Commissioning of a type approved PLC

Ekkehard Pofahl
TÜV Rheinland,
Cologne, Germany

Differences between ESD and Continuous Control Systems
PLC restrictions as a result of a type approval
Representative restriction
Commissioning and acceptance test

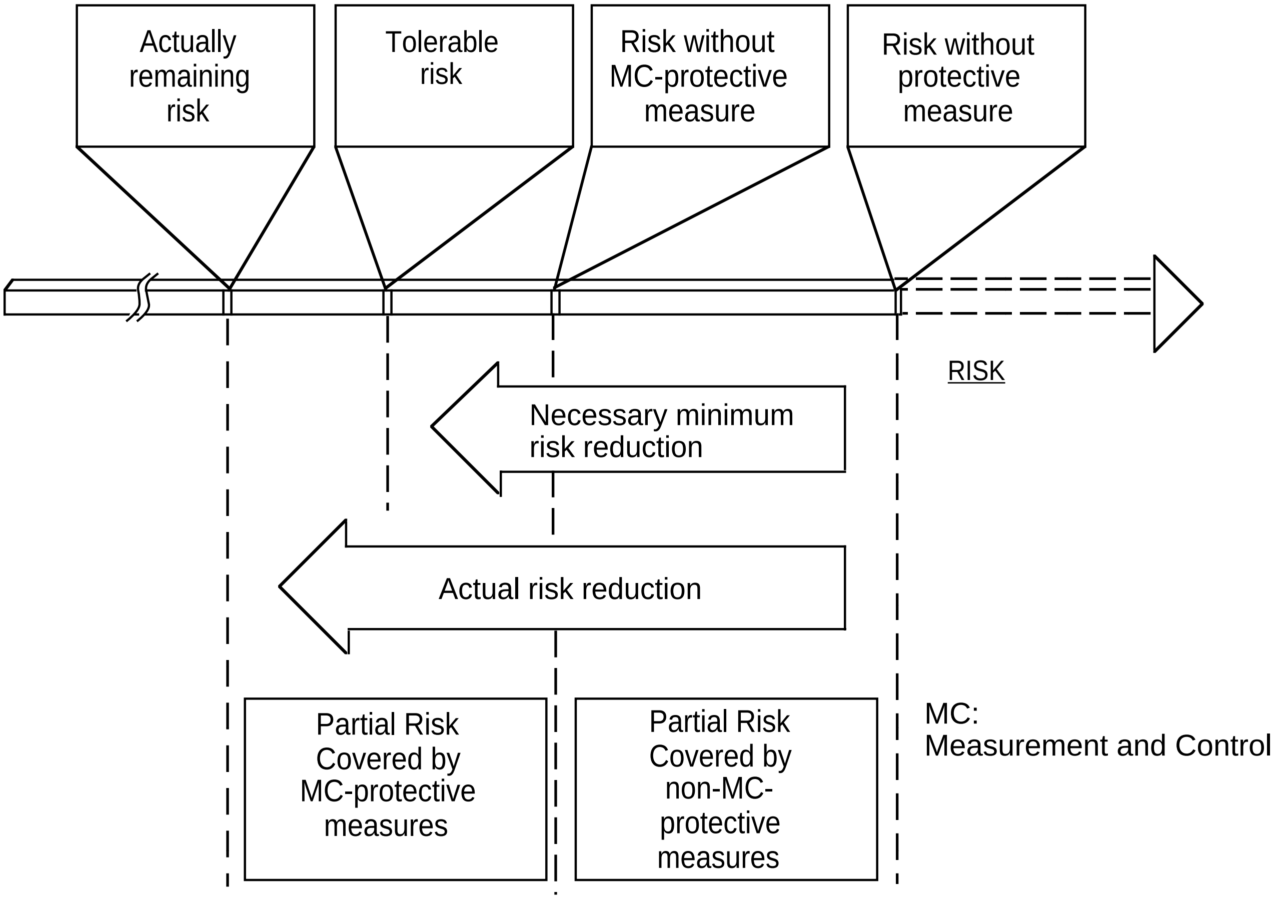
Introduction

Today there are a many technical systems and applications where the proper and safety function of measurement and process control equipment is essential for the prevention of human injury or death. As an integral part of this equipment, computer based systems (programmable electronic systems, PES) increasingly perform safety functions. The fast development of computer technology has led to too many different applications with programmable electronic systems (PES) in safety related systems.

As a subgroup of all PES one finds programmable logic controllers (PLC) in plants for safety critical applications. Sometimes however there is not enough confidence in the complex hardware and software design of modern PLCs.

Using type approved components, i.e. TUV approved PLC's, to build large installation control protective systems is not enough. Careful planning and other provisions have to be made to insure proper operation of these components within their designated operation field. During commissioning of an application, proper validation for all components operation as a system must be checked.

One of the aims in using PLCs in a plant is to reduce risk, not to increase it by inappropriate technology. This principle is shown in the DIN 19250 "Fundamental safety aspects to be considered for measurement and control equipment", and in the paper Draft IEC 1508 (former subcommittee 65A), "Functional safety: Safety related systems", part 5: "Guidelines on the application of Part I (of IEC 1508)".

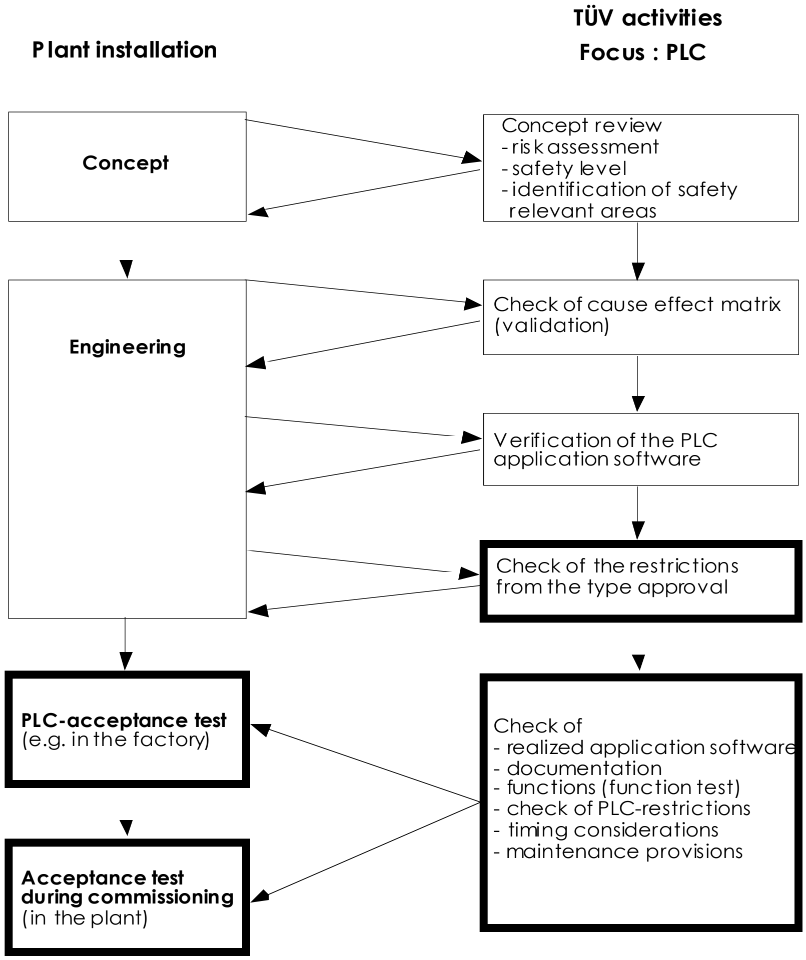

Actually remaining risk
Tolerable risk
Risk without MC-protective measure
Risk without protective measure
RISK
Necessary minimum risk reduction
Actual risk reduction
Partial Risk Covered by MC-protective measures
Partial Risk Covered by non-MC-protective measures
MC:
Measurement and Control

Risk reduction by use of protective measures

The TÜV checks the design, hardware and the operating software of PLCs within a type approval. This gives confidence in the PLC itself for the end user.

Before a PLC is set to work in the plant however other steps are necessary to ensure the PLC provides additional safety to reduce risk to an acceptable level as required by the specific application. This is depicted in the following diagram.

On the left-hand side all sequential activities, necessary from concept level to the acceptance test in the plant, are shown. On the right hand side the corresponding TÜV activities are shown. As one can imagine, these activities need interdisciplinary knowledge.


Plant installation
TÜV activities
Focus : PLC
Concept
Concept review
- risk assessment
- safety level
- identification of safety relevant areas
Engineering
Check of cause effect matrix (validation)
Verification of the PLC application software
Check of the restrictions from the type approval
PLC-acceptance test (e.g. in the factory)
Acceptance test during commissioning (in the plant)
Check of
- realized application software
- documentation
- functions (function test)
- check of PLC-restrictions
- timing considerations
- maintenance provisions

Commissioning of a type approved PLC

Differences between ESD and Continuous Control Systems

There are significant differences between Emergency Shutdown (ESD) Systems and Continuous Control Systems.

A typical ESD system is designed in such ways, that zero or de-energised is the safe state. From the safety point of view therefore availability considerations are not needed. As soon as faults, which can not be handled, are encountered, the system shuts down the application. A burner control system demands an ESD system, which closes the relevant valves in the event of errors. On the other hand, by system design one application can be subdivided in logical groups, which could do a partial shutdown, as long as the main controllers work. A typical example would be a large vessel with many groups of burners.

Most fire and gas applications are typical Continuous Control Systems. If a fire control system detects failures within the system, an alarm must be generated. Shutting down the system is not allowed and would not increase the safety. In the event of a fire it must be possible to activate the relevant fire extinguisher. For Continuous Control Systems high safety and high availability is required. Normally this is implemented by using more redundancy than would be needed for a specific level of safety.

PLC restrictions as a result of a type approval

A programmable logic controller (PLC) is a general-purpose device, which may be, used anywhere in a plant. It may be used it for measuring and controlling and it also may be used in areas, where the safety of the whole plant is involved.

As most PLCs are not designed exclusively for safety applications, restrictions must be compiled for PLCs used in a safety critical environment. As there is a manifold of PLC technology on the market, each PLC has its own, specific restrictions. The restrictions are compiled as a result of a type approval of the PLC. These restrictions must be followed to ensure the whole system complies with safety standards.

PLC vendors publish the TÜV restrictions within their user documentation. This ensures, that everyone knows about the restrictions for the use of a PLC in safety critical applications. TÜV is working on a paper, where the overall valid restrictions are combined regardless of the PLC brand. This has already been done on the restrictions for maintenance override in safety relevant PLCs. See also the paper "Maintenance Override", which is attached.

Representative restrictions

While the restriction:

"Disabling diagnostic on safety relevant modules is not allowed"

is obvious, the following restriction resulted from experience in the field:

"The PLC may be run with disabled points only during the commissioning phase. Before final operation it must be checked, that no points are left disabled".

It is possible to disable a physically connected device logically from the PLC, e.g. for test and maintenance reasons. The "normal" disabling feature of a PLC does this, and as a result, there is a high chance that enabling the points will be forgotten. Therefore simply "forcing" inputs or outputs for maintenance and repair is forbidden. How this task can be carried out is shown in the appendix "Maintenance override", which is attached.

Commissioning and Acceptance Test

Commissioning means bringing the PLC-system, other control-equipment and the process into interaction. It is TÜV-philosophy to do accompanying consulting and acceptance testing throughout construction and commissioning. Knowing that the plant constructor is sometimes more concerned with meeting the time schedule this is recommendable. Working under this pressure the constructors' main interest is not safety and reliability. From our point of view it is less the function of the system, which has priority, more than for the commissioning and construction engineer. We have to focus our attention on the restrictions given by the government and technical rules, which have to be fulfilled in order ensure safety and reliable operation throughout the lifetime of the plant. This ensures early detection of construction, design or installation errors and can therefore be easily corrected. Commissioning and acceptance engineers must work closely together at the same time maintaining their independence. This ensures that the time schedule is met while considering all aspects.

The use of PLCs in safety related systems require special measures throughout the whole lifecycle of the plant. The following typical factors must be considered when using a PLC in a safety related system:

- Personnel
- Controlled equipment and related processes
- Environment
- Controlling equipment, e.g. PLCs and associated equipment
- Wiring (flammability, insulation temperature, survival of function for defined time)
- Installation requirements

Therefore before commissioning, the commissioning engineer normally expects the following to be carried out:

- Validation of safety requirements according to the safety analysis and the subsequent cause-effect-diagram.
- Verification of the logic diagram and its conversion into the application software. From the point of view of safety a quality control plan is needed for the user software in order to help ensure thorough examination. Besides the testing of software by the authors and the users, independent testing and evaluation is highly recommended.
- Pre-installation simulation in the factory of the PLC with a complete function test of the I/O level.

  In the event of a complex system a process simulator is required. Among others the following characteristics are tested:

  - response time,
  - behaviour of the system during PLC power failure, emergency stop and run mode change.

- Software-testing, including simulation of expected error conditions (communication lines, operator mistakes, etc.).

The testing of the PLC-system is the next step and includes the following:

1. **Testing of installation** by using an installation report. This test must be carried out extensively and concerns all relevant safety aspects. These are:

   - **Field wiring,** e.g. separate installation of redundant wiring and function survival of very essential cables.
   - **Protective and functional earthing,** E.g. appliance of the correct functional earthing techniques to get a proper PLC function. Earthing of signal cable shield where the maximum capacity is located.
   - **Noise and transient suppression measures of noise coupling**

     - Correct length of wiring,
     - Separation of the cables for inputs, outputs and power circuits, routing
     - Mains live conductors (spacing of 10 cm or more from signal cables)
     - Separation of the field wiring from internal I/0 cabling and from bus lines
     - Use of twisted pair and/or shielded cables with low inductance cable shield
     - Filtering of I/0 cables presumed to be sensitive to electrical noise
     - Special attention where mechanical contacts are in series with inductive loads in DC circuits

2. **Compliance** with the current **service and environmental conditions**, e.g. temperature, contaminants shock and vibration, electromagnetic influence and sensitivity to lightning.

3. **Successive set up and checks**

The set up of the PLC system is carried out in steps.
One of the most important things during commissioning and testing is the check of the I/0. In these steps the right interaction between PLC system and process periphery will be verified (loop checks).

The criteria are:

Binary inputs: Checking binary and digital input signals to ensure that physical states of sensors comply with signal latches in PLC.

Analogue inputs: Checking analogue input signals to ensure agreement of physical value and data received by PLC.

Binary outputs: Ability to switch, checking that no forced binary and digital outputs are set.

Analogue outputs: Functionality

Supervised inputs and outputs: Detection of opens and shorts

4. System function tests and fault simulation

The commissioning functionality checks of PLC, process and other control equipment must be performed according to a commissioning test plan. This test plan must also include different modes of operation of the PLC:

- Local mode
- Remote operation with DCS interaction
- Maintenance

In this context special care has to be taken concerning restrictions written in the type approval for the PLC system.

The fault simulation is usually performed after system functional tests. For this test a list of faults must be generated. Experience shows that most of the faults occur at the I/0 and other interfaces to the PLC. Therefore this list must include failure modes of:

- Sensors, contacts and actuators
- Inputs and outputs
- Field wiring e.g. exchanged connections
- Fuses and circuit breakers
- Interruption of mains
- Guards and related motion detection (false alarm or failed alarm)
- Interlocks

The simulation must verify that an identified fault causes an output to go into a pre-defined state, as the system operation requires.

Conclusion

Special attention must be paid to the commissioning of PLCs, which are used in safety critical applications. In addition to electrical aspects architectural features of a PLC also have to be considered. **The items, which have to be looked at, are pointed out in the user documentation and in the chapter “restrictions“ in the report of the type approval of the specific PLC.**

References

IEC 1131	Programmable Controllers - Part 4 : User Guidelines
Draft **IEC 1508** Part 1 to 7	Functional safety of programmable electronic systems (PES)
DIN V 19250	Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen Measurement and Control Fundamental Safety Aspects to be considered for Measurement and Control Equipment
DIN V VDE 0801	Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben Principles for Computers in Safety Related Systems
VDI VDE 2180	Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Meß-, Steuerungs- und Regeltechnik.

Contact

TÜV Rheinland Sicherheit und Umweltschutz GmbH (ISEB)
Am Grauen Stein
D-51105 Cologne
Germany
Ekkehard Pofahl + 49-221-806-2981
Fax: + 49-221-806-1736
Email: Ekkehard_Pofahl@compuserve.com

Maintenance Override

Abstract

Suggestions are made about the use of maintenance override of safety relevant sensors and actuators. Ways are shown to overcome the safety problems and the inconvenience of hardwired solutions. A checklist is given.

Maintenance Override

There are basically two methods used now to check safety relevant peripherals connected to PLC's :

- Special switches connected to inputs of the PLC. These inputs are used to deactivate actuators and sensors under maintenance. The maintenance condition is handled as part of the application program of the PLC.

- During maintenance sensors and actuators are electrically switched off of the PLC and checked manually by special measures.

In some cases, e.g. where space is limited, there is the wish to integrate the maintenance console to the operator display, or to have the maintenance covered by other strategies. This introduces the third alternative for maintanence override :

- Maintenance overrides caused by serial communication to the PLC.

This possibilty has to be handled with care and is introduced in this paper.

Maintenance Override Procedures

Connecting to PLC via serial lines is possible in mainly two ways:

A. The serial link is done via the MODBUS RTU protocol or other approved serial protocols. The maintenance override may not be performed by the engineering workstation or programming environment.

B. The engineering workstation or programming environment is allowed to be connected to the PLC to perform maintenance override. That requires additional safety measures inside the associated PLC to prevent a program change during maintenance intervals. These measures shall be approved, e. g. by TÜV.

The following table shows common requirements. The differences between solution A and B are shown by typeface italic.

Requirements for maintenance override handling	**Responsibility**
Already during the software configuration of the PLC system it is determined in a table or in the application program, whether the signal is allowed to be overridden.	Project engineer and commissioner responsible for correct configuration
The configuration may also specify by a table, whether simultaneous overriding in independent parts of the application is acceptable.	*A: Project engineer* *B: Project engineer, Type approval*
Maintenance overrides are enabled for the whole PLC or a subsystem (process unit) by the DCS or a hard-wired switch (e.g. key switch).	Operator or Maintenance engineer *B: Type approval*
A: The override is activated via DCS. *B: The maintenance engineer activates the override via the programming environment.* As an organisational measure the operator should confirm the override condition.	*A: Operator, Maintenance engineer* *B: Type approval, Maintenance engineer*
Direct overrides on inputs and outputs are not allowed. Overrides have to be checked and to be implemented in relation to the application. Multiple overrides in a PLC are allowed as long as only one override is used in a given safety related group. The alarm shall not be overridden..	*A: Project engineer* *B: Project engineer, Type approval*
The PLC alerts the operator, e. g. via the DCS, indicating the override condition. The operator will be warned until the override is removed.	Project engineer, Commissioner
A: The override is removed via DCS. *B: The maintenance engineer removes the override via the programming environment.*	*A: Operator, Maintenance engineer* *B: Maintenance engineer*
A: There should be a second way to remove the maintenance override condition. *B: If urgent, the maintenance engineer can remove the override by the hard-wired switch.*	*A: Project engineer* *B:Maintenance engineer, Type approval*
During the time of override proper operational measures have to be implemented. The time span for overriding shall be limited to one shift (typically not longer than 8 hours), or hard-wired common maintenance override switch (MOS) lamps shall be provided on the operator console (one per PLC or per process unit).	Project engineer, Commissioner, DCS program, PLC program

Recommendations

The following recommendations are given to improve the primary safety as described by the list:

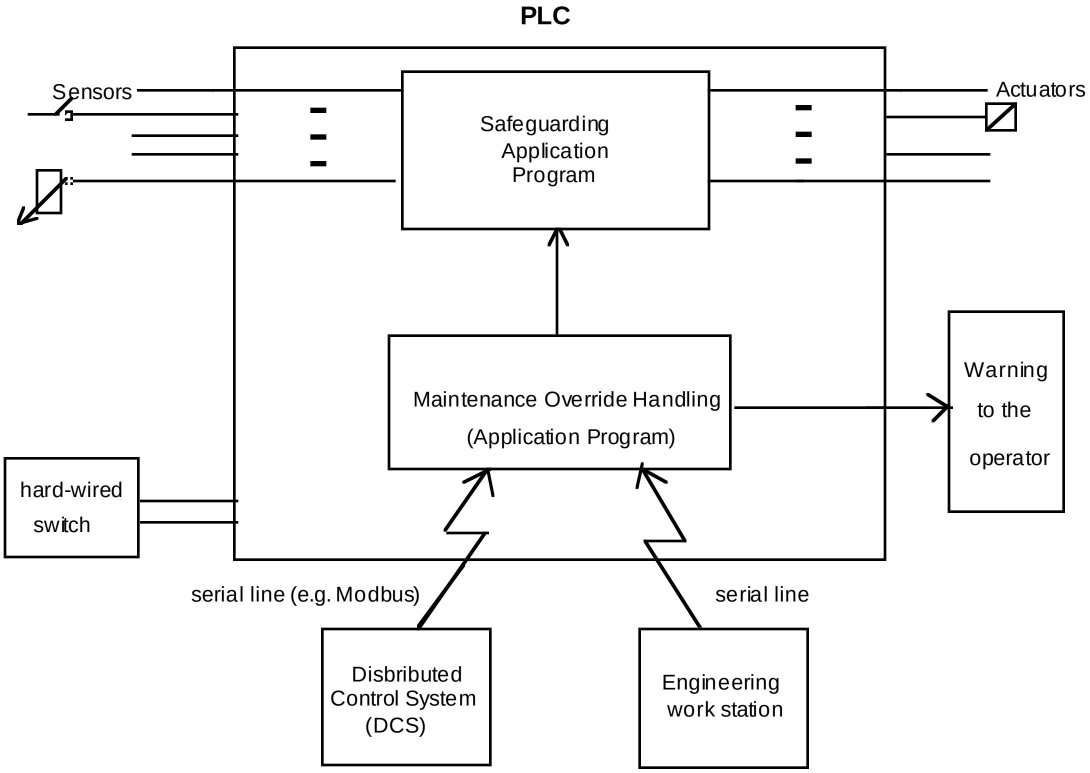
=> A program in the DCS that checks regularly that no discrepancies exist between the override command signals from the DCS and the override activated signals received by the DCS from the PLC.

=> The use of the maintenance override function should be documented on the DCS and on the programming environment if connected. The print-out should include:

- time stamp of begin and end
- ID of the person who is activating the maintenance override — maintenance engineer or operator (if the information cannot be printed, it should be entered in the work-permit)
- tag name of the signal being overridden

=> The communication packages different from a type-approved MODBUS should include CRC, address check and check of the communication time frame.

=> Lost communication should lead to a warning to the operator and maintenance engineer. After loss of communcation a time delayed removal of the override should occur after a warning to the operator.


PLC
Sensors
Actuators
Safeguarding Application Program
Maintenance Override Handling (Application Program)
Warning to the operator
hard-wired switch
serial line (e.g. Modbus)
serial line
Disbributed Control System (DCS)
Engineering work station