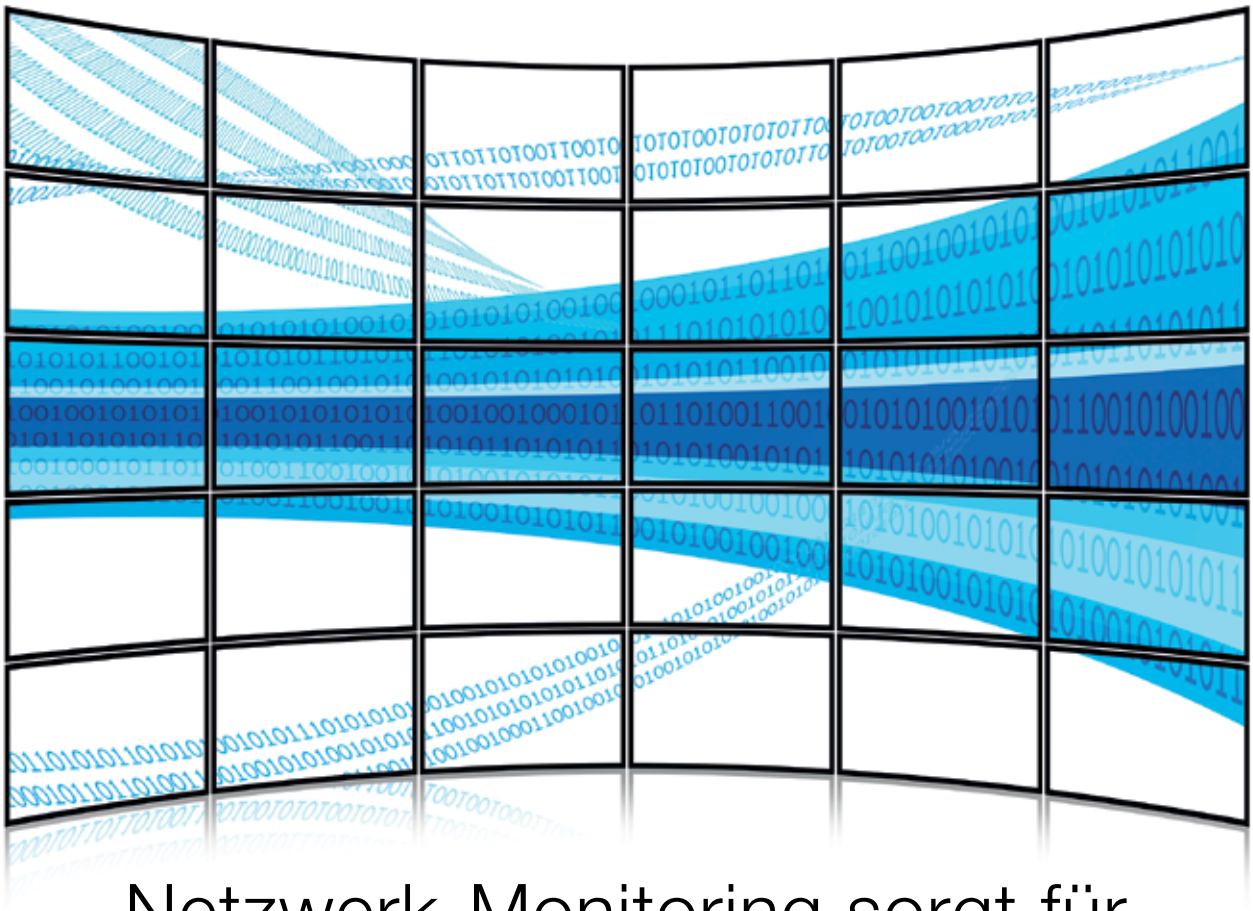

# Netzwerk-Monitoring sorgt für Verfügbarkeit und Sicherheit

„Nur ein stabiles Netzwerk ist ein gutes Netzwerk“ – dieses Credo ist die Grundlage allen instandhalterischen Handelns. Für eine störungsfreie Maschinen- und Anlagenfunktion ist eine permanente Netzwerküberwachung essentiell. Bei diesem Konzept werden historische und aktuelle Daten aus dem Netzwerk analysiert, um die Verfügbarkeit und Sicherheit zu gewährleisten.

**TEXT:** Christian Wiesel, Indu-Sol **BILDER:** iStock, kaan tanman; Indu-Sol

Im Zuge der allseits diskutierten Entwicklung hin zu einer Industrie 4.0 mit steigendem Vernetzungsgrad intelligenter Komponenten und Maschinen werden vermehrt Ethernet-basierte Netzwerke wie Profinet eingesetzt. Daraus ergeben sich einerseits viele neue Freiheiten, beispielsweise hinsichtlich der Netzwerktopologie (z. B. Stern- oder Ringstrukturen) oder der Mischung verschiedener Protokolle (z. B. TCP/IP mit Profinet). Diese bringen andererseits jedoch auch eine zunehmende Komplexität in Aufbau und Diagnose mit sich – die Herausforderungen an die Instandhaltung steigen.

Treten Fehler auf, so sind diese dann oft schwer zu finden und die Fehlersuche wird langwierig, da es zahlreiche Parameter zu überwachen gilt. Aus diesem Grund hat Indu-Sol zum Zwecke einer vorbeugenden, zustandsorientierten Wartung von Profinet- und anderen Netzwerken das Konzept der Permanenten Netzwerküberwachung (PNÜ) entwickelt. Dazu wird das passiv arbeitende Mess- und Diagnosetool Profinet-Inspektor NT zwischen dem Controller und dem ersten Switch beziehungsweise I/O-Device ins Netzwerk eingebunden. Dort überwacht


**Mit dem Profinet-Inspektor NT hat Indu-Sol ein intelligentes, passiv arbeitendes Mess- und Diagnosetool für Profinet-Netzwerke entwickelt. Es analysiert permanent den logischen Datenverkehr und warnt den Betreiber sofort bei ersten Auffälligkeiten.**

es rückwirkungsfrei permanent den logischen Datenverkehr und damit die Einhaltung von Qualitätsparametern der Kommunikation, wie Aktualisierungszeiten, Telegrammjitter oder Fehlertelegramme. Werden vordefinierte Schwellwerte überschritten, alarmiert das Gerät den Betreiber sofort wahlweise über SNMP, E-Mail oder die Web-Oberfläche des Inspektors.

## Zustand in Echtzeit

Die zentrale Netzwerküberwachungssoftware PROmanage NT führt die Daten aller Inspektoren zusammen und bündelt so die jeweiligen Netzwerkzustände zentral auf einem Server. Zudem fragt die Software im Minutentakt die Portstatistiken der managebaren Switche ab. Durch die zentrale Aufbereitung aller Daten können sich Betreiber automatisierter Maschinen und Anlagen jederzeit Informationen über den Zustand ihres Netzwerks auf Knopfdruck anzeigen lassen und Echtzeit-Aussagen über den „Gesundheitszustand" treffen.

Bisher passiert all dies mit dem Ansatz, die Verfügbarkeit des Netzwerks und damit der Maschinen und Anlagen zu gewährleisten. Durch die Warnung bei ersten Auffälligkeiten können nicht nur verschleißbehaftete oder strukturbedingte Störursachen ermittelt werden. Auch das Thema der Netzwerk-Security spielt im Zuge von Industrie 4.0 eine immer größere Rolle. In Ethernet-basierten Netzwerken laufen zyklischer und azyklischer Datenverkehr gleichzeitig ab. Da Maschinen und Komponenten immer intelligenter werden und selbstständig Daten zu Zeitpunkten austauschen, die der eigenen Logik entsprechen und für den Menschen mitunter kaum noch nachvollziehbar sind, wird das Wissen um Datenwege künftig immer wichtiger. Es gilt, jederzeit zu wissen: Wer hat in meinem Netzwerk wann, was, mit wem, auf welchem Weg kommuniziert?

## Netzlast sorgfältig planen

Die Relevanz des Themas ist bereits erkannt und wird in schriftlichen Vorgaben erfasst. So empfiehlt die Dachorganisation Profibus & Profinet International (PI) in ihrer aktuellen Profinet Inbetriebnahmerichtlinie, das eigene Netzwerk zu maximal 20 Prozent mit zyklischem Datenverkehr auszulasten, um genügend „Platz" für azyklischen Datenverkehr zu haben. Dies wird insbesondere dahingehend sicherheitsrelevant, dass ein Großteil der „Angriffe" auf Automatisierungsnetzwerke von innen kommt und mitunter sogar unbeabsichtigt ist. Eine Ermittlung der Topologie, beispielsweise durch eine aktive Scan-Abfrage, produziert ebenso zusätzlichen Datenverkehr im Netzwerk und erhöht die Last wie das Aufspielen von Firmware-Updates. Kommt es infolgedessen zu Qualitätsproblemen, sind die historischen Diagnoseinformationen aus der PNÜ für Betreiber unerlässlich, um zu wissen, was in ihrem Netzwerk los war beziehungsweise ist.

Deshalb löst der Profinet-Inspektor NT die Netzwerklast millisekundengenau auf und ermöglicht so eine Erkennung von Lastspitzen. Außerdem schlägt er sofort Alarm, sobald unbekannte Teilnehmer im Netzwerk auftauchen. Indem Anomalien wie diese jedoch aufgezeichnet und die zugehörigen Daten historisch verfügbar gehalten werden, erhält der Betreiber wichtige, sicherheitsrelevante Hinweise. Somit hat er eine reelle Chance, den Angriff überhaupt mitzubekommen und eventuell notwendige Gegenmaßnahmen einzuleiten.

Angesichts komplexer werdender Instandhaltungsbedingungen braucht es eine Lösung, die die Vielzahl an Informationen zur Kommunikationsdiagnose aus dem Netzwerk zu qualitätsrelevanten Aussagen verdichtet. Mit steigender Intelligenz der Komponenten und Maschinen erhöhen sich auch die Sicherheitsanforderungen und sind eben nicht mehr nur Thema für die IT-Abteilung des Unternehmens, sondern zunehmend auch für die Automatisierungstechnik. Das Konzept der Permanenten Netzwerküberwachung kann für beide Ansätze genutzt werden und bietet vielfältige Diagnosemöglichkeiten. ❐