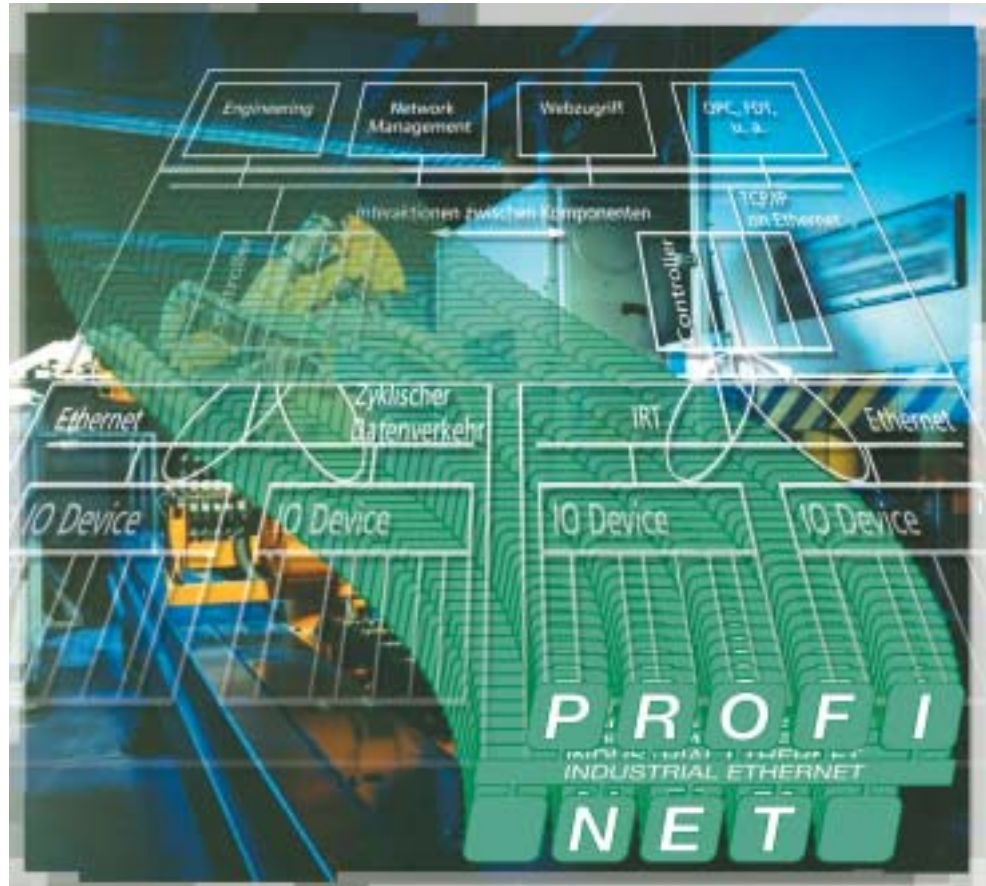


Webintegration und IT-Security

Einfacher und sicherer Zugriff auf Daten und Funktionen über Profinet

Neue Konzepte in der Feldbus- und Automatisierungstechnik setzen auf die durchgängige Verwendung von Ethernet und den darauf aufsetzenden IT-Protokollen wie beispielsweise TCP/IP, FTP oder HTTP bis in die Feldebene. Eine berechtigte Person oder Anwendung kann so zum richtigen Zeitpunkt vom aktuellen Ort aus auf benötigte Information und Funktionalität zugreifen. Durch eine Kombination von Profinet-Webintegration und Standard-Sicherheitsmechanismen kann diese Vision Realität werden.

FRANK IWANITZ



Profinet verwendet Standard-IT für die nahtlose Integration von Daten und Funktionen



FRANK IWANITZ ist Product Manager OPC und Profinet bei der Softing AG in Haar

KONTAKT
T +49/89/45656-332
frank.iwanitz@softing.com

Die Profibus Nutzerorganisation PNO hat mit Profinet ein vollständig neues Automatisierungssystem definiert. Die verschiedenen Aspekte werden in unterschiedlichen Spezifikationen beschrieben. Einige grundlegende Eigenschaften von Profinet sind das Erfüllen verschiedener Echtzeitanforderungen (von 100 ms nicht-deterministischer Zykluszeit bis 1 ms Zykluszeit und <math>< 1\mu\text{s}</math> Jitter), die Skalierbarkeit, der Einsatz von Ethernet und die nahtlose Integration in vorhandene IT-Strukturen, definierte Migrationspfade für vorhandene Anwendungen und Geräte sowie eine Komponentenorientierung für die Anwendung und das Engineering.

Das Profinet-Modell unterscheidet zwischen Controllern (z. B. SPS) und IO Devices (Drives, einfache Feldgeräte, etc.). Die Anwendungsfunktionalität in Controllern kann in abgeschlossenen Softwarebestandteilen enthalten sein, die auch als Komponenten bezeichnet werden. Diese Komponenten tauschen Informationen unter Nutzung eines Komponentenbusses aus. Eine portierbare Version der entsprechenden Software steht kostenlos für PNO-Mitglieder zur Verfügung. Komponentenanwendungen können durch ein herstellerübergreifendes Engineering entworfen und in Betrieb gesetzt werden. Bei der Interaktion zwischen Controllern und IO Devices setzt Profinet auf das bewährte Profibus-DP-Modell, das unter Berücksichtigung

der neuen Möglichkeiten (Ethernet als Medium) und vorhandener Anforderungen erweitert wird.

Möglichkeiten der Profinet-Webintegration

Die meisten Spezifikationen sind inzwischen fertig gestellt und freigegeben. Auf der Hannover Messe 2004 wird eine Vielzahl entsprechender Produkte gezeigt. Neben der Integration der Profinet-Stacks in Geräte und der Erweiterung von Anwendungen spielt besonders die Webintegration gegenwärtig eine wichtige Rolle. Ziel dieser Spezifikation ist das Festlegen eines einheitlichen Weges für den Zu-

griff auf Profinet-Daten aus Webanwendungen. Offenheit, Skalierbarkeit und Interoperabilität der Webintegration-Lösung sollen gewährleistet werden durch Festlegen der zu verwendenden Webtechnologien und Protokolle, Definieren eines entsprechenden Adressierungsschemas basierend auf Profinet-Runtime-Spezifikationen und Vorschlagen verschiedener Lösungen für das Implementieren der Spezifikation (Best practice pattern).

Ein Profinet-Webserver kann auf dem Profinet-Gerät laufen, von dem die Daten kommen. Eine andere Möglichkeit besteht darin, einen übergeordneten Server zu verwenden. Dieser Server wird dann mit den Profinet-Geräten über das jeweilige Profinet-Protokoll (Komponentenbus oder IO-Kommunikation) kommunizieren.

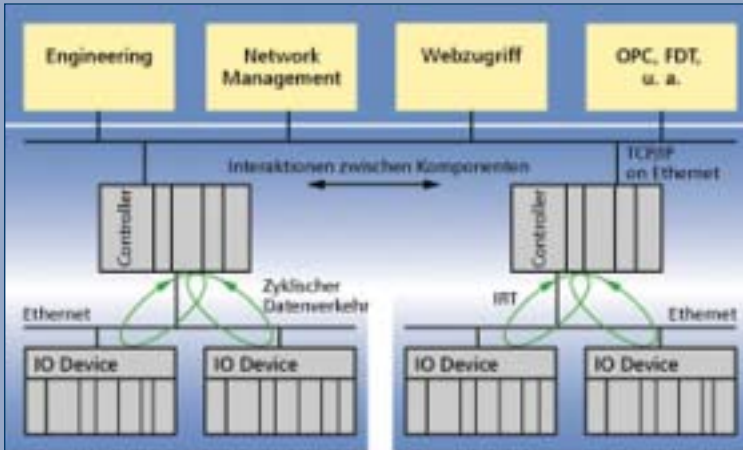
Profinet-Webclients können entweder über statische HTML-Seiten oder über Webservices auf Daten zugreifen. Für das Gestalten statischer Seiten wird ein Styleguide festgelegt. Als Vorgabe für das Implementieren von Webservices wird OPC XML DA angegeben.

Da für eine Profinet-Webintegration-Anwendung nur allgemein genutzte Technologien des Internet Verwendung finden, werden keine speziellen Anforderungen hinsichtlich der Implementierung gestellt. An einer Profinet-Webanwendung sind drei Teilnehmer beteiligt: Das Profinet-Gerät stellt Daten zur Verfügung und nimmt sie entgegen. Bei diesen Daten handelt es sich um Informationen über den Prozess, die Anlage, das Automatisierungsgerät oder die Automatisierungsanwendung. Diese ►

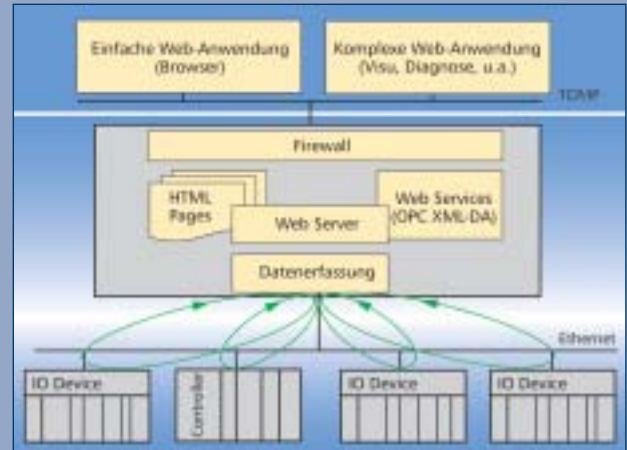
Anzeige

Besuchen Sie uns auf der Hannover Messe 2004, Halle 9, Stand G32





Profinet – Systemstruktur und Integrationsmöglichkeiten in automatisierungstechnische Anwendungen



Anwendungsstruktur: Das Bild zeigt die verschiedenen Bestandteile eines Profinet-Webintegration-Gerätes

Informationen werden über den Profinet-Komponentenbus oder das IO-Protokoll ausgetauscht. Das Profinet-Webintegration-Gerät implementiert einen Webserver, der die Informationen in Form von HTML-Seiten zur Verfügung stellt. Das Spektrum kann dabei von der einfachen HTML-Seite mit festen Werten bis zur HTML-Seite mit Skriptanteilen für die Client- oder Server-seitige Verarbeitung reichen. Diese Informationsübermittlung ist für die Interaktion mit Menschen vorgesehen. Webservices stellen Informationen für die An-

wendung zur Weiterverarbeitung zur Verfügung. Mit OPC XML DA nutzt man auch hier einen verfügbaren Standard. Der Profinet-Webintegration-Client nutzt die zur Verfügung gestellten Daten und leitet sie weiter. Jeder HTML-Browser kann dabei als Client verwendet werden und auf die Information in den HTML-Seiten zugreifen. Mit Hilfe von Webservices lassen sich auch weitere Anwendungen, etwa aus den Bereichen Visualisierung, Diagnose, Asset Management, Gebäudeüberwachung, Qualitätssicherung,

Betriebsdatenerfassung oder Produktionsmanagement steuern.

Datensicherheit im IT-Umfeld

Die Profinet-Webintegration ermöglicht es Personen und Anwendungen, von einem beliebigen Ort auf benötigte Informationen zuzugreifen. Um zu gewährleisten, dass dies ausschließlich durch berechtigte Personen und Anwendungen geschieht, müssen entsprechende Rahmenwerke für die IT-Sicherheit definiert und implementiert werden.

Zugriffsversuche auf Daten und Funktionen lassen sich in die folgenden Kategorien einteilen:

- ▶ gewollt positiv – In diesem Fall greift der autorisierte Mitarbeiter (die autorisierte Anwendung) erlaubt auf ihm zugeordnete Daten und Funktionen zu.
- ▶ ungewollt negativ – Der Mitarbeiter hat sich unbeabsichtigt geirrt, z. B. einen anderen Rechner angewählt oder eine falsche Variable gesetzt.
- ▶ gewollt negativ – In diesem Fall hat eine Person bewusst destruktiv gehandelt, entweder durch eine falsche Aktion oder es wurde eine Aktion eingeleitet, um das Nutzen verfügbarer Funktionalität unmöglich zu machen (aus der IT bekannt als Denial of Service).

Dabei darf nicht vergessen werden, dass ungewollt negative und gewollt negative Zugriffe sowohl aus dem Internet als auch aus dem unternehmenseigenen Intranet heraus erfolgen können. Der Schutz der Anlagen und des Prozesses hinsichtlich ungewollt oder gewollt negativer Zugriffe ist gegenwärtig ein wichtiges Arbeitsfeld in der Automatisierungstechnik.

Entsprechend gibt es bereits einige theoretische Lösungsansätze für den Schutz der Anlage und Geräte. Da die Automatisierungstechnik Anleihen bei der IT macht, muss für das Realisie-



Besuchen Sie uns auf der Hannover Messe 2004, Halle 9, Stand F05

ren der Sicherheitsmechanismen nichts Neues entwickelt werden. Vorhandene, bewährte Lösungen für das entsprechende Einsatzfeld können übernommen und gegebenenfalls angepasst werden. Die Ansätze im IT-Umfeld werden auch in Zukunft unabhängig von der Automatisierungstechnik weiter entwickelt. Das ist ebenfalls ein Vorteil.

Definieren eines Security-Konzeptes

Bei einem Profinet-Webintegration-Gerät überprüft die Firewall-Software die IP-Adresse des aufrufenden Rechners. Somit ist eine erste Zugangskontrolle möglich. Aufrufe von Rechnern mit anderen als den konfigurierten IP-Adressen werden abgewiesen. Durch die Adresstranslation verhindert die Firewall, dass aus dem Internet direkt auf Rechner im Netz hinter der Firewall zugegriffen werden kann. Alle Zugriffe sollten zudem protokolliert werden. Hat der Aufruf die Firewall passiert, geht er zum Webserver. HTTP unterstützt per definiertem Protokollbestandteil eine Basic-Authentifizierung. Möchte der Client auf eine gesicherte HTML-Seite oder Webservice-Funktion zugreifen, so fordert der Server entsprechende Authentifizierungsinformationen an. Basic Authentication sendet die Information unverschlüsselt über das Netz. Durch Verwenden von HTTPS ist aber auch eine verschlüsselte Übertragung möglich. Dieser Ablauf ist allgemein bereits vom Home Banking bekannt. Basierend auf der übergebenen Authentifizierungsinformation führt der Webserver entsprechende Entscheidungen durch, HTML-Seiten werden übertragen oder nicht. Das Nutzen von Diensten und Funktionalität wird erlaubt oder abgewiesen.

Um Sicherheitsmechanismen zusammen mit Profinet-Webintegration zu implementieren, gibt es zwei Möglichkeiten. Die Webintegration-Komponente kann hinter einer existierenden Firmen-Firewall im Intranet laufen oder sie ist autark und direkt mit dem Internet verbunden. Im ersten Fall laufen viele Sicherheitsmechanismen auf der Firewall ab. Durch eine Redirektion der Aufrufe im Webserver auf der Firewall können diese an die Webintegration-Komponente weitergeleitet werden. Es darf aber auch in diesem Fall nicht auf die eigene Firewall der Webintegration-Komponente verzichtet werden. Schließlich kommen ungewollt oder gewollt negative Zugriffe nicht ausschließlich aus dem Internet. Mit dem Einsatz eines Webintegration-Gerätes mit integrierter Firewall lassen sich sichere informationstechnische Inseln im Intranet schaffen. Es gibt einen einzelnen Zugangspunkt, an dem genau festgelegt und überwacht werden kann, welche Person oder Anwendung Zugriff auf welche Daten und Funktionen hat. Damit erfüllt die vorgestellte Lösung die Anforderungen hinsichtlich:

- ▶ Connection authorization (Autorisieren der Verbindung)
- ▶ User authorization (Autorisieren des Nutzers)
- ▶ Action authorization (Autorisieren der Aktion)

Die Punkte Deterrence (Abschreckung), Response (Antwort), Intrusion Detection (Entdecken des Eindringens) und Mechanism Protection (Schutz des Sicherheitsmechanismus) müssen durch administrative Maßnahmen in der Firma selbst gewährleistet sein.

Einfache IP-Adressenvergabe

Ein positiver Nebenaspekt des vorgestellten Ansatzes besteht in der einfacheren Vergabemöglichkeit für IP-Adressen. Die Profinet-Geräte lassen sich über IP-Adressen ansprechen, die für Geräte am Intranet einer Firma zentral vergeben werden. Befinden sich die Profinet-Geräte in

Aktueller Status der Profinet-Spezifikationen (Stand Februar 2004)	
Spezifikation	Status
Chapter 0 Overview and Introduction	2.01, Juli 2003
Chapter 1 Objects in Automation	2.01, Juli 2003
Chapter 2 Profinet Runtime Model	2.02, Februar 2004
Chapter 3 Profinet Engineering Model	2.02, Februar 2004
Chapter 4 Profinet Extensions - Webintegration	0.73, Januar 2003
Chapter 5 Profinet Network Management	0.61, Juli 2002
Profinet IO Device model and System integration (White paper in Deutsch)	0.99, Mai 2003
Profinet IO Application Layer Service Definition	0.3, Juli 2003
Profinet IO Application Layer Protocol Definition	0.2, Oktober 2003
Profinet Guideline – Installation Guideline Profinet	1.8, November 2002

einer abgegrenzten Zone, wie es durch die vorgestellte Lösung möglich ist, so ist es weitestgehend dem Projektierer oder Inbetriebnehmer überlassen, welche IP-Adressen für die Geräte verwendet werden. Konflikte mit Adressen in anderen Bereichen können durch das Verwenden der Firewall nicht auftreten. Einzig bei Vergabe der IP-Adresse für die Firewall ist eine Absprache notwendig. ■

Beitrag als PDF auf www.aud24.net

[more @ click](#) **AD044252** >

Anzeige