

Safety Systems and Concepts for Process Applications

Holger Wicht Pilz GmbH & Co. KG, 73760 Ostfildern, Germany

Justin C. Farrell Pilz Safe Automation, Clayton, Victoria, Australia.

As process steps are more and more linked together, control systems have become more and more complex. Reactions to errors in such control systems are therefore becoming more difficult to evaluate and difficult to prevent.

Some errors can not be foreseen and at critical process steps electrical safety is necessary to bring the process into safe conditions. It is just a matter of the risk to fail and the hazard: This is the safety aspect of a control system summarized in a simplistic manner, in reality there is often a large amount of documentation just for one plant or production process. Safety is often considered as a question of what is acceptable. Therefore safety is influenced by the worker, management, company culture and national authorities which represent the interests of the national population.

On the other hand, there are errors which only have an impact on productivity – at least initially. These negative results are normally prevented with a fall back solution. It is usually a financial decision based on the downtime costs as to how much a company is willing to spend. This is the availability aspect of control systems.

Maintenance is due to wear and tear or for cleaning and the prevention of calculated, or repair of unexpected failures. The first part of the maintenance job makes safety obvious. The second part of the maintenance aspect is to keep the system running and to maintain safety.

All these aspects have to be optimized in control systems. There might be regional differences in the solution, but the control system is a compromise regarding these aspects and of course cost. The safety concepts we present in this paper are two examples of how safety can be implemented, with benefits for the maintenance and productivity, and in summary less expensive than traditional solutions. It is just a question of good concept design and using the possible technical solutions.

Tank farms are a common process application which is spread across a large number of industries. The example shows a leading independent logistic and storage capacity supplier for oil and gas. The company has facilities worldwide. Tank farms are their primary source of income, without tanks there is no business. The need for reliability of tank farm control system is obvious. Tank farms normally cover a significant area, meaning the control signals are distributed and wiring goes over long distances.

A traditional safety system was previously installed. This solution was based on relays to cover the most important functions. For two significant reasons it was reasonable to consider changing the safety concept: 1. Communication between the separate safety circuits was necessary but not feasible, due to complex relay interconnections. For the same reason diagnostics were very poor. 2. In case of emergency it was not unusual for maintenance to have a lengthy search for the cause, instead of having a diagnostic display for safety messages or integration into the SCADA system. Due to upcoming expansion a global safety concept was setup. In general the safety concept design and realization can be described in different steps as shown in Fig.1. Often companies choose external services for the individual steps. The Distribution of I/O over a large area is typical for tank farm safety systems. This

and the aforementioned aspects led to the choice of a system based on safety PLC's and a Safety bus network.

Regarding the safety aspects, the system fulfills category of the European Norm EN954-1. Economically, the new systems cost was clearly below a relay based concept. Not calculated was the benefit for later enlargements. In respect to the maintenance aspect: the safety system provides full diagnostics to the SCADA system. Modifications are to be done with software.

What is the difference to safety between software and hardware based solutions? It seems to be easier for human errors to lead to faults in programming and thus safety problems. This is not true on the second view: Software in safety applications has to be approved as part of the whole system. To assist in safe programming, the safety component supplier can provide a range of approved software function blocks, for example - Emergency Stop. In general there is no disadvantage regarding safety due to errors during programming or wiring a safety control system. Normally there is just more functionality integrated in a software based system, than in a relay based concept for the same application.

The overview of the area (fig. 2) shows the distribution of the main IO points. Beside the typical safety functions the loading and unloading points as well as the control room has to be integrated in the safety system, especially for maintenance reasons. With the interconnection of loading points, tanks and the control room, complete communication and diagnostic can be realized, which makes it easier to react in terms of safety error messages. Certainly important for new investment is to check the compatibility of a safety system to the standard control part and it's different bus protocols (Modbus or the different Ethernet protocols).

Phase one included 3 Bus systems: One bus system for gas and fire detection and to control the sprinkler systems. The other 2 bus systems were mainly responsible for the control of Emergency Stops (E Stops). Bus number 2 was for the E stop chain of the jetties, gas unloading points and the chemical pits. On the output side the major part of the signals were linked to the valves for shut down or to re-route. A major benefit for the company was the existing fibre optic cabling in the ground. The safety bus system is able to communicate on fibre optic and it was easy to install the rest around. It gets more difficult if the wiring has to be done from new, and even worse if it is not just a bus cable but arm thick parallel wiring. Recent developments already use radio frequency controlled communication which is also available for this safety bus system. There are several very useful hardware components for such a safe bus system which make it much easier to realize certain bus structures. Typical for a system with several safety networks is the interconnection between the bus systems with a bridge or router to drive different baud rates and therewith to enlarge the complete system over long distances.

Just to give an impression about what is possible regarding bus structures: Today typical dimensions for safety bus systems are around 500m up to 3 km (extreme :6km) with traditional bus cable. With fibre optic routers the safety network can be expanded up to 40 km. Radio transmission on a safety protocol is already in use for cable cars in mountains.

The diagnostics and visualization of the example uses a local display where the messages of each safety controller are displayed and the monitoring in an operation control room.

To summarize the most important aspects for tank farms and their safety control systems: Today there are technical solutions which offer decentralized safe data communications and reduce the investments for the installation. There are major advantages for maintenance regarding diagnostics and visualization. Enlargements can easily be done and shut downs for later modifications are reduced to a minimum. The availability aspect: by splitting such safety networks into different groups it is possible to selectively shutdown, which helps to maintain productivity. Redundant safety control systems (3003) for high availability are not necessarily required.

The second example for an optimized safety system is about burner management applications(BMS): All around the world thousands of BMS are installed which do not fulfill appropriate safety levels. But this is not the only reason to change such a BMS: often these relay based control systems have reached a life cycle where relays do not work reliably any longer. For small BMS it is rather easy to fix such an error. But as many modifications are done during time critical situations (unexpected downtime during a failure: the system has to be made operable again) changes are often not documented which makes the next repair more difficult. Therefore even small BMS applications with traditional relay control are not maintainable after a certain time. A different reason for a renovation is to reduce emissions and make the system more efficient. Safety can be an additional aspect. Calculations show that after 3 years the investment has payed off for a new BMS system which offers better control possibilities and is efficient. Beside a relay based control system there are special components in use for the complete system: flame detection, flame control, burner control. The objective is to replace the relay based control systems and to integrate the safety functions into one system. Depending on the size of the BMS different solutions are possible. Typical safety functions of a small BMS are presented in fig. 3. Fig 4 shows a typical control cabinet of an old BMS.

This example shows the aforementioned different control devices of such a BMS.

Looking at the maintenance aspect: Obviously the cabling is already complicated but at least there was a low level of diagnostics. Not only for maintenance but also for operators a very critical situation: the control system was not in a closed cabinet but just mounted on a panel, open and with 230 V loaded. The reliability was a major problem because of relay failures.

The new system was based on a safety PLC. The safety requirements for the new system where:

- < Replacement of the burner control device
- < Replacement of the leak control device
- < Control of the flame detectors
- < Control of the safety sequence
- < Control of E stops
- < Control of software parameters such as temperature, gas pressure, air pressure, flame intensity

Beside the safety aspects the system fulfilled some non safety related functions:

- < Communication to the SCADA system
- < First level error diagnostics

It is an appropriate example to show how in new solutions software replaces hardware functions. In the safety system there are software function blocks used which offer typical BMS functions. A major concern certainly is to be sure that the software is safe. This includes application software (program, programming tool, software blocks) as well as the operating system. There are two major possibilities why software can be unsafe: technical reasons like changed signals during download or upload from the program editor hardware to the controller or human mistakes. Alterations in the application can lead to unexpected results such as an E-stop perhaps will not shut down or other reactions are not performed. Therefore software based systems for safety require certain measurements which prevent unsafe conditions. This is a completely separate issue and will not be treated at this time but examples can be provided on inquiry. Fig 5 shows a typical sequence of a software block for a BMS application.

Those controller/software based safety systems are able to serve small burner applications with just one oven or up to huge applications even for power and steam generation. Another BM application shows an example with 69 Burners.

To summarize: BMS electronic safety devices such as safety PLC's offer a good foundation to optimize a relay based control system. Flexibility and the diagnostics are of great benefit for maintenance. From

Conference RAM + Safety

Kuala Lumpur 29-30. Nov 2004

the point of view of production it is obvious that these wear free solutions offer a clear advantage in availability.



Fig 1

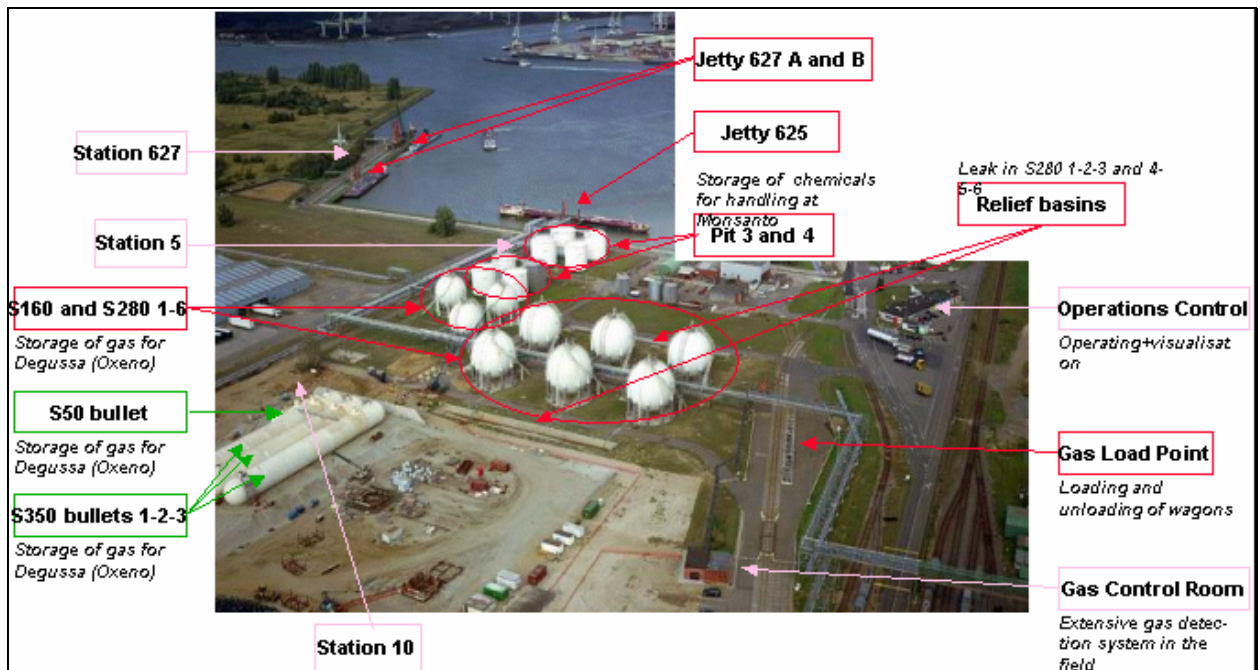


Fig 2

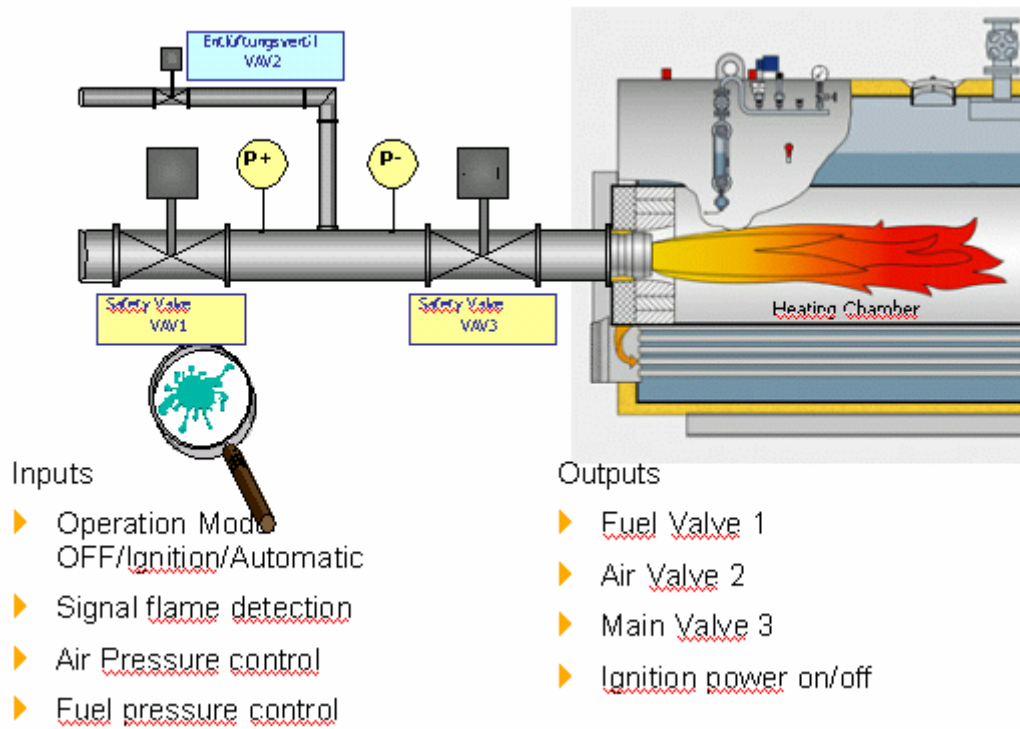


Fig 3

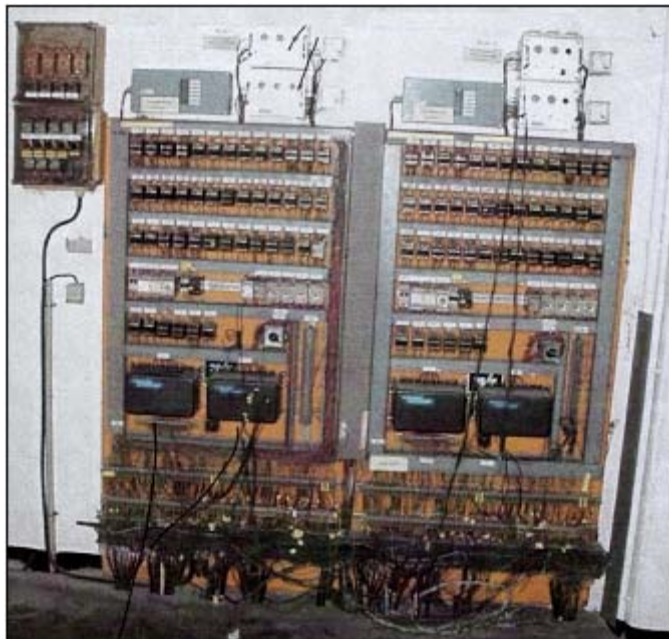


Fig 4

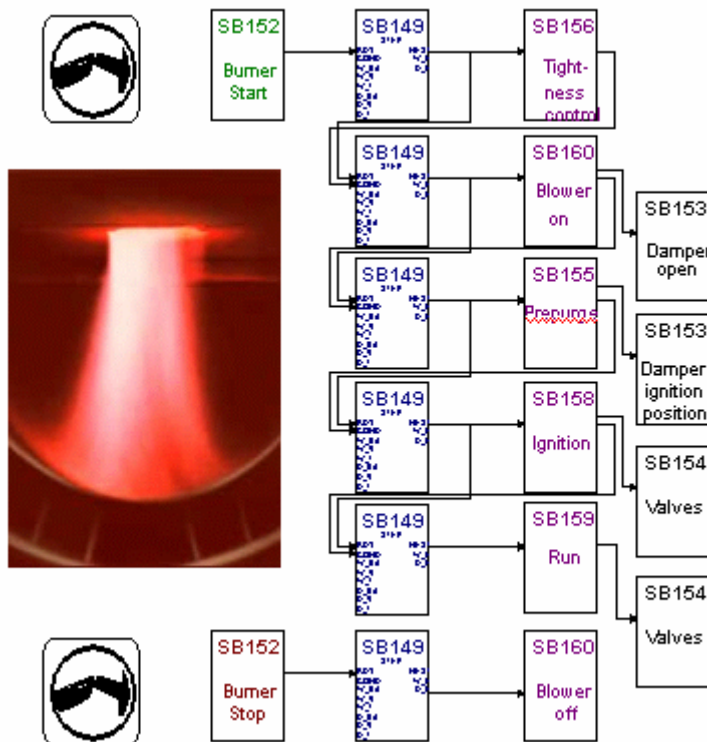


Fig 5