



Wartungseingriffe Maintenance Override

Version 2.2, 08. September 1994

TÜV Rheinland
Anlagentechnik
Automation, Software,
Informationstechnologie
Am Grauen Stein
D-51105 Köln
Telefon +49 (221) 806-1790
Telefax +49 (221) 806-1736
Email pofahl@tuv.com

TÜV Bayern
Institut für Qualität und Sicherheit
in der Elektronik (IQSE)

Westendstraße 199
D-80686 München
Telefon +49 (89) 5791-1842
Telefax +49 (89) 5791-1396

Wartungseingriffe

Übersicht

In diesem Papier werden Vorgehensweisen für Wartungseingriffe im Bereich sicherheitsrelevanter Geber und Stellglieder vorgeschlagen. Daneben werden auch Vorschläge gemacht, die Sicherheitsprobleme und die Unannehmlichkeiten der festverdrahteten Lösungen zu bewältigen. Ferner ist eine Checkliste aufgeführt.

Wartungseingriffe

Es gibt zwei Grundmethoden zur Überprüfung der an die SPS angeschlossenen sicherheitsrelevanten Peripherie:

- Spezielle Schalter sind mit Eingängen der SPS verbunden. Diese Eingänge werden genutzt um Stellglieder und Geber im Wartungsbetrieb abzuschalten. Die Wartungsvoraussetzungen sind ein Teil des Anwenderprogramms der SPS.
- Während des Wartungsbetriebs werden Geber und Stellglieder von der SPS spannungsfrei getrennt und manuell mit besonderen Maßnahmen überprüft.

In einigen Fällen ist es wünschenswert (z.B. dort, wo das Platzangebot begrenzt ist) die Wartungskonsole in die Bedienanzeige zu integrieren oder die Wartung durch andere Strategien abzudecken, dies bedingt die 3. Alternative für Wartungseingriffe:

- Wartungseingriffe durch serielle Kommunikation mit der SPS.

Diese Möglichkeit ist mit Sorgfalt zu handhaben und wird im folgenden vorgestellt.

Verfahren für Wartungseingriffe

Die Anbindung an die SPS über serielle Schnittstellen ist hauptsächlich auf 2 Arten möglich:

- A Die serielle Kopplung wird mit Hilfe des MODBUS-RTU Protokolls oder anderer zugelassener Protokolle ausgeführt. Die Wartungseingriffe dürfen nicht durch SPS-Entwicklungssysteme ausgeführt werden.
- B Der Anschluß von SPS-Entwicklungssystemen an die SPS zur Ausführung von Wartungsarbeiten ist erlaubt. Dies erfordert zusätzlich Sicherheitsmaßnahmen in der betreffenden SPS zur Verhinderung von Programmänderungen während des Wartungsintervalls. Diese Maßnahmen sollen durch die Baumusterprüfung (z. B. durch den TÜV) abgesichert werden.

Die folgende Tabelle zeigt die allgemeinen Anforderungen. Die Unterschiede zwischen den Lösungen A und B sind in kursiver Schrift dargestellt.

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 maintenance override :

- Maintenance overrides caused by serial communication to the PLC.

This possibility 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.

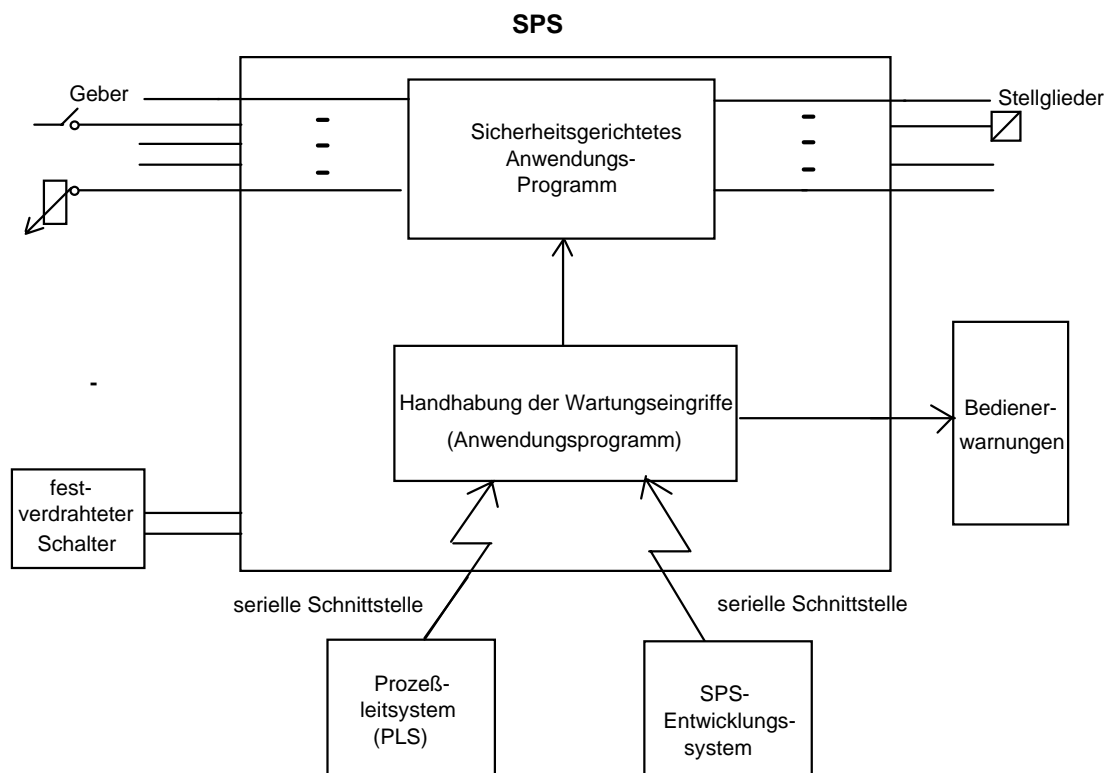
Anforderungen an die Ausführung der Wartungseingriffe	Verantwortung
Schon während der Softwarekonfiguration der SPS ist in einer Tabelle oder in dem Anwenderprogramm zu entscheiden, ob das Signal überschrieben werden darf.	Projektingenieur und Inbetriebnahmeperson sind für die korrekte Konfiguration verantwortlich.
Die Konfiguration muß in einer Tabelle aufzeigen, ob ein gleichzeitiges Eingreifen in unabhängige Teile der Anwendung erlaubt ist.	<i>A: Projektingenieur</i> <i>B: Projektingenieur, Baumusterprüfung</i>
Wartungseingriffe werden für die komplette SPS oder ein Teilsystem (Prozeßteil) durch das Prozeßleitsystem (PLS) oder einen festverdrahteten Schalter freigegeben (z.B. Schlüsselschalter) .	Bediener, Wartungsingenieur <i>B: Baumusterprüfung</i>
<i>A: Eingriffe werden durch das PLS aktiviert.</i> <i>B: Wartungsingenieur aktiviert den Eingriff über ein SPS-Entwicklungssystem.</i> Der Bediener sollte die Eingriffsvoraussetzungen aus organisatorischen Gründen bestätigen.	<i>A: Bediener, Wartungsingenieur</i> <i>B: Baumusterprüfung, Wartungsingenieur</i>
Direkte Eingriffe auf Ein- und Ausgänge sind nicht erlaubt. Eingriffe sind in Verbindung mit der Anwendung zu überprüfen und durchzuführen. Mehrere Eingriffe in einer SPS sind erlaubt, solange nur ein Eingriff in einer sicherheitsrelevanten Gruppe ausgeführt wird. Der Alarm soll nicht überschrieben werden.	<i>A: Projektingenieur</i> <i>B: Projektingenieur, Inbetriebnahmeperson</i>
Die SPS alarmiert den Bediener (z.B. über PLS) durch Anzeige der Eingriffe. Der Bediener wird gewarnt bis alle Eingriffe zurückgesetzt worden sind.	Projektingenieur, Inbetriebnahmeperson
<i>A: Die Eingriffe werden durch PLS zurückgesetzt.</i> <i>B: Der Wartungsingenieur setzt die Eingriffe mit Hilfe des SPS-Entwicklungssystems zurück.</i>	<i>A: Bediener, Wartungsingenieur</i> <i>B: Wartungsingenieur, Baumusterprüfung</i>
<i>A: Es sollte einen zweiten Weg für die Zurücknahme der Wartungseingriffe geben.</i> <i>B: Sofern erforderlich, kann der Wartungsingenieur mit einem festverdrahteten Schalter den Wartungseingriff zurücksetzen.</i>	<i>A: Projektingenieur</i> <i>B: Wartungsingenieur, Baumusterprüfung</i>
Während der Zeit der Eingriffe sind geeignete betriebliche Maßnahmen zu treffen. Die Zeitspanne für Eingriffe sollte auf eine Arbeitsschicht begrenzt sein (normalerweise nicht länger als 8 Stunden) oder an der Bedienerkonsole sind festverdrahtete Anzeigen (eine pro SPS oder pro Prozeßteil) für den Wartungseingriff vorgesehen.	Projektingenieur, Inbetriebnahmeperson, PLS-Programm, SPS-Programm

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.	<i>A: Project engineer</i> <i>B: Project engineer, Type approval</i>
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 <i>B: Type approval</i>
<i>A: The override is activated via DCS.</i> <i>B: The maintenance engineer activates the override via the programming environment.</i> As an organisational measure the operator should confirm the override condition.	<i>A: Operator, Maintenance engineer</i> <i>B: Type approval, Maintenance engineer</i>
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.	<i>A: Project engineer</i> <i>B: Project engineer, Type approval</i>
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
<i>A: The override is removed via DCS.</i> <i>B: The maintenance engineer removes the override via the programming environment.</i>	<i>A: Operator, Maintenance engineer</i> <i>B: Maintenance engineer</i>
<i>A: There should be a second way to remove the maintenance override condition.</i> <i>B: If urgent, the maintenance engineer can remove the override by the hard-wired switch.</i>	<i>A: Project engineer</i> <i>B: Maintenance engineer, Type approval</i>
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

Empfehlungen

Die folgenden Empfehlungen sollen die Sicherheit bei Wartungseingriffen erhöhen.

- => Ein Programm des Prozeßleitsystems (PLS) überwacht kontinuierlich die Übereinstimmung der Eingriffe durch das PLS mit den von der SPS mitgeteilten Eingriffen.
- => Die Wartungseingriffe sollten durch das PLS und das SPS-Entwicklungssystem dokumentiert werden. Der Ausdruck sollte beinhalten:
 - Zeitstempel über Anfang und Ende des Wartungseingriffes
 - Identifikation der Person, die den Wartungseingriff aktiviert - Wartungsingenieur oder Bediener (falls die Information nicht ausgedruckt werden kann, sollte sie im Arbeitsauftrag enthalten sein)
 - Bezeichnung des beeinflussten Signals
- => Kommunikationspakete, unterschiedlich von typgeprüften MODBUS-Protokollen, sollten mit CRC-Prüfsumme, Adressprüfung und einer Überprüfung der Kommunikationszeit verbunden sein.
- => Kommunikationsstörungen sollten zu einer Warnung für den Bediener und den Wartungsingenieur führen. Nach einer Warnung sollte der Wartungseingriff zeitverzögert aufgehoben werden.



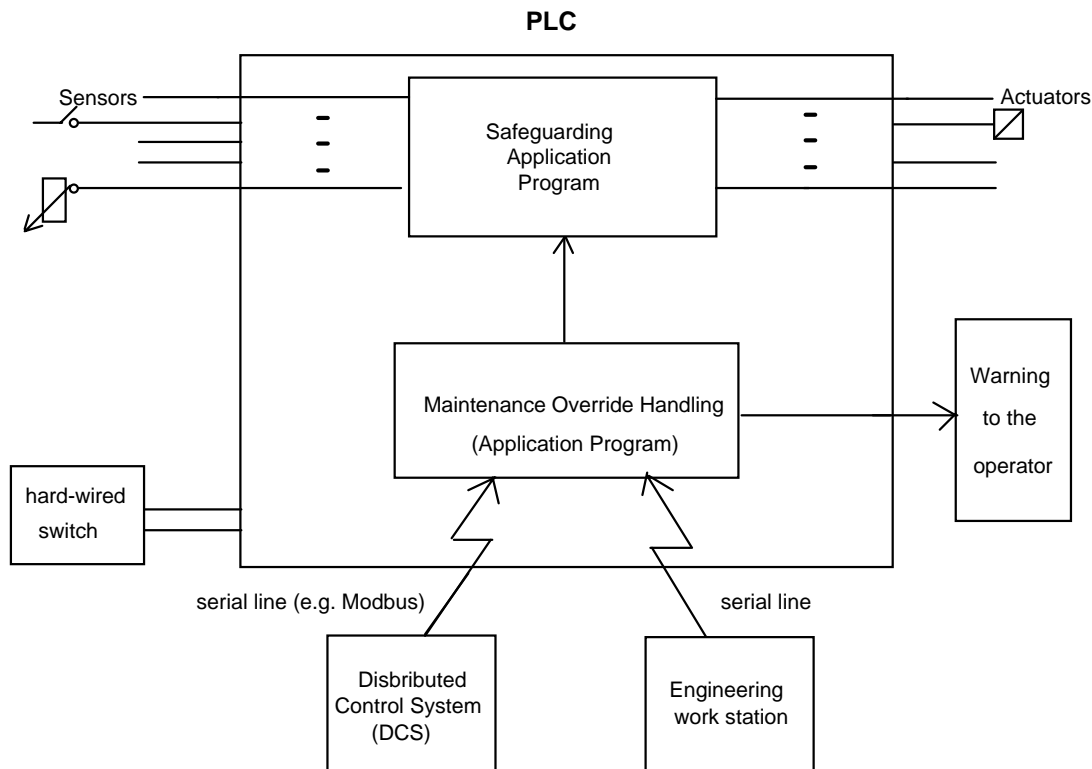
Ausgabestand

Diese Version 2.2 ersetzt die Version 2.1 vom 24. Juni 1994.

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 communication a time delayed removal of the override should occur after a warning to the operator.



Version history

This version 2.2 supersedes the version 2.1 from 24. June 1994.