

OPC

„Eine Gute Alternative?“

Wilhelm Uhlenberg

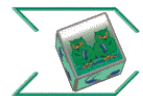
wu@sv-uhlenberg.de



Vortrag 1K01 20. April 2004 13:00-13:25 Uhr zum DECUS Symposium 2004 in Bonn

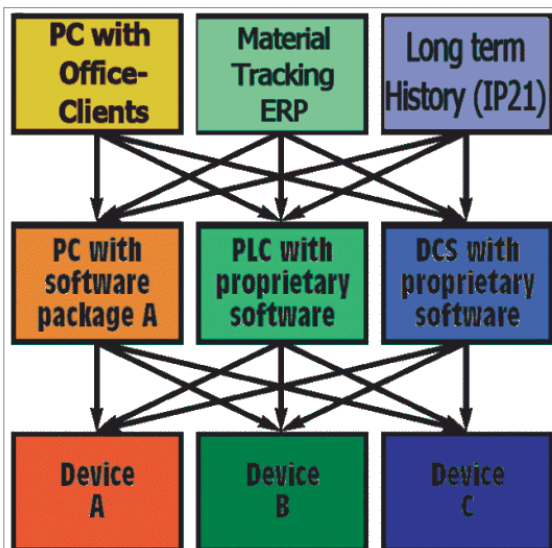
- 1K01 DECUS 2004 -

1

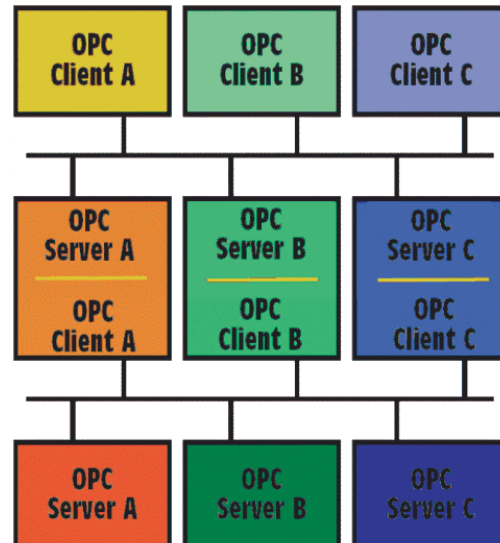


Was hat man, was will man...

■ Ausgangslage ←



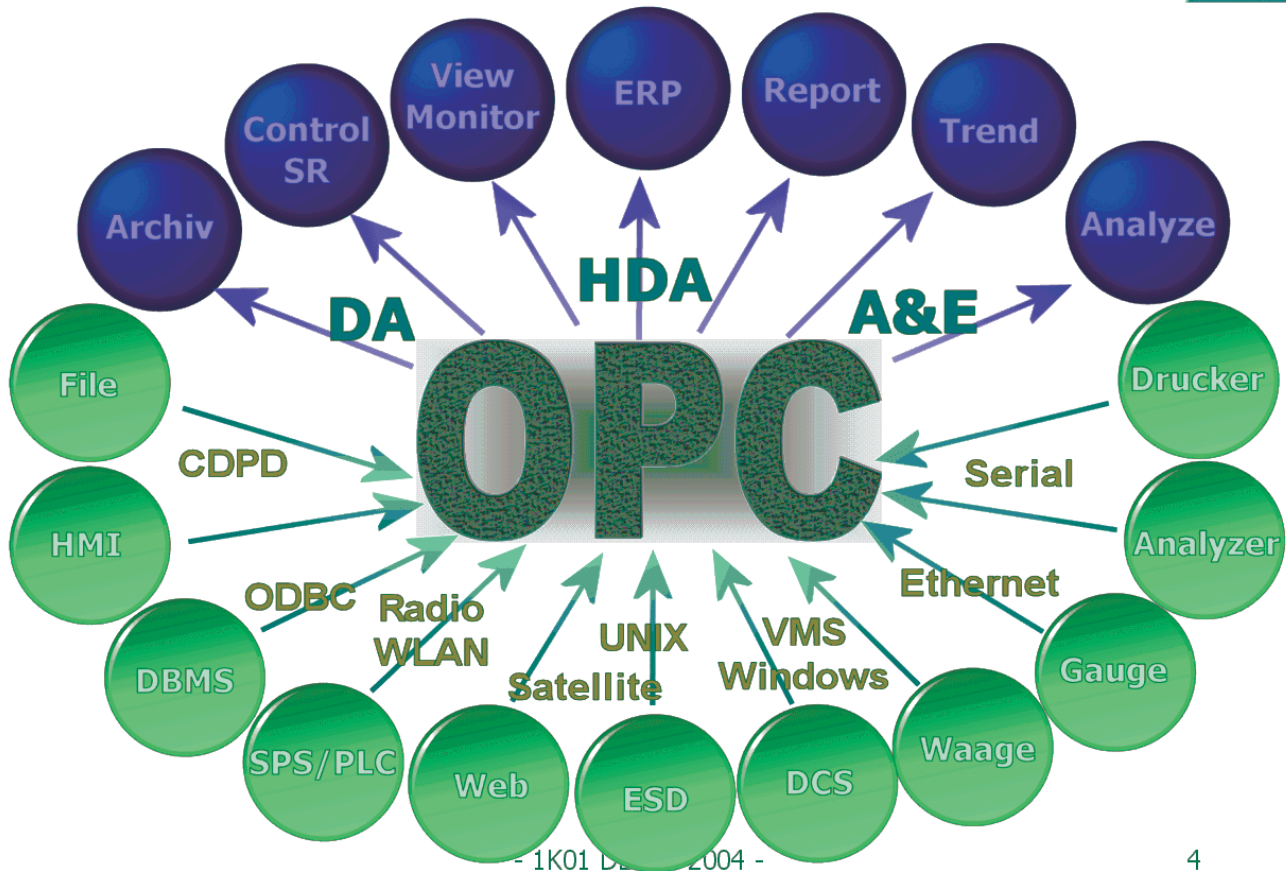
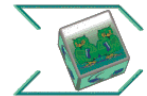
→ Zielstruktur



- 1K01 DECUS 2004 -

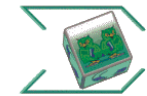
3

Die Vision



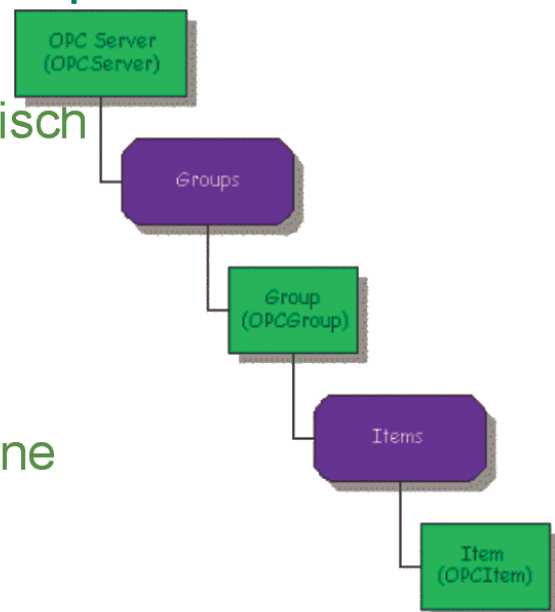
4

Grundlagen



■ Konzept der Datentransportsichten aller OPC-Teile

- Dreigliedrige hierarchisch organisiertes Objekt-Zugriffsmodell.
- Server bildet reale Objekte auf Items ab
- Client verwaltet eingene Gruppenbildungen



Einführung

■ Was soll das Ganze? (OPC)

- Interoperabilität durch „irgendeinen“ Standard
 - ◆ „Automatisierungs Esperanto“
 - ◆ Marktmacht und Verbreitungsgrad gab den Ton an
- Zielnutzen der Anwender (z.B. HMI, Office, Math., DBs)
 - ◆ Wichtigstes Ziel der OPC Aktivitäten ist es, ein einheitliches Softwareinterface zu schaffen, das aufbauend auf Microsoft-Technologien für die Nutzer einfach zu handhaben sowie für die Anbieter von Automatisierungssystemen einfach zu implementieren ist.
- Strukturierung des erforderlichen Datenaustausches
- Integrität der prozessnahen Systeme nicht beeinflussen
 - ◆ z.B. Realtime, Redundanz ohne Leistungsunterbrechung
- Unabhängigkeit von Herstellern (SPS, Geräte, DCS, PLS)
- Akzeptanz auf Anwenderseite

Einführung

■ Woher kommt das Ganze?

- Initiatoren: task force “5er-Bande”:
Fisher-Rosemount, Rockwell Software, Opto 22, Intellution und Intuitive Technology in 1995
- Industriestandard seit Version 1 im August 1996
- “OPC Foundation” managed seit 1996 den Standard
- Mehr als 280 (~15 Große) aktive Mitglieder und >1000 Anbieter von Lösungen (weit mehr als 200 OPC Server verfügbar)
- Nebeneffekt: Kooperation mit MS soll mit Vorinformation/ Richtungsfindung kleinerer Firmen stärken.

OPC History

Year	Event
1990	Windows 3.0: DDE → NetDDE
1992	OLE 2.0 → COM/DCOM
1995	OPC Task Force formed
1996	OPC Foundation, OPC DA 1.0a
1996	OPC DA 2.0 released
2008	OPC DA 3.0 released

Einführung

■ Was ist dabei herausgekommen?

- Eine Implementation bis jetzt unter ActiveX und „COM/DCOM+“-Gesichtspunkten (Früher OLE)
- Mindestanforderungen werden vorgegeben
- Server/Client Konzept (kombinierbar)
 - ◆ Datenlieferant ist (meist) Server und Konsument braucht den OPC-Client-Anteil.
- MS hat dadurch erreicht: Alle OLE-fähigen Anwendungen (z.B. Office) mit der Automatisierungsumgebung gekoppelt.
- .NET Strukturen brauchen weiterhin DCOM+

Einführung

■ Wohin entwickelt sich OPC weiter

- ERP Einbindung (z.B. SAP)
- Complex Data Types
- Redundancy Concepts
- Automated Browser Interface (ASP.NET?)
- Telemetry SCADA specials
- Mobile (PDA) clients (GPS OPC server)

Grundlagen

- Was ist ein OPC Server?
 - Spielt die Rolle der Datenquelle
 - Reagiert nur auf Anforderungen
 - Erfüllt eine Nachfrage, erzeugt sie aber nicht!
- Was ist ein OPC Client (Beispielsicht)?
 - Arbeitet als Datensinke
 - Erzeugt Anforderungen
 - Erzeugt die Nachfrage, aber befriedigt sie nicht!

Begriffshierarchie in der Theorie

- Der Oberbegriff „OPC“ vereint heute (major issue):
 - DA Data Access (2.05a, 3.0)
 - AE Alarm and Event (1.10)
 - HDA Historical Data Access (1.10)
 - DX Data eXchange (1.0)
 - Batch (2.0)
 - XML DA (Web Zugriffe)



Wofür ist was gedacht (1)?

■ OPC DA 3.0

- Data Access ist die simpleste Form Momentan-Werte/ Zustände austauschen zu können.
- Obligate Items (z.B. Value, Timestamp, Quality)
- Optionale Items oder Properties an Items je nach Anbieter (z.B. Limits, Deviation, ROC)
- Browser Interface zur Item-Konfiguration optional
- Server-, (global)Group-, Item- Namensraum eindeutig.
- Client kann permanente, eigene Listen (Gruppen) aufbauen
- Die möglichen Eigenschaften zur Datenlieferung legt der Server fest.
 - ◆ Intervallstaffelung, Asynchron, globale Gruppen

Wofür ist was gedacht (2)?

■ OPC AE 1.10

- Alarm und Event dient zur Generierung von melde- und archivierungbedürftigen Ereignissen im Clienten.
- Obligate Items (z.B. Timestamp, Message, Severity, Status)
- Optionale Items oder Properties an Items je nach Anbieter (z.B. Limits, shutdown alarms, global notifications)
- Browser Interface optional
- Server-, (global)Group-, Item- Namensraum eindeutig.
- Client kann permanente, eigene Listen (Gruppen) aufbauen

Wofür ist was gedacht (3)?

■ OPC HDA 1.10

- Historical Data Access ist eine Form gespeicherte historische Werte/Zustandsverläufe zugänglich zu machen.
- Obligate Items (z.B. Time frame, Time span, Item-ID, Quality)
- Optionale Items oder Properties an Items je nach Anbieter (z.B. SPC Werte, Reduktionsanwendungen, Mittelwerte)
- Browser Interface optional
- Server-, (global)Group-, Item- Namensraum eindeutig.
- Client kann permanente, eigene Listen (Gruppen) aufbauen

Wofür ist was gedacht (4)?

■ OPC DX 1.0

- Data eXchange ist die simpleste Form Momentanwerte/zustände zwischen OPC-Servern direkt austauschen zu können bzw. of Geräteebene miteinander zu reden.
- Obligate Items (z.B. Value, State, Timestamp, Quality)
- Optionale Items oder Properties an Items je nach Anbieter (z.B. Limits, Deviation, ROC)
- Feldbus Devices (Ventile, Schieber, SIMOCODE, Motoren)
- Externe Geräte (Analysatoren, Sensoren [Druck...], Regler)
- SPS Verriegelungen über Zellenebene
- Wireless Field-Devices (Radar Level, Ultraschalldetection)

Wofür ist was gedacht (6)?

■ OPC XML DA 1.0

- Soll den Austausch auf Internet-Ebene (abgesetzt) koordinieren.
- Item-Struktur ähnlich der DA Interface specification
- Unkritische Zeitintervalle?
- Verbindungsloser (Netzwerk) Support
- Datenstrukturen als SOAP messages in SOAP Körper-Strukturen.
- Höherer Konvertierungs-Overhead
- Log. Struktur

Tatsächliche Beispiele

- Energie Versorgung/Verteilung USA ☹️ 😊
 - ◆ Bedarfserfassung, Prognose, Verteilung
- Gebäude-Management 😐
 - ◆ Bindeglied zwischen Teilsystemen.
- Chemische Verfahrenstechnik 😊
 - ◆ Weltweite Produktionsdatenverfolgung und Planung
- Maschinensteuerung ☹️
 - ◆ Geschwindigkeitsreglung an Spindeln

Zielanwendungen Einsatzgebiete

- Inhomogener Zoo an Front-End (Erfassungs-) Systemen in Office
- Office-Welt erhält leichten Zugang (Automation I/F)
 - ◆ Diverse Bridge-Produkte (OPCDDE usw.)
- Integration in PIMS (IP21, PI, TnT, EH).
- Querkommunikation unter Zellen (SPS, PLS, ERP)
- Redundency Broker
 - ◆ Mehrfachredundanzen nachrüstbar
- Wireless Sensors, Fieldbus Devices, Profibus Teilnehmer können als OPC Server agieren (parallel zum native access)
- Kommandos/Ausgaben zum Server sind möglich



Vorteile für den Anwender

- Liefereinheit wird nicht durch Fremd-Interfaces „aufgebohrt“
 - ◆ Verantwortlichkeiten
 - ◆ Technische Stabilität
- Interoperabilität
- Kosten
- „Freie“ Software kon
- Externes Know-How

Wenn drei verschiedene Leitsysteme oder SPS-Ebenen an drei verschiedene Konsumenten-Systeme vollständig zu koppeln sind, müssen bisher 9 Individual-Softwareinterfaces programmiert werden !

Positive Sicht

■ Einige Vorteile

- Unabhängigkeit der Software von den Steuerungsherstellern.
- Mehrere Clients können auf Prozessdaten gleichzeitig zugreifen.
- OPC Server für alle namhaften Hersteller und Bussysteme verfügbar (fast alle mit Rang- und Namen sind dabei).
- Viele Hersteller bieten ein OPC-Client-I/F zum Import von Prozessdaten fremder Leitsystem ins jeweils eigene an.
- Netzwerkfähigkeit im Intranet (COM/DCOM Technologie).
- Lösungen über Domain-Grenzen hinaus verfügbar.
- einfache Konfiguration des Datenaustauschs (Browsing).
- schnelle Integration von neuen Geräten oder Automatisierungskomponenten.

Bewertung

■ Gibt es auch Nachteile (Einschränkungen)?

- Es kommt darauf an wen man fragt
 - ◆ „MS“ sieht keine, sondern ☺ (Was B.G. dazu meinte)
 - ◆ „Leichter Zugriff aller Ebenen auf Prozess-Daten“; aber RPC und DCOM „Löcher“ vorhersehbar oder zu stopfen?
- Realtime muss sich die Grenzen vor Augen führen
 - ◆ Client-Server Verbindungsprotokoll beruht nicht auf deterministischen Ansätzen.
 - ◆ Minimal-Zyklen werden durch Server-Implementation bestimmt. OPC-Server mit künstlicher Lastbremse.
- Indirekt nimmt die Abhängigkeit von Monopolen zu und die Differenzierbarkeit einzelner Hersteller ab ☹.
- Sekretärinnen und Controller glauben Sie verstehen die MSR-Technik weil die „life“-Daten von der Produktionsmaschine in „ihrem“ Excel-Sheet sind.

Häufige Fehler

- Kein Konzept (insbesondere kein Sicherheitskonzept).
- Fehlendes Verständnis technischer Art.
 - Eigene Anforderungen unklar (nicht definiert)
 - Fehlerhafte Anwendung
- Falsche Partner.
- Die Wirkungen der Daten-Transparenz nach Außen werden falsch und unterschiedlich beurteilt.
- Unrealistische Terminabläufe.
- *Ich habe OPC gekauft und warum geht es nicht?*
 - Subjektive Drucksituation wird empfunden.

Zwischenfazit

- OPC lebt und entwickelt sich weiter
- Ersteller und Designer sind in „compatibility camps“ zum Nutzen der Anwender aktiv
- Jede neue Geräteentwicklung und neuere Datenerfassungssysteme haben OPC standardmäßig „onboard“
 - Kostengünstige erste Alternative
- DA, HDA, AE, DX, XML viele begriffliche Untervarianten von OPC werden gern vermischt und im evt. Nicht optimal ausgewählt.
 - Auswahlhilfen nach Analyse des Einsatzumfeldes
- Positive Erfahrungen bei Integration von Fremdsystemen.
 - Der kleinste gemeinsame Nenner hilft sich zu verstehen!
- Orientierung.

Referenzen / Quellen

- OPC Foundation <http://www.opcfoundation.org>
- Trebing & Himstedt Prozessautomation GmbH, diverse Fachaufsätze
- Matrikon, Edmonton, Canada <http://www.matrikon.com/opc>
- Softing AG <http://www.softing.de>
- Siemens Automatisierung
- AspenTech OPC CIM-IO <http://www.aspentech.com/>
- ABB IndustrialIT <http://www.abb.com/de>

Referenzen / Quellen

- Nuefelder, A. M., Ensuring Software Reliability, Marcel Dekker, New York, NY, 1993.
- Goble, W. M., Control Systems Safety Evaluation and Reliability, ISA, Research Triangle Park, NC, 1998.
- C't, Zeitschrift Heft 5 2004 Reihe „Das intelligente Gebäude“
- Software Bug Contributed to Blackout By *Kevin Poulsen*, SecurityFocus Feb 11 2004 3:55PM
- 'CYBER SECURITY OF THE ELECTRIC POWER INDUSTRY', DECEMBER 2002; INSTITUTE FOR SECURITY TECHNOLOGY STUDIES AT DARTMOUTH COLLEGE
- Cyber-Security: Are Plant Operations Vulnerable? Brian M. Ahern, President and CEO, Verano Inc., September 16, 2003
- Reliability in Control Systems Software, Dr. William M. Goble, Principal Partner <http://www.exida.com>
- 'Critical Infrastructure Security and You', Rik Farrow, Network Magazine, October 5, 2002 - <http://www.networkmagazine.com/article/NMG20020930S0008>
- 'Hackers Target Energy Industry', Charles Piller, Los Angeles Times, July 8, 2002 - http://www.latimes.com/news/nationworld/nation/la-scihackers8jul08005047_story?coll=la%2Dheadlines%2Dnation%2Dmanual
- 'E-Terrorism', Robert Lemos, John Borland, Lisa Bowman and Sandeep Sunnarkar, C-Net News, August 26, 2002 - <http://news.com.com/2009-1001-954728.html>
- 'Cyber Attacks by Al Qaeda Feared', Barton Gellman, Washington Post, June 27, 2002 - <http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26>
- und andere.