) is characterized by the following specifications:

- Diesel engine power up to 147 kW
- Harvesting speed up to 6.5 kph
- On-road speed up to 40 kph
- Maximum steering angle of 90°

Due to the optimized weight distribution in between front axle (45 %) and rear axle (55 %) and the overall machine design, the grape harvester can realize the following driving characteristics:

- Inclines of up to 45 %
- Side slope compensation of 36°% (up to 75 cm cylinder stroke)

This short overview of the most challenging machine characteristics inevitably makes it clear, that for the design of many of the machine functions safety requirements need to be considered.

Figure 2: Driving on-road

Safety Compliant Concept of the Machine Controls

Whilst redeveloping the model range, the control system of the grape harvester was completely revised. This revision was particularly necessary to comply with the tighter safety requirements of the Machinery Directive 2006/42/EC [1]

The development of the safety-related parts of the machine control system is based on EN ISO 13849 [3].

This standard enables the electrical, mechanical and hydraulic subsystems, as well as the complex programmable electronic control technology, to be included in the safety considerations of a complex machine control system. In contrast to other standards, EN ISO 13849 with several physical domains, offers a comprehensive approach, unique for the use in the safety analysis of the controls of mobile machines. The standard is on its way to being developed into a standard approach for machine manufacturers.

It is particularly significant to consider the safety requirements of a control system from the very start of the design process.

At the beginning of the development process the safety functions of a machine must be identified. Furthermore, the following specific characteristics (chosen as examples) of the safety functions need to be defined:

- Error reaction times
- Safe state (in case of error)
- Safety-related function parameters (such as permitted acceleration, speed, temperature, ...)
- Transient response or function sequence into the safe state, as well as
- Priorities between the individual safety functions

Subsequently a hazard and risk analysis must be carried out to determine the required performance level (PL_r) of the individual safety-related machine functions. To enable an efficient, clear approach in the analysis of the individual functions, the machine functions were subdivided into groups:

- Work functions
- Drive functions
- Steering
- Height adjustment

The risk analysis of the machine gave a maximum required performance level of PL_r"c".
It is important to be aware of, that an increased safety level at machine level results not only exclusively into increased requirements concerning electronic components. In fact it results into increased requirements concerning:

- the design of the hydraulic and electronic control system,
- the communication system,
- the configuration of the user interface (HMI),
- the safety-related characteristics of the components, as well as,
- the layout of the software architecture and its implementation

The implementation of the safety requirements in the development of the new series is described below.

Electronic Control System of the Machine

Besides the mandatory consideration of the functional requirements, the design of the electronic control system of a machine is generally based on three main principles:

- the safety requirements arising from the results of the risk analysis,
- the components available and
- the target costs.

The complete electronic system architecture of the machine controls is shown in **Figure** 3. In order to implement the comprehensive functions of the working hydraulics, a total of three control units were installed. The control units are connected to each other, to the "machine control CAN" and to the 10.4" display via a CAN bus connector. Another CAN bus connector, the so-called "Powertrain CAN", enables a direct communication with the control units of the diesel engine and the hydrostatic drive unit.
As the core module of each control, the electronic controller, an in-house safety certified controller HY-TTC90 [7] with PL"d" was chosen. The architecture of the controller generally determines the architecture of the whole system. In order to achieve optimum functionality of the control system the different machine functions each had to be allocated to one of the three control units C1, C2 and C3 that were installed. Optimization of the bus communication was, therefore, crucial to the design of the software.

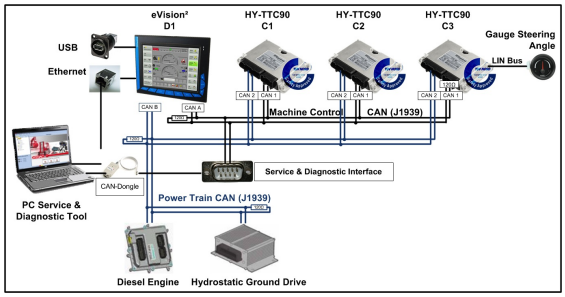

Figure 3: Machine communication architecture

The USB port on the display allows data to be up-/downloaded and provides a simple, customer-friendly means of downloading software in the field. As well as being downloaded to the screen, the software is automatically transferred to control units C1, C2 and C3.

Operating Concept

The operating concept was revised with regard to the requirements of the safety functions. Due to the fact, that many of the *safety functions* are related to:

- a "Prevention of unintentional start-up"

of an e.g. specific fan drive or a conveyor belt, special attention need to be given to the user interface (HMI) design of the activation (start-up) commands.
In respect of the avoidance of an unexpected activation and since the display is not a safety certified component, specifically the activation commands have to be implemented as a solution based on hard wired switches or buttons.

Figure 4: Operating elements for safety compliant function activation

After the re-design the only remaining significant components to activate a harvesting function are the "Harvester activation button" and the "Main hydraulic

switch”. Their position in the driver's cab is shown in **Figure 4**.
Alongside these safety-related amendments to the user interface, all of the machine's, monitoring, parameter setting, comfort and configuration functions are on the other hand completely realized and monitored from the operator's cab on the intuitive 10.4´´ color touch-screen (see **Figure 5**).

Figure 5: Main screen on 10.4´´ display

It shows a complete overview of the harvest parameters and simplifies the operation of the grape harvester considerably. The harvest parameters can easily be adjusted by the driver during operation (online) via the touch-screen.
All of the working hydraulics (shaking unit, fan, conveyor belts, grape bin, ...), the automatic steering and even the de-stemmer are controlled by HYDAC safety controller units. A high level of precision is demanded. For example, the oscillation of the shaking unit must be a maximum of 0.5 %, even under fluctuating load conditions. This means that the operation of the whole machine is permanently monitored. As well as a visualization of the harvest parameters, stoppages in the conveyor belts and the speed of the harvesters, the driver can also see displayed on the terminal information from the diesel engine and hydrostatic drive unit. This enables the operator to deal with malfunctions immediately.

Integrative electro-hydraulic Drive System

The electro-hydraulic drive system of the working hydraulics was completely revised during the redevelopment. The redesign incorporated the following aspects:

- Compliance to the increased safety requirements,
- Improved machine functionality (e.g. control accuracy and sensitivity),
- Reduction in assembly time and end-of line commissioning times,
- Reduction in leakage points,
- Improvement of the filter system and the suction performance of the pumps, as well as,
- Reduction in material costs and production costs.

The result of this redesign is a modern, integrated modular electro-hydraulic drive system. The use of HYDAC's flexible "HyFlex" range (see **Figure 6**) on the one hand and customized valve block solutions on the other, led to a significant reduction in assembly costs and leakage points. The number of hoses was essential reduced by approx. 60 %. The assembly time was therefore substantially shortened.

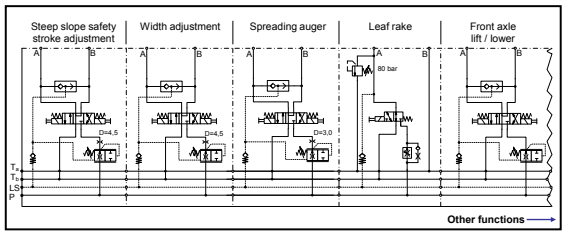

Figure 6: Section of a customized block solution based on the HyFlex

The customized valve technology resulted e.g. in significantly improved and precise speed control of the fan drives. Calibration work on the speed drives is now not any longer needed.
The increased safety requirements were an integral part, amongst other things, of the design of the customized valve blocks, e.g. for steering and the speed-controlled fan drives. As a means of increasing the failure robustness in the system two valves (a proportional pressure reducing valve and a switching valve are) were connected in series (see **Figure 7**).

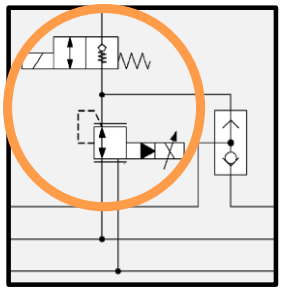

Figure 7: Redundant valve installation

The new filter concept is based on a combined return line & suction boost filter (see **Figure 1**). The component was tailored exactly in size and function to the required application, enabling it to guarantee the filter function and ensure problem-free suction performance of the variable displacement pumps. With this specific design concept, the return lines of all the pumps are combined within the filter housing before going through the filter element. This ensures, generally speaking, that more oil is returned than can be extracted by the variable displacement pumps. A corresponding back-pressure valve in the tank port of the filter housing provides constant positive pressure in the suction port of the pumps. This effectively prevents cavitation in the suction port.

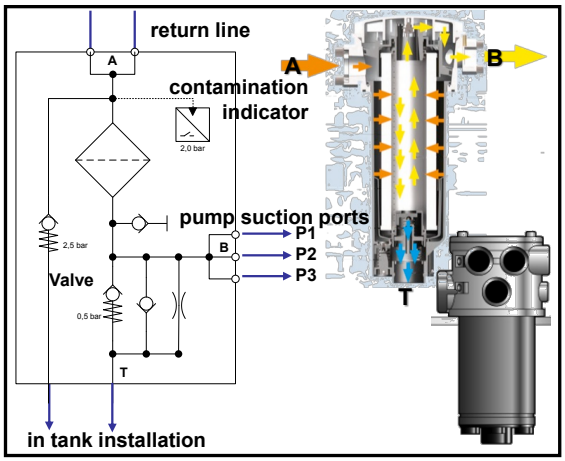

Figure 1: Combined return line and suction boost filter

When calculating the safety function parameters, an accurate filter function is furthermore incorporated into the calculation of the common cause failure with a score of 25.

Automatic Auxiliary Steering System

The automatic steering function is an example for the complex functional and control engineering requirements of the drive system of the grape harvester.
During the harvesting process the machine is guided along the grape-vine rows by an automatic steering system (s. **Figure 2**).
The operation of the automatic steering was assessed as having a safety-related function in the risk analyses. The following safety functions need to be implemented for the automatic steering:

- Safe activation
- Faultless steering function
- Safe deactivation to standard steering

The safe state is “Deactivated automatic steering function”. A maximum error reaction time of 300 ms needed to be covered by the solution.

Figure 2: Automatic steering along the grape-vine rows

The basic function of the automatic steering relies on the signals from a fully-redundant angle sensor on the steering axle, the sensor being operated when the positioning control loop is closed. The steering angle can be manually input to compensate for a gradient.
The position of the vine row is detected automatically by a combination of mechanical steering column switches and ultrasonic sensors. The steering column switches are prioritized.

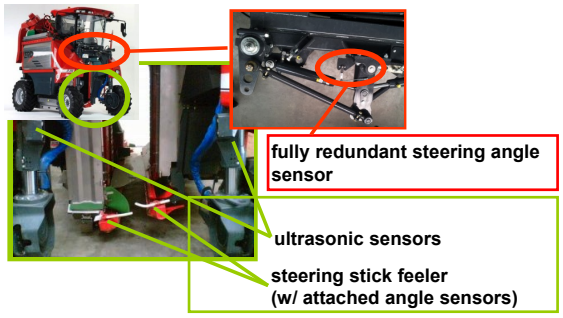

Figure 3: Automatic steering sensors

In order to meet the safety requirements of the steering function a fully-redundant position sensor was fitted for the central sensor element of the position-controlled steering axle. This fully-redundant version also fulfills the requirements of the system FMEA.
The control concept is based on a cascade control loop with PID controllers. The front axle is in the position control loop. The control corrections of the

steering column switches and ultrasonic sensors are superposed onto it.
The change-over function from automatic steering to the standard steering system is also a safety function (see above). The changeover function is coupled to the LS pressure. This means that a sensor with an increased level of safety is used to detect the hydraulic pressure. Within the project the safety certified cost-effective, single channel, Category 2 pressure sensor HDA 8000 sensor was used (see **Figure 4**).

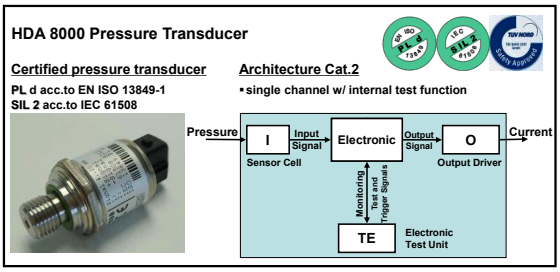

Figure 4: Certified pressure sensor w/ PL"d" in Category 2

In the grape harvester the electro-hydraulic auxiliary steering function was further enhanced by the so-called quick steer function (joystick steering). The activation and deactivation of the function placed a special demand on the user interface. The integrated functionality meant, however, that a very cost-effective architecture could be achieved.

Service and Diagnostic Concept

A state of the art PC service and diagnostics tool enables to service the entire machine independently form the specific manufacturer of the different control units. As well as access to the display and to the three controllers of the working functions, the tool also allows access to the error and software information from the hydrostatic drive and the diesel engine. Therefore the relevant diagnostic interfaces of the manufacturers control units were adapted to enable the integration into the service design of the machine.
A large portion of the service and diag-nostics tool functionality was also directly integrated on the machine display to meet the need for very simple serviceability in the field. As well as providing access to all the different error information, allowing configuration of the machine equipment, providing access to parameters and enabling diagnostics of the inputs and outputs (see **Figure 5)**.

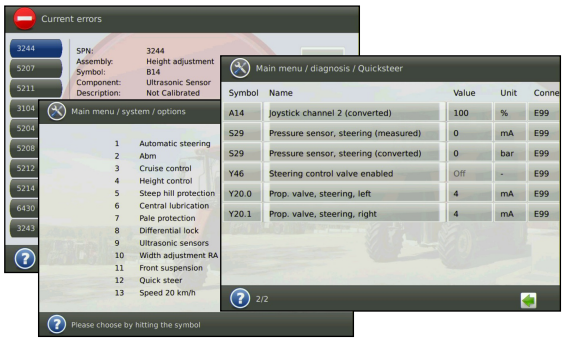

Figure 5: Diagnostics in display

A parameter backup functionality allows a trouble-free replacing of one controller in system. By applying this backup function the replaced controller unit automatically gets the identical parameter setting after replacement.
The display also includes a simulation capability of the output states of the hydraulic valves in order to apply appropriate test scenarios directly on machine (see **Figure 6**). In consideration of the safety requirements the procedure to release the simulation mode is:

(1) Ground speed below 1kph
(2) Select 1st or 2nd gear
(3) Change to simulation page
(4) Start by "harvester unit button"

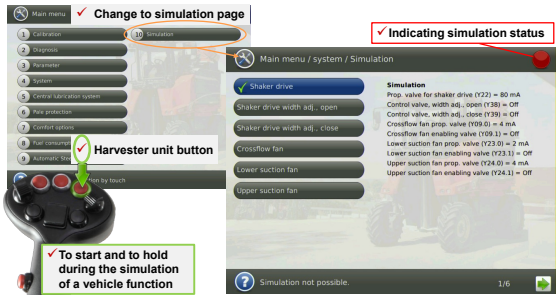

Figure 6: Simulation of valve outputs

All the functionality is multilingual, and the number of languages can easily be extended via an Excel spreadsheet without recompiling the software.

Some Software Aspects

The software design was done specifically under consideration of functional modularity, clear separated layers as well as on a reusability of software library blocks.

The overall software design concept is based on the following three different layers:

- BSP w/ API
- “Standard core software module” w/ connection to the communication protocols and an interface to the library modules
- Application software

The advantage of this concept is specifically the reusability of standard functionalities within the core software. The embedded standard core covers e.g.:

- Hardware I/O initialization
- I/O diagnostics
- NvMem parameter management
- Error management
- Service tool interfaces

The encapsulated core module will be application specific “configured” by means of an auto-code builder.
All of the diagnostic, configuration and parameterization information for the PC service and diagnostic tool as well as for the version on display is automatically generated.

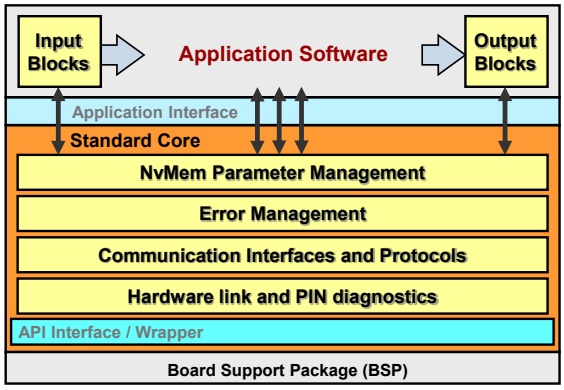

Figure 7: Software layer architecture

Within the application library modules for signal elements as well as input and output driver blocks are used. The library blocks (including the I/O driver objects) have access to the error management system too.
While designing the application software a particular requirement was on the modular design of the software. The modular design is a fundamental prerequisite for an efficient testing of the software.

Summary and Outlook

The new series of grape harvester is impressive with its excellent machine characteristics, an innovative control system and a new operating design which meets the safety requirements of Machinery Directive 2006/42/EC [1]. It has been shown that, in order to implement the requirements of the Machinery Directive successfully and with an eye to market activity, it pays dividends to taken the requirements into account right from the beginning of the development process. The result is a cost-effective, homogeneous control system solution which conforms to safety standards.
Within the scope of development process, functionally sophisticated solutions were also found. The integrated valve design and the new filter design meant that on the one hand the hydraulic functions were considerably improved and, on the other hand leakage sites were reduced and assembly times shortened. Furthermore, it was possible to achieve a reduction in the commissioning time of the machine.
An integrated service concept was developed for the harvester which enabled access to data on all subsystems. A large part of the functionality of the PC service and diagnostics tool could also be integrated in the machine display.
A robust software design concept based on a multi-layer approach in connection with an auto code builder was applied for the application software development.

Erik Lautner
Hydac International GmbH
Projektbüro Potsdam
Behlertstraße 3a, Haus H1
D-14467 Potsdam
+49 (0)331 505701 4440
+49 (0)331 505701 4449
erik.lautner@hydac.com
www.hydac.com

References

[1] Official Journal of the European Union, L157/24,EN,9.6.2006 “Machinery directive” DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast). 2006

[2] ERO-Gerätebau GmbH. Operators Manual Grape Harvester SF200. 2009

[3] DIN Deutsches Institut für Normung e.V., Safety of machinery – Safety-related parts of control systems – 2008,
Teil 1: Part 1: General principles for design (ISO 13849-1:2006), German Version EN ISO 13849-1:2008.
Part 2: Validation (ISO 13849-2:2003), German Version EN ISO 13849-2:2008

[4] DIN Deutsches Institut für Normung e.V., Safety of machinery – General principles for design – Risk assessment and risk reduction (ISO 12100:2010); German version EN ISO 12100:2010. 2010

[5] DIN Deutsches Institut für Normung e.V., und VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V., Functional safety of electrical/elctronic/programmable electronic safety-related systems -
Part 1: General requirements (IEC 61508-1:2010) German version EN 61508-1:2010
Part 2: Requirements for electrical/ electronic/programmable electronic safety-related systems (IEC 61508-2:2010) German version EN 61508-2:2010
Part 3: Software requirements (IEC 61508-3:2010) German version EN 61508-3:2010

[6] Michael Hauke et al., Department 5 accident prevention – product safety, BGIA (today: IFA) – Institute for Occupational Safety and Health of the German Social Accident Insurance. BGIA-Report 2/2008 Functional safety of machine controls – Application of EN ISO 13849. 2008

[7] HYDAC specification sheets:
Pressure sensor HDA8000 SIL2,
Safety Controller HY-TTC90,
Display HY-TTC 10,4“ (w/ touch screen)