

Zweiter Teil des Leitfadens zur Fehlersuche in Profibus-Netzwerken

Verdruss mit Profibus? (Teil 2)

Der Einsatz des Bussystems ist denkbar einfach, da die Kommunikation vollautomatisch zwischen den Geräten abläuft. Aufeinander abgestimmte Mechanismen zur Fehlervermeidung und -behandlung sorgen für zuverlässige Übertragung. Werkzeuge zur automatischen Konfiguration des Datenaustausches machen Detailkenntnisse des Protokolls überflüssig und helfen, Zeit und Kosten zu sparen. Dennoch treten in einzelnen Netzwerken mitunter Kommunikationsstörungen auf, deren Ursachen oft einfacher Art sind, die aber nicht mit Bordmitteln behoben werden können. Auf Grund der umfassenden Tool-Unterstützung während der Projektierung fehlt oft das Bewusstsein für grundlegende Zusammenhänge innerhalb von Profibus. Hier hilft die Fortsetzung des Leitfadens zur Fehlersuche aus unserer März-Ausgabe.

PRAXIS PLUS

- Statische Kommunikationsprobleme in Profibus-Netzwerken lassen sich mit dem Softing Analyzer mobil sehr einfach untersuchen, der physikalisch rückwirkungsfrei über ein Profiprobe-Kabel angeschlossen wird und ohne eigene Stationsadresse den Verkehr aller Stationen mit exakten bitzeitgenauen Zeitstempeln mithört.
- Sporadische Kommunikationsprobleme lassen sich z.B. über eine geeignete „Watchdogzeit“ in den Griff bekommen, die erfahrungsgemäß bei mindestens 125% der Datenzykluszeit bzw. in Netzen, bei denen zeitweise weitere Master z.B. als Parametriergeräte aktiv sind, über der Sollumlaufzeit liegen sollte.

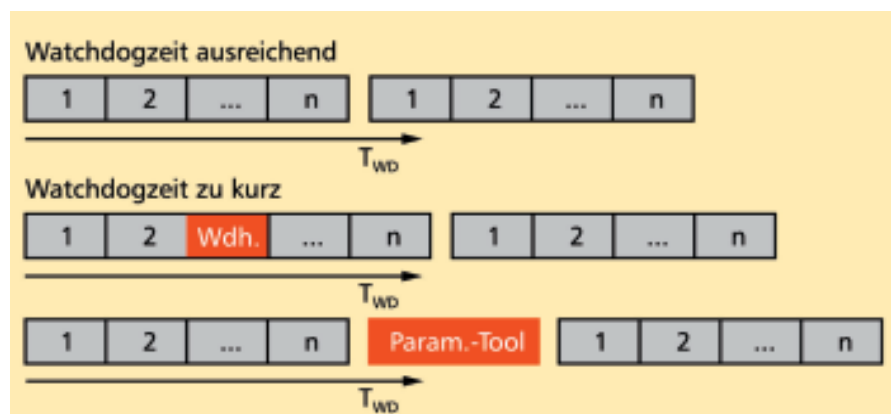


Bild 1: Kommunikationszyklus bei Profibus: Die erste Zeile zeigt den Standardablauf der Kommunikation; die Zeilen darunter illustrieren die Auswirkungen von Verzögerungen auf Grund von Telegrammwiederholungen oder zusätzlichen Teilnehmern. Wird die Überwachungszeit nicht angepasst, kann es zu Unterbrechungen der Kommunikation kommen

Tritt eine Störung auf, muss diese schnell behoben werden, um die Folgekosten durch Produktionsausfall klein zu halten. Häufig will man mittels „Versuch und Irrtum“ Abhilfe schaffen. Die unüberlegte Anpassung von Einstellungen vermag die Situation zwar eventuell kurzfristig zu entspannen, sie kann aber auch zur Folge haben, dass Fehlerbehandlungsmechanismen von

Profibus nicht mehr oder zum falschen Zeitpunkt wirksam werden. So steht die Produktion nach kurzer Zeit erneut still. Mit grundlegenden Kenntnissen und geeigneten Werkzeugen lässt sich der oft unnötige Austausch von Geräten vermeiden. Im Vorfeld eingesetzt, wird es möglich, die Kommunikation für den jeweiligen Anwendungsfall robust auszulegen und die Ursachen potenzieller Störungen zu eliminieren.

DER AUTOR



Dipl.-Ing. Harald Wenke ist Leiter Technischer Support der Softing AG in Haar und berät Anwender u.a. beim optimalen Einsatz von Feldbussen

Woher kommen die Störungen?

Die Quellen für Kommunikationsprobleme lassen sich grob in zwei Kategorien einteilen: Störungen auf Grund von Umwelteinflüssen

und Störungen durch ungeeignet gewählte Kommunikationsparameter. Erstere wurden bereits in Teil 1 des Leitfadens vorgestellt (eA 3/2004, S. 60); auf die verbleibenden wird nachfolgend eingegangen. Abhängig vom zeitlichen Verlauf lassen sich Kommunikationsprobleme unterschiedlichen Typen von Störungen zuordnen:

- Fall 1: Die Kommunikation zu einzelnen Stationen ist dauernd gestört. Dies deutet auf Fehler in der Projektierung der Stationen hin.
- Fall 2: Die Störung tritt nur zeitlich unregelmäßig auf, die Kommunikation fällt zeitweise aus, eine eindeutige Zuordnung zu Stationen ist nicht möglich. In diesem Fall sollte die Timing-Situation im Netzwerk untersucht werden. Im Hinblick auf die Untersuchungsrichtung ist von Interesse, ob die Anzahl der Stationen am Bus gleich bleibt oder die Störung mit dem Hinzufügen bzw. Entfernen eines Teilnehmers einhergeht. Grundlage der Untersuchungen bildet in jedem Fall eine mit Zeitinformation versehene Aufzeichnung des Busverkehrs. Diese kann z.B. mit dem Softing Analyzer mobil sehr einfach erstellt werden. Physikalisch rückwirkungsfrei über ein Profiprobe-Kabel angeschlossen, hört der Analyzer ohne eigene Stationsadresse den Verkehr aller Stationen mit und speichert die aufgezeichneten Botschaften mit exakten bitzeitgenauen Zeitstempeln.

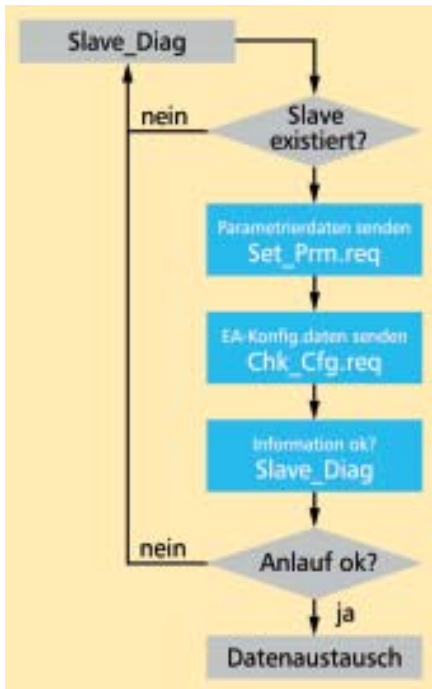


Bild 2: Anlauf der Profibus-Kommunikation zu einem Slave: Ist die empfangene Projektierungsinformation korrekt, geht der Slave zum Datenaustausch über, andernfalls bleibt er im Anlaufzustand

Parametrierungs- und Konfigurationsfehler

Die Kommunikation zwischen Master und Slave in einem DP-Netzwerk läuft zyklisch ab, d.h. je Slave sendet der Master Ausgangsdaten und der Slave antwortet unmittelbar mit Eingangsdaten. Wurde die letzte Station bedient, schließt sich ein neuer Zyklus an (Bild 1, erste Zeile). Um schnellen Datenaustausch zu gewährleisten, finden während der Übertragung nur die notwendigsten Überprüfungen statt. Der Typ des Slaves und die angeschlossenen Module werden dem Datenaustausch vorgelagert während des Anlaufs geprüft. Die entscheidenden Botschaften sind in Diagnose-, Parametrier- und Konfigurationstelegrammen enthalten (Bild 2). Mit dem Diagnosetelegramm wird zunächst geprüft, ob unter der im Master definierten Adresse ein DP-Slave am Bus angeschlossen ist. Wird keine Antwort empfangen, erhält die Steuerung eine Diagnosemeldung „Station_non_existent“. Mögliche Ursache kann eine falsch eingestellte Stationsadresse des Slave (am Gerät selbst oder in der Steuerung) sein. Welche Slavestationen am Bus vorhanden sind, zeigt die „Live List“ des Busmonitors. Anwendungsorientierte Stationsnamen erlauben einen schnellen Vergleich von Soll- und Ist-Struktur des Busses. Ist der Slave erreichbar, aber kein Datenaustausch möglich, liefert das Diagnosetele-

gramm weitere Hinweise auf mögliche Fehlerursachen. Fehlercodes wie „Prm_Fault“ oder „Cfg_Fault“, deuten auf Unstimmigkeiten bei Parametrierung oder Prüfung der Konfiguration hin. Im Parametriertelegramm wird z.B. der Gerätetyp anhand der „Ident_Number“ abgefragt. Schickt der Master im Parametriertelegramm einen Code, der von dem im Slave gespeicherten abweicht, ist keine Kommunikation möglich, da dann projektierte und montierter Slavetyp nicht identisch sind. Die im Slave gespeicherte Nummer ist im Diagnosetelegramm enthalten. Die Klartextdecodierung des Analyzers erlaubt einen unmittelbaren Vergleich ohne Verwendung zusätzlicher Hilfsmittel (Bild 3). Abhilfe kann so direkt durch Änderung der Projektierung oder Austausch des Feldgeräts geschaffen werden. Auf ein ganz ähnliches Problem deutet die Meldung „Cfg_Fault“ im Diagnosetelegramm hin: Beim Anlauf überprüft der Master ebenfalls, ob der im Master projektierte Aufbau mit dem des montierten Slave identisch ist. Basis ist eine codierte Darstellung der Module, die in der Steuerung hinterlegt wird. Beim Einschalten ermittelt der Slave im Selbsttest die tatsächlich gesteckten Module. Während des Hochlaufs werden die beiden Codes verglichen. Bei Abweichungen wird der Datenaustausch mit dem Diagnosecode „Cfg_Fault“ (Konfigurationsfehler) unterbunden, weil projektierte und montierte Module nicht übereinstimmen und so eine einwandfreie Funktion nicht gewährleistet ist. Abhilfe wird durch eine Anpassung der Projektierung oder des montierten Geräts geschaffen.

Timing ist alles – sporadische Fehler vermeiden

Neben den beschriebenen statischen Kommunikationsproblemen treten häufig Schwierigkeiten auf, die nur kurz wirksam sind. Dennoch reichen sie aus, um die Steuerung aus dem Tritt zu bringen. Sie äußern sich darin, dass der Datenaustausch zu den Slaves scheinbar ohne erkennbaren Grund plötzlich abbricht, dann aber fortgesetzt wird. Je nach Einstellung der Steuerung geht diese jedoch in einen steuerungsspezifischen Fehlerzustand, auch wenn der Bus längst wieder fehlerfrei läuft. Nach Quittierung des Fehlers funktioniert dann alles wieder normal. Eine besondere Rolle spielt hier die Ansprechüberwachung im DP-Slave. Mit dem „Watchdog-Timer“

überwacht der Slave, ob er innerhalb einer gewissen Zeitspanne („Watchdogtime“, T_{WD}) mindestens einmal vom Master angesprochen wird (Bild 1). Ist dies nicht der Fall, bringt der Slave seine Ausgänge in den Sicherem Zustand und setzt seine Busanschaltung zurück. Zur Fortsetzung der Kommunikation ist dann ein Neuanlauf des Slave erforderlich. Der Wert des Timer bestimmt auch die Abschaltzeit der Slaveausgänge beim Master-Ausfall. Deshalb werden unter Sicherheitsaspekten möglichst kleine Werte bevorzugt. Bei einem zu kleinen Wert ist allerdings keine Kommunikation möglich. Die Slaves kommen über den Anlauf nicht hinaus, sie setzen sich immer wieder selbst zurück. Ist der Wert nicht ausreichend groß, reichen kleine Unregelmäßigkeiten im Kommunikationsablauf aus, um den Timer ansprechen zu lassen.

Welcher kleine Wert ist ausreichend groß?

Um Datenaustausch zu ermöglichen, muss die „Watchdogzeit“ mindestens das Intervall zwischen zwei Datentelegrammen zum selben Slave abdecken. Allerdings führt jetzt jede Verzögerung im Datenaustausch – z.B. auf Grund von Telegrammwiederholungen zur Fehlerbehandlung – zu einer Überschreitung der „Watchdogzeit“. Die positive Wirkung der Fehlerbehandlung muss also durch einen zeitlichen Zuschlag ermöglicht werden. Je größer dieser Zuschlag ist, umso stabiler ist die Kommunikation, desto träger ist aber auch die Reaktion im Fehlerfall (Bild 4). Praxisorientierte Empfehlungen gehen von mindestens 125 % der Datenzykluszeit aus. Ob die Einstellung des Watchdog-Timer auf einen zu geringen Wert Ursache von Kommunikationsproblemen ist bzw. werden kann, lässt sich mittels Analyser sehr einfach bestimmen. Zu achten ist dabei auf eine genaue und zuverlässige Zeitstempelung der Telegramme,

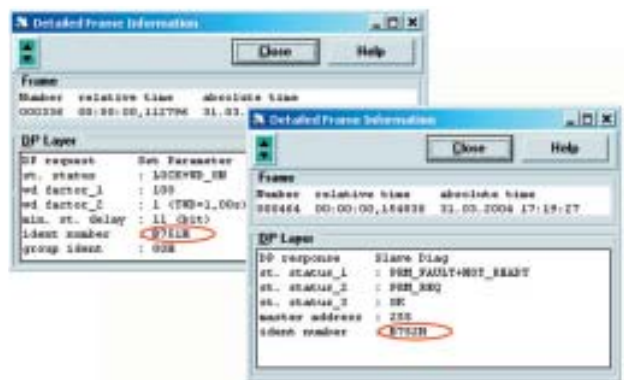


Bild 3: Mittels Busanalyzer lassen sich projektierte und montierter Slave anhand der „Ident_Number“ vergleichen – ohne dass auf Informationen aus der Projektierungs-Software zurückgegriffen werden muss

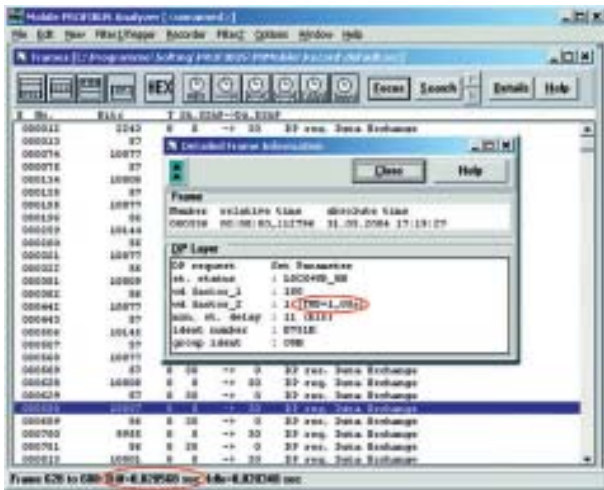


Bild 4: Vergleich der Dauer eines Datenzyklus mit der Watchdog-Zeit: Im Beispiel steht einer Zykluszeit von rund 21 ms ein überdimensionierter Watchdog von 1 s gegenüber; die Kommunikation ist zuverlässig gewährleistet, allerdings wird Reaktionszeit im Fehlerfall verschenkt

um die entsprechenden Intervalle präzise ermitteln zu können. Die Watchdogzeit entnimmt man der Klartextdarstellung des Parametrieretelegramms. Das Intervall zwischen zwei identischen Zugriffen auf einen Slave wird per Mausklick aus den aufgezeichneten Telegrammen bestimmt. Im Fehlerfall helfen Filter und Trigger, die Kommunikationshistorie bis zum Slave-Wiederanlauf aufzuzeichnen. Schließlich kann festgestellt werden, ob T_{WD} überschritten und so der Wiederanlauf ausgelöst wurde.

In Netzwerken, in denen zeitweise weitere Master, z.B. in Form von Parametriergeräten, aktiv sind, muss im Timerwert auch deren Zeitbedarf für Kommunikation berücksichtigt werden. Dieser Aspekt verdient besondere Beachtung, da sich die Projektierung manchmal nur auf die zeitliche Auslegung der Kommunikation Master-Slaves konzentriert und den Tool-Bedarf nicht berücksichtigt. Die Token-Sollumlaufzeit T_{TR} muss in allen Stationen ausreichend hoch eingestellt werden, andernfalls fallen beim Tool-Anschluss entweder Slaves aus oder dem zusätzlichen Master wird ausreichender Zugang zum Bus verwehrt, sodass Parameter weder geschrieben noch gelesen werden können. Für die Watchdogzeit sind hier Werte, die über der Sollumlaufzeit liegen, sinnvoll.

Übung macht den (Profibus-)Meister

Anhand der Beispiele in den beiden Teilen des Leitfadens wird klar, dass auftretende Probleme sehr vielgestaltig sein können. Daher kann ein Leitfaden im vorliegenden Umfang keine Lösung für jedes Problem bieten. Vielmehr soll er für die möglichen Arten von Einfluss sensibilisieren und Einstiegspunkte in

die zielgerichtete Untersuchung aufzeigen.

Bei vielen Notfall-Einsätzen, die das zertifizierte „Profibus Competence Center“ von Softing durchgeführt hat, stellte sich heraus, dass Problemquellen in Anlagen unbewusst „eingebaut“ wurden und nicht auf Unzulänglichkeiten des Protokolls zurückzuführen waren. So werden beispielsweise häufig zu viele Geräte an zu langen Leitungen betrieben. Dies hat mangelhafte Übertragungspegel zur Folge. Ein kleiner zusätzlicher Einfluss reicht aus, um den Datenverkehr zu stören. Ein vorschriftsmäßig eingestellter Bus würde standhalten. Immer wieder stellt sich auch heraus, dass das projektierte Timing manche Geräte überfordert. Diese Situation ist insbesondere bei Netzwerken zu beobachten, die unterschiedliche Übertragungsmedien kombinieren. Der wiederkehrende Ausfall von Anlagenteilen ist die Folge, stets verbunden mit Produktionsausfall. Andererseits sind Betriebsgrößen eines Netzwerks einfach bestimmbar. Viele Probleme können bereits durch das Beachten simpler Beziehungen zwischen wenigen Parametern vermieden werden. Die Erfahrung zeigt jedoch, dass die entsprechenden Kenntnisse noch nicht ausreichend Verbreitung gefunden haben.

Den Profibus-Spezialisten bei Softing zufolge ist die technische Abnahme eines Netzwerks nach der Montage ein zuverlässiger Weg aus dem Dilemma. Nachhaltiger wirkt die Qualifikation von Instandhaltungs-Teams in Troubleshooting-Trainings, wie sie Softing anbietet. Hier erwerben die Teilnehmer kompakte Grundkenntnisse der relevanten Zusammenhänge von Profibus und trainieren die schnelle Behebung von Problemen mittels geeigneter Tools.

eA-INFO-TIPP

*Sollten Sie den ersten Teil des Profibus-Leitfadens von Ulrich Schuster verpasst haben, so können Sie ihn in der März-Ausgabe der elektro Automation ab Seite 60 nachlesen oder unter dem folgenden Link aus dem Fachartikel-Archiv der elektro Automation downloaden:
www.ea-online.de/O/35/Y/82108/VII/30153796/V5/softing/default.aspx*