MatrikonOPC

Effektive OPC-Sicherheit für Steuerungssysteme – Lösungen, auf die Sie zählen können

Darek Kominek
Manager, OPC Marketing, MatrikonOPC,

Eric Byres
P. Eng., ISA Fellow CTO,
Byres Security Inc.

2011

1. VORWORT

In den letzten zehn Jahren versuchten Ingenieure und Administratoren industrieller Steuerungssysteme sich einzureden, dass es zwischen ihren Systemen und dem Rest der Welt tatsächlich einen „Grenzwall" gäbe. Sie hofften, dass sie frei nach dem Motto „Sicherheit durch Unklarheit" (Security by Obscurity) von Sicherheitsbedrohungen verschont bleiben würden. Diese Zeiten sind vorbei – das zeigen aktuelle Sicherheitsvorfälle wie der Stuxnet-Wurm, der die Siemens-Systeme WinCC und PCS7 im Iran attackierte, sowie die Fernsabotage eines texanischen Stromversorgers. Die genannten Beispiele sind ein Weckruf für die Automatisierungsbranche. Die aggressiven, zielgerichteten Angriffe machen klar, wie angreifbar und ungeschützt Automatisierungssysteme wirklich sind. Sie bieten uns zudem einen Ausblick auf zukünftige Bedrohungen der Branche. Letzten Endes sind sie eine deutliche Warnung: Schützen Sie Ihre Steuerungs- und Automatisierungssysteme, wenn Sie nicht die Zuverlässigkeit und Sicherheit Ihres gesamten Betriebs riskieren wollen.

Auch wenn kein Zweifel mehr an den Konsequenzen solcher Cyberattacken und Schadprogramme besteht, bleibt die Frage: „Wie kann ein Ingenieur sein Steuerungssystem zuverlässig schützen?" In diesem Whitepaper erhalten Sie eine einfache und kostengünstige Lösung für dieses Problem – eine auf OPC-Technologie basierende Sicherheitslösung, die heute in so gut wie allen Industrieanlagen anwendbar ist.

„Man ist oft der Meinung, dass Steuerungssysteme keine „beliebten Ziele" für Angriffe sind. Das stimmt nicht. Alle Systeme, die in großen Mengen hergestellt werden, sind beliebt genug. Wenn Sie in irgendeiner Weise mit Steuerungssystemen arbeiten, insbesondere im Bereich Sicherheit, machen Sie Cybersicherheit am besten sofort zu einem wichtigen Bestandteil Ihres Prozesses. Die Konsequenzen können katastrophal sein, wenn Sie Sicherheitserwägungen in Bezug auf bestimmte Applikationen außen vor lassen."

Bob Mick, Vice President
Emerging Technology,
ARC Advisory Group

Beispiel:

Aktuelle größere Sicherheitsvorfälle in Industrieumgebungen Nr. 1

Der Wurm Stuxnet, ein Schadprogramm, das speziell für den Angriff auf Projekte entwickelt wurde, die WinCC, PCS7 und S7 PLC von Siemens verwenden, gelangt über infizierte USB-Sticks in ein Steuerungssystem (eine Verbindung zum Internet ist somit für die Infizierung nicht erforderlich). Einmal eingedrungen, verbreitet sich der Wurm auf andere Computer, die Protokolle für die Datei- und Druckerfreigabe sowie den SQL-Datenbankzugriff nutzen.

Da es für derartige „Angriffe" keine Patches gab, als der Wurm entdeckt wurde, war die beste Verteidigung, zu verhindern, dass die betroffenen Protokolle auf kritische Server zugreifen konnten, wenn dies nicht unbedingt nötig war. Leider verhielten sich, wie im Dokument erwähnt, altmodische OPC-Lösungen genau entgegengesetzt – alle vorhandenen Protokolle konnten ungehindert an den OPC-Server gesendet werden, unabhängig davon, ob sie zur Steuerung nötig waren oder nicht.

2. SYSTEME ÄNDERN SICH

Informationsnetzwerke sind zum Herzstück der SCADA-Systeme (Supervisory Control and Data Acquisition Systems) geworden, die in Unternehmen für das zentralisierte Management und die Überwachung sorgen. Traditionell bauten Unternehmen Prozessleitsysteme (PLS) und SCADA-Systeme getrennt von anderen Unternehmenssystemen auf. Diese Art von Systemen war durch proprietäre Geräte oder Protokolle effektiv „abgeschirmt".

Geschäftliche Faktoren haben nun zur Annäherung von Unternehmensnetzwerken und Industrietechnologien geführt. So hat z. B. der Bedarf an Remotezugriff zu Datenzugriffs- oder Supportzwecken bewirkt, dass auf viele Steuerungssysteme nun auch über Nicht-SCADA-Netzwerke zugegriffen werden kann. Darüber hinaus setzen viele Unternehmen gemeinsam genutzte Hardware, Basisnetze und Netzwerksupportressourcen ein, um die Kosten für Netzwerkbereitstellung und -management zu senken. Vor allem aber hat der gesteigerte Einsatz von kommerziellen Standard-Computerkomponenten und Office-Netzwerktechnologien die geschäftlichen Abläufe in fast allen größeren Branchen verändert. Aufgrund dieser Standardisierungsstrategien und des damit einhergehenden unmittelbaren Datenzugriffs im gesamten Betrieb einschließlich des Fertigungsbereichs können Unternehmen kostengünstig operieren, effizienter kommunizieren und agilere Geschäftspraktiken umsetzen.

Während man in den Unternehmen die Früchte dieser Initiativen erntet, entdecken viele auch die Gefahren, die damit einhergehen, wenn Steuerungsnetzwerke für einen weiteren Nutzerkreis zugänglich gemacht werden. Indem man Unternehmenssysteme verbindet, um Kunden, Lieferanten und anderen Zugriff zu gewähren, wird die Verwundbarkeit der sensiblen und vertraulichen Daten dieser Systeme signifikant gesteigert. Zudem macht es die Systeme angreifbar für externe Bedrohungen wie Würmer, Viren und Hacker. So wird es immer schwieriger für Systemadministratoren, den Spagat zwischen notwendiger Zugänglichkeit und ausreichendem Schutz der Integrität und Nutzbarkeit ihrer unternehmenskritischen Steuerungssysteme zu schaffen.

3. DIE ANGRIFFSFLÄCHE REDUZIEREN

Einer der effektivsten Wege, mit dem Konflikt zwischen den Anforderungen von effizientem Zugriff und effektiver Sicherheit umzugehen, ist, so wenig verschiedene Schnittstellen und Protokolle wie möglich zwischen dem Steuerungssystem und externen Netzwerken zu unterhalten. Der Einsatz einer einzigen genehmigten Verbindungslösung, die verschiedene Unternehmensanforderungen erfüllt, senkt nicht nur die Kosten für die Bereitstellung und Verwaltung, sondern bietet Angreifern oder Würmern auch weniger Möglichkeiten einzudringen. Daher ist diese Maßnahme dafür bekannt die „Angriffsfläche" eines Systems zu reduzieren.

Die erste Aufgabe eines Administrators besteht also darin, eine geeignete Kommunikationstechnologie auszuwählen, die von den meisten Steuerungs- UND Geschäftssystemen unterstützt wird. Es gibt zwar eine Reihe möglicher Kandidaten, darunter Modbus-TCP oder Hyper Text Transfer Protocol (HTTP), doch OPC ist ohne Frage einer der einfachsten und am weitesten verbreiteten Standards, der die Anforderungen eines universellen Datenzugriffs in der Industrieautomatisierung erfüllt.

Beispiel:

Aktuelle größere Sicherheitsvorfälle in Industrieumgebungen Nr. 2

Bei einem weniger bekannt gewordenen Vorfall im Jahre 2009 wurde ein großer Energiekomplex durch ein Virus infiziert, als ein Auftragnehmer zu Wartungszwecken eine Remoteverbindung mit einem Schwingungsüberwachungssystem herstellte. Das Virus konnte sich von den Computern des Überwachungssystems auf verschiedene PLS-Server ausbreiten und verursachte wiederholte Abstürze zentraler Server und Produktionsausfälle.

Zu diesem Zeitpunkt kamen dort traditionelle IT-Firewalls zur Isolierung der verschiedenen Steuerungssysteme zum Einsatz. Unglücklicherweise bewirkte die Verwendung von dynamischen Ports durch OPC Klassik, dass Firewall-Regeln zum Einsatz kamen, die das Virus nicht stoppen konnten. OPC-fähige Firewalls wie Tofino OPC Enforcer verwenden strengere Regeln und hätten verhindern können, dass sich der Wurm ausbreitet.

OPC das früher für OLE for Process Control stand, heißt nun offiziell OPC Klassik und ist der weltweit am meisten verbreitete Integrationsstandard in Industrieumgebungen. Er kommt in zahlreichen Industrie- und Geschäftsapplikationen zum Einsatz, z. B. in Workstations mit HMIs (Human Machine Interfaces), sicherheitstechnischen Systemen (Safety Instrumented Systems – SIS) und PLS im Fertigungsbereich, in Unternehmensdatenbanken, ERP-Systemen (Enterprise Resource Planning) und anderen geschäftsorientierten Softwarelösungen für Unternehmen .
Doch wie sieht es in Bezug auf Sicherheitsanforderungen aus – wird OPC auch diesen gerecht? Dieses Whitepaper wird zeigen, dass die Antwort darauf definitiv JA lautet. Anhand von auf OPC ausgelegten Schutzebenen lassen sich Hochsicherheitslösungen entwickeln, die die verschiedenen Erwartungen von Unternehmen in Bezug auf Sicherheit und Zugänglichkeit gleichermaßen erfüllen, ohne das Netzwerk- oder das Steuerungsteam durch administrative Aufgaben zu überlasten. Das Ergebnis ist eine standardbasierte Lösung, die sich bei vielen unterschiedlichen Steuerungssystemen bewährt hat.

4. SCHUTZEBENEN

Wenn der erste wichtige Schritt zu einer verbesserten Sicherheit ist die Angriffsfläche zu reduzieren, ist der zweite das Anlegen von Schutzmechanismen auf verschiedenen Ebenen. Dies wird auch als tiefgestaffelte Verteidigung (engl. „Defense in depth“) bezeichnet und folgt dem Konzept, Risiken mit unterschiedlichen Verteidigungsstrategien zu begegnen. Das Anlegen mehrerer Schutzebenen hat verschiedene Vorteile. Dabei ist der offensichtlichste Vorteil, dass, wenn eine Schutzebene kompromittiert wird, die nächste Schutzebene anhand einer anderen Sicherheitsmethode ein zusätzliches Hindernis darstellt, um ein weiteres Eindringen zu verhindern.

Ein subtilerer, aber genauso großer Vorteil: Es gibt Angriffe und Bedrohungen verschiedenster Art und die einzelnen Schutzebenen können jeweils für die Abwehr einer spezifischen Bedrohungsart optimiert werden. Die Verteidigung gegen einen Standardcomputerwurm erfordert z. B. andere Techniken als die gegen einen verärgerten Mitarbeiter. Der Schlüssel zur Verbesserung der einzelnen Ebenen der tiefgestaffelten Verteidigung ist zu gewährleisten, dass jede Schutzebene den Kontext der zu schützenden Informationen oder Systeme berücksichtigt.

5. TIEFGESTAFFELTE VERTEIDIGUNG: ANALOGIE AM BEISPIEL EINER BANK

Die Sicherheitsvorkehrungen in einer Bank bilden eine gute Analogie zur tiefgestaffelten Verteidigung für Steuerungssysteme. Was macht eine typische Bank sicherer als ein normales Haus oder ein Lebensmittelgeschäft? Die Bank setzt verschiedene Sicherheitsmaßnahmen ein, um höchstmögliche Sicherheit und Schutz ihrer Angestellten, Kunden und Vermögenswerte zu gewährleisten. Es gibt nicht nur mehr Schutzebenen, sondern jede Ebene richtet sich auch an ihrem speziellen Einsatzort gegen eine bestimmte Art von Bedrohung. Eine typische Bank hat z. B. Stahltüren, Fenster aus kugelsicherem Glas, Wachpersonal, Schlüssel für Bankschließfächer, Tresore und Schalterangestellte mit Sicherheitstrainings, um nur einige Sicherheitsmaßnahmen zu nennen. Banktüren sind effektive, aber einfache Sicherheitsmaßnahmen.

Entweder sind sie verschlossen oder unverschlossen. Sie gewähren oder verwehren entweder allen oder keinem Kunden den Zutritt – unabhängig davon, wie ein Besucher aussieht oder sich verhält.

Eine Schutzebene höher befindet sich das Wachpersonal – es führt eine Zugangskontrolle durch, um den Besucherstrom der Bank „sauber zu halten". Es sorgt dafür, dass nur Personen Zugang zur Bank erhalten, die einen legitimen Grund haben, dort zu sein, und sich im Rahmen der erwarteten Normen verhalten. Die Wachleute beurteilen jeden Besucher nach speziellen Kriterien, z. B. das Tragen einer Maske, verdächtiges Verhalten, zielloses Verhalten usw..

Auf einer weiteren Ebene hindern Schalterangestellte, Schließfachschlüssel, Passwörter etc. diesen bereits gefilterten Kundenstrom daran, auf andere als die ihm zustehenden Konten oder Informationen zuzugreifen. Statt sich damit zu befassen, ob ein Besucher in der Bank sein sollte oder nicht, stellen Schalterangestellte und Passwörter eine andere Sicherheitsebene dar: die Kontosicherheit. Durch die genannten Methoden wird in Abhängigkeit davon, um wen es sich handelt, „gefiltert", welche Art von Kontozugriff einzelne Kunden erhalten.

Es ist zu beachten, dass die Sicherheitsebenen kontextspezifisch sind, weshalb Banken nicht einfach weiteres Wachpersonal auf jeder Ebene einsetzen. Die Sicherheitslösung muss zum Kontext der auf dieser Ebene erwarteten Bedrohung passen.

Hintergrund:

Unter die Bezeichnung „OPC Klassik" fallen alle OPC-Standards vor Einführung des neuen Standards OPC-UA (OPC-Unified Architecture). Dazu gehören verbreitete Spezifikationen wie OPC Data Access (OPC DA), OPC Alarms and Events (OPC A&E) und OPC Historical Data Access (OPC HDA).

Weiterführende Informationen zu diesem Thema finden Sie auf der Webseite der OPC Foundation.

6. SICHERHEIT VON INDUSTRIELLEN STEUERUNGSSYSTEMEN

Was hat all das nun mit der Sicherheit im Fertigungsbereich zu tun? In der industriellen Kommunikation lassen sich die Rollen des „Bankwachpersonals" und des „Schalterangestellten" im weitesten Sinne durch „Netzwerksicherheit" und „Anwendungsbezogene Sicherheit" ersetzen. Die Firewall funktioniert in diesem Fall wie das Wachpersonal und lässt bestimmte Protokolle entweder zu oder verwehrt ihnen den Zugriff auf das Steuerungsnetz. Wie ein Bankwachmann mit mehr Erfahrung beobachten komplexere SCADA-fähige Firewalls den Datenverkehr hinter den augenfälligen Protokolltypen und treffen zusätzliche Filterentscheidungen basierend auf Verhalten und Kontext der Systeme, die diese Protokolle innerhalb des Netzwerks verwenden.

Analog kann ein OPC-Server mit einer robusten Implementierung der OPC-Sicherheit wie ein gut geschulter Schalterangestellter funktionieren. Nachdem ein Nutzer erfolgreich eine Verbindung zu einem OPC-Server herstellen konnte, sorgt die OPC-Security-Konfiguration dafür, dass er nur Zugriff auf die speziellen Datensätze erhält, die für ihn bestimmt sind. Versuche, auf Daten anderer zuzugreifen, werden idealerweise geblockt und aufgezeichnet. Wie auch in dem Wächter-/Schalterangestellten-Beispiel bilden die Firewall, die für Netzwerksicherheit sorgt, und der für die anwendungsbezogene Sicherheit zuständige OPC-Server ein essenzielles Team. Eine Firewall kann z. B. Millionen von beliebig SPAM-Nachrichten blockieren, die im Rahmen einer DoS-Attacke (Denial of Service) an einen Server gesendet werden. Gleichzeitig lässt sich durch Benutzerauthentifizierung und Autorisierungsüberprüfungen verhindern, dass ein Angreifer, der die Firewall überwunden hat, auf Prozesssollwerte in einem System zugreifen und dort Änderungen vornehmen kann, die Eigentum oder Leben in Gefahr bringen.

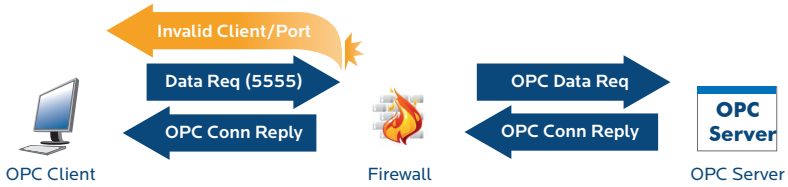
Step 1

Die OPC-Firewall fängt eine Verbindungsanfrage vom OPC-Client ab und bestätigt, ob es sich um einen genehmigten Server eines genehmigten Clients handelt, und ob es sich bei der Nachricht um eine korrekt gebildete OPC-Verbindungsanfrage handelt.

Step 2

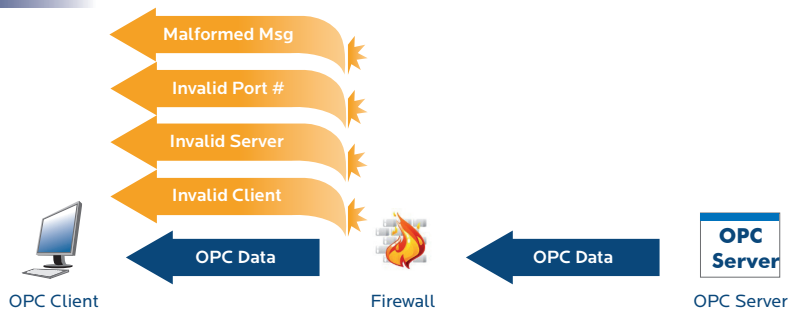
Die OPC-Firewall fängt die Verbindungsantwort vom OPC-Server ab und bestätigt, dass sie sich an den ursprünglichen Client richtet und korrekt gebildet wurde. Sie bestimmt zudem auch den neuen TCP-Port, den der Server verwenden möchte.

Step 3



Die OPC-Firewall öffnet für den Moment den in der Antwortnachricht angegebenen TCP-Port, jedoch nur für die Kommunikation zwischen diesem Client und diesem Server. Erfolgt innerhalb von wenigen Sekunden keine korrekte TCP-Sitzung, wird der Port wieder geschlossen.

Step 4



Gültige OPC-Daten fließen weiter, während SPAM-Nachrichten, Nachrichten, die ungültige Ports verwenden oder Nachrichten von ungültigen Clients oder Servern blockiert und von der Firewall protokolliert werden.

Abbildung 1 – Funktionsweise einer OPC-Firewall

7. NETZWERKBEZOGENE SICHERHEIT

Um ein grundlegendes Verständnis für netzwerkbezogene Sicherheit entwickeln zu können, muss man wissen, dass die meisten TCP/IP-Protokolle, wie z. B. Modbus-TCP, in jeder Nachricht eine international anerkannte Nummer (Portnummer genannt) mitsenden, um die Nachricht als Teil einer bestimmten höheren Protokollschicht zu identifizieren. Durch diese konsistente Protokollidentifizierung ist es für Firewalls einfach, Nachrichten bestimmter Protokolle zu blockieren oder sie passieren zu lassen. Um zum Beispiel den gesamten Modbus-TCP-Traffic zu blockieren, muss eine Firewall nichts weiter tun, als die Nachrichten zu suchen, die die Modbus-TCP zugewiesene Nummer (nämlich 502) in bestimmten Feldern enthalten, und diese dann blockieren.

Ein Standard-OPC-Server verwendet keine feste TCP-Portnummer. Der Server weist stattdessen jedem Prozess, über den er mit OPC-Clients kommuniziert, dynamisch eine neue TCP-Portnummer zu. Der OPC-Client muss diese zugewiesenen Portnummern dann herausfinden, indem er sich mit dem OPC-Server verbindet und nachfragt, welche TCP-Portnummer er für die Sitzung verwenden soll. Dann stellt der OPC-Client unter Verwendung der neuen Portnummer eine neue TCP-Verbindung zum OPC-Server her. OPC-Server können alle Portnummern zwischen 1024 und 65535 verwenden, weshalb OPC Klassik „firewallunfreundlich“ ist.

Wenn man eine herkömmliche IT-Firewall so konfiguriert, dass sie ein solch breites Spektrum an Ports offen lässt, ist es, als ließe man einen schlafenden Wachmann den Eingang einer Bank bewachen. Wenn man dagegen alle diese Ports sperrt, blockiert man auch die gesamte OPC-Kommunikation. Dennoch sind die Probleme der dynamischen Portzuweisung in OPC heutzutage kein Grund mehr, seine OPC-Server nicht durch Firewalls zu schützen. Neue OPC-fähige Firewalls können das OPC-Klassik-Problem der dynamischen Ports nun automatisch verfolgen und verwalten. Diese Firewalls lassen sich in bestehenden Netzwerken installieren, ohne Änderungen an den bereits vorhandenen OPC-Clients und -Servern vornehmen zu müssen.

Ein gutes Beispiel ist die Tofino Security Appliance von Byres Security mit dem Tofino OPC Enforcer™ – eine Sicherheitslösung mit OPC-Firewall. Derartige Lösungen sind darauf ausgelegt, in aktiven Steuerungsnetzwerken installiert zu werden, ohne dass Änderungen am Netzwerk nötig werden oder es zu Stillstandszeiten der Anlage kommt. Sie stellen einen einfachen und kostengünstigen Weg dar, in einem Steuerungssystem Sicherheitszonen zu bilden, wie sie von den Standards ANSI/ISA99, NERC CIP und IEC empfohlen werden.

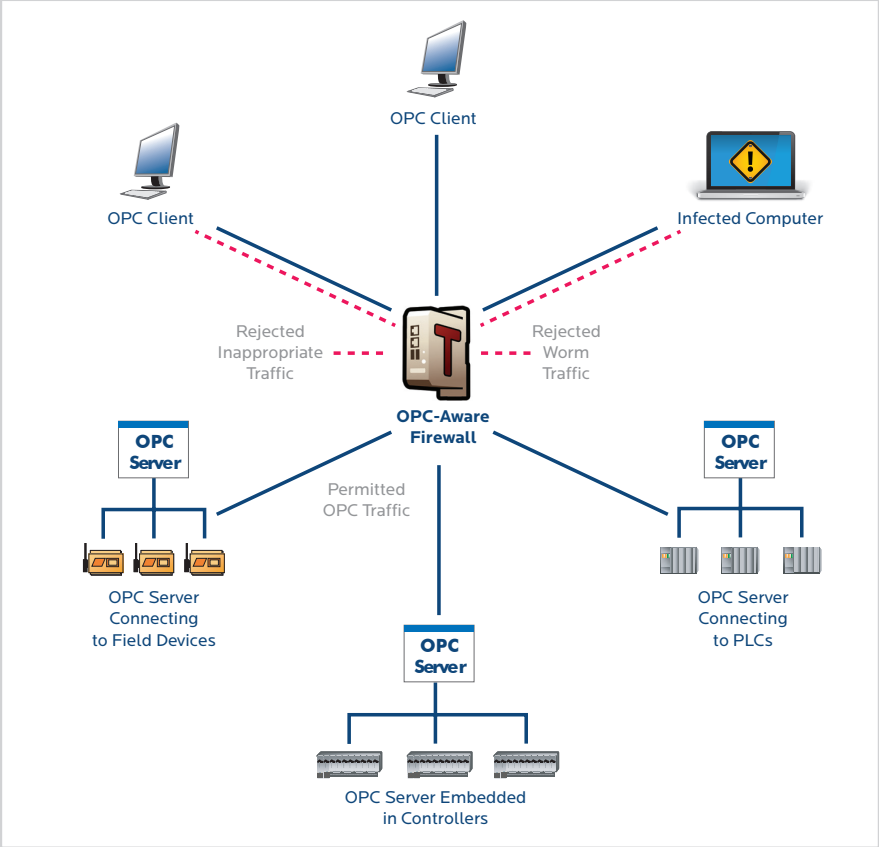


Abbildung 2 – Eine OPC-fähige Firewall schützt OPC-Clients und -Server

8. ANWENDUNGSBEZOGENE SICHERHEIT

Um zur Bankanalogie zurückzukehren: Haben Besucher einmal die Eingangstür und den Wachmann passiert, gehen sie zum Schalter, um ihre Transaktionen durchzuführen. Die Aufgabe des Schalterangestellten ist es, sowohl die gewünschten Transaktionen durchzuführen, als auch dafür zu sorgen, dass diese sich nur auf Konten erstrecken, auf die der Besucher Zugriff hat. Die OPC-Server praktisch aller OPC-Anbieter verlassen sich im Bezug auf die Sicherheit ausschließlich auf DCOM (der Wachmann an der Tür) und bieten keine speziellen Sicherheitsmaßnahmen in Form von Zugriffskontrollen (die Schalterangestellten).

Um die Sicherheit durch Zugriffssteuerung bzw. die anwendungsbezogene Sicherheit zu gewährleisten, sind OPC-spezifische Sicherheitsmaßnahmen und sorgfältig geplante OPC-Architekturen erforderlich. Mit der zunehmenden Konnektivität in Unternehmen ist eine ordentlich implementierte tiefgestaffelte Verteidigung entscheidend. Sonst kann es dazu kommen, dass Systeme, die einer stetig länger werdenden Liste von Bedrohungen ausgesetzt sind, nicht innerhalb ihrer Zielparameter arbeiten und möglicherweise kostspielige Sicherheits-, Umwelt- und Produktionszwischenfälle verursachen.

Während man sich bei vielen OPC-Installationen auf die Unternehmensfirewall und eine korrekte DCOM-Konfiguration als Schutzmaßnahme verlässt, zeigen Untersuchungen, dass offene Firewalls und freizügige DCOM-Zugriffsrechte nach wie vor verbreitete

Beispiel: OPC-Sicherheit einmal richtig!

MatrikonOPC Security Gateway basiert auf der OPC-Sicherheitsspezifikation der OPC Foundation und steuert für jeden Benutzer und für jeden Punkt, welche Anwender Elemente durchsuchen und zu Gruppen hinzufügen dürfen sowie Lese- und Schreibzugriff erhalten. Durch eine derart granulare Kontrolle über den Datenzugriff wird gewährleistet, dass die richtigen Daten an die richtigen Empfänger gesendet werden, und unbeabsichtigte oder nicht autorisierte OPC-Datenzugriffe auf OPC-Servern werden verhindert.

Indem das MatrikonOPC Security Gateway als OPC-Server der höchsten Stufe verwendet wird, kann auf Daten der darunter liegenden ungesicherten OPC-Server nur von Anwendern zugegriffen werden, die zuvor vom Systemadministrator die entsprechenden Berechtigungen erhalten haben. Ein solcher rollenbasierter Sicherheitsansatz bietet effektiven OPC-orientierten Schutz, der direkt zur gesamten Strategie der tiefgestaffelten Verteidigung eines Systems beiträgt.

Schwachstellen sind. Selbst korrekt konfigurierte Systeme bieten keine ausreichende Granularität der Sicherheitsfunktionen, um das System vollständig zu schützen. Worin liegt das Problem? Unternehmensfirewalls und die allgemeine Windows-DCOM-Sicherheit sind nicht auf den OPC-Kontext ausgelegt. Nur durch den Einsatz von speziell auf OPC ausgelegten Sicherheitsprodukten, die die OPC-Sicherheitsspezifikation unterstützen und die dadurch zur Verfügung gestellten Informationen richtig nutzen, kann ein effektives Schutzniveau gewährleistet werden.

9. SICHERHEITSOPTIONEN VON OPC-SERVERN

Bei allen OPC-Servern oder -Produkten besteht die Möglichkeit, eine von drei Sicherheitsstufen zu implementieren: kein Schutz, DCOM oder OPC-Sicherheit. Jede Stufe bietet mehr Sicherheit und Kontrolle darüber, wer Zugriff auf die Daten innerhalb der OPC-Architektur hat.

- Kein Schutz – Es werden keine Schutzmaßnahmen umgesetzt. Start- und Zugriffsberechtigungen für den OPC-Server werden jedem gewährt und Zugriffsberechtigungen für Clients bestehen ebenfalls für jeden. Der OPC-Server steuert nicht den Zugriff auf anbieterspezifische Sicherheitsfunktionen.

- DCOM-Sicherheit – Nur die Windows-DCOM-Sicherheit wird umgesetzt. Start- und Zugriffsberechtigungen für den OPC-Server sind auf ausgewählte Clients beschränkt, ebenso die Zugriffsberechtigungen für Client-Anwendungen. Der OPC-Server steuert jedoch nicht den Zugriff auf spezifischere Sicherheitsfunktionen. Dies ist die Standardsicherheitsstufe von DCOM.

- OPC-Sicherheit – Unterstützt die OPC-Sicherheitsspezifikation. Der OPC-Server dient als Referenzüberwachung und steuert den Zugriff auf spezifische Sicherheitsfunktionen, die vom OPC-Server bereitgestellt werden. Ein OPC-Server kann die OPC-Sicherheit zusätzlich zur DCOM-Sicherheit oder nur die OPC-Sicherheit allein implementieren.

10. ROLLEN- UND ANWENDERBEZOGENE SICHERHEIT

Die OPC-Sicherheitsspezifikation stützt sich auf Client-Identifizierung durch vertrauenswürdige Anmeldedaten, anhand derer der OPC-Server über die Zugriffsrechte entscheidet. So können OPC-Produkte spezielle Sicherheitskontrollen für das Hinzufügen, Durchsuchen, Lesen und/oder Schreiben einzelner OPC-Elemente bereitstellen. Im Fertigungsbereich sind für die verschiedenen Positionen der Mitarbeiter unterschiedliche Arten von Datenzugriff erforderlich:

- Steuerungssystemingenieure benötigen möglicherweise vollen Lese- und Schreibzugriff auf alle Punkte des Automatisierungssystems.

- Der Zugriff von Bedienern könnte z. B. auf Datenpunkte beschränkt sein, die mit dem Status und der Steuerung von Maschinen in ihrem eigenen Anlagenbereich in Verbindung stehen.

- Mitarbeiter aus dem Managementbereich benötigen mit großer Wahrscheinlichkeit nur Lesezugriff auf wichtige Leistungskennzahlen.

Damit die jeweils passende Zugriffsstufe zum Einsatz kommt, müssen Anwendungen verstehen können, in welchem Kontext bestimmte Anwender auf Informationen zugreifen . Die OPC-Sicherheitsspezifikation ermöglicht es OPC-Servern, Zugriffsentscheidungen aufgrund von anwenderbezogenen Informationen zu treffen, doch wie diese Informationen verwendet werden, bleibt dem OPC-Anbieter überlassen. MatrikonOPC ist der einzige Anbieter, der sich speziell darauf konzentriert zu gewährleisten, dass Anwender ihre OPC-Architekturen vollständig schützen können, indem eine robuste Implementierung der OPC-Sicherheit bereitgestellt wird, die Schutz bis hinab zur Anwender- und Tag-Ebene bietet – unabhängig davon, von welchem Anbieter die OPC-Server stammen.

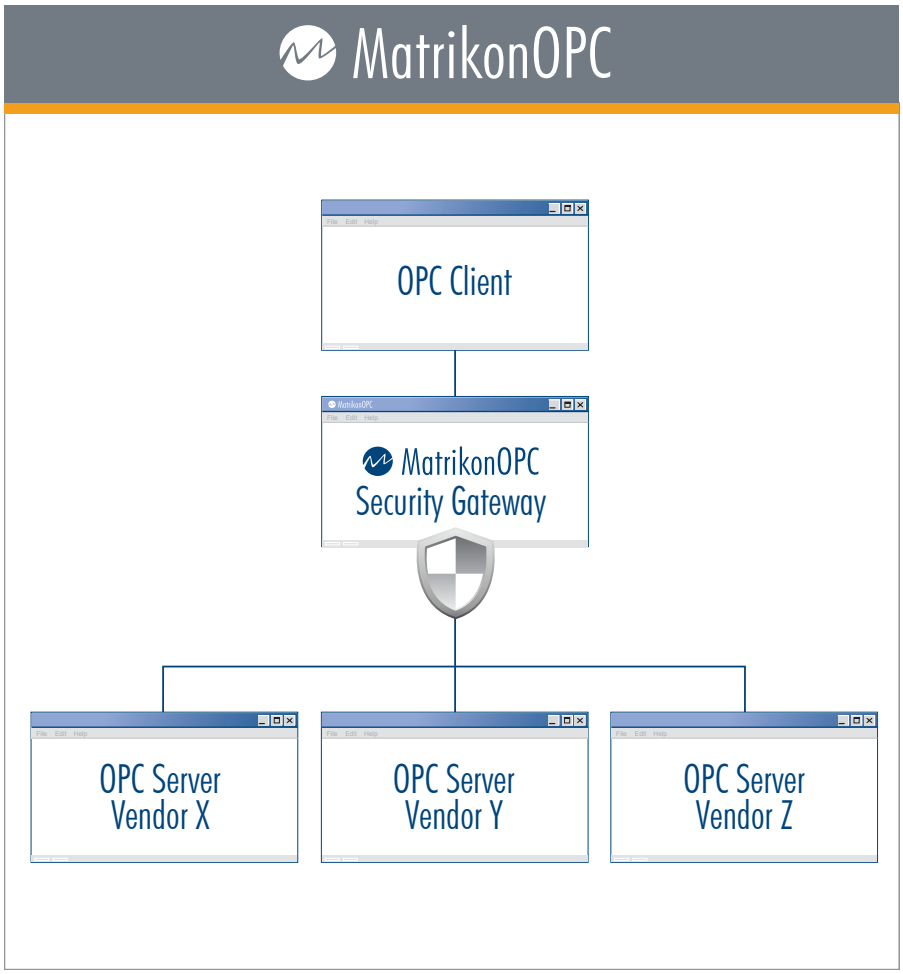


Abbildung 3 – Architektur des MatrikonOPC Security Gateway

Sicherheitstyp	Bank	Industrielles Steuerungssystem (Industrial Control System – ICS)	Beispiele für ICS-Sicherheitslösungen
Netzwerk-bezogene Sicherheit	Wachpersonal	OPC-Firewall	Tofino Security Appliance und Tofino OPC Enforcer: • Tofino Security Appliances werden installiert, um Sicherheitszonen für Gruppen von SPS, PLS und HMIs mit ähnlichen Sicherheitsanforderungen zu bilden. • Nach der Installation ist sofortiger Schutz gegeben und es sind weder Vorkonfigurierungen noch Anpassungen des Netzwerks oder Stillstandszeiten der Anlage erforderlich. • Automatische Verfolgung und Verwaltung von dynamischen OPC-Klassik-Ports; jede von einer OPC-Anwendung hergestellte Verbindung wird überprüft, verfolgt und gesichert.
Anwendungs-bezogene Sicherheit	Schalterangestellte • Bestimmen über den Zugriff auf Konten und Bargeld sowie über den Zugang zum Tresor und sogar zum Bankdirektor. • Die Effektivität dieser Schutzebene hängt davon ab, wie gut geschult und sorgfältig die Schalterangestellten sind.	OPC-Server mit OPC-Security • Bestimmen, in welchem Ausmaß OPC-Client-Anwendungen Zugriff gewährt wird. • Die Effektivität hängt davon ab, wie vollständig die OPC-Sicherheitsspezifikation vom OPC-Server-Anbieter umgesetzt wurde.	MatrikonOPC Security Gateway: • Bietet eine umfassende Umsetzung der OPC-Sicherheitsspezifikation. • Für alle Datenzugriffsentscheidungen kommen durch die OPC-Sicherheitsspezifikation zur Verfügung gestellte Sicherheitsdaten zur Anwendung – nicht nur beim Zulassen von Verbindungen. • Schützt alle OPC-Server – unabhängig davon, von welchem OPC-Anbieter sie stammen. Anwender können ihre bestehenden OPC-Infrastrukturen schützen, ohne die OPC-Server ersetzen zu müssen.
Rollen- und anwender-basierte Sicherheit	• Verschiedene Kunden haben unterschiedliche Zugriffsrechte auf ein Bankkonto. Es kann z. B. sein, dass alle Mitglieder einer Familie den Kontostand abfragen und Geld einzahlen können, dass aber nicht jeder Geld abheben kann.	• Steuerungssystem-ingenieure haben möglicherweise Lese- und Schreibrechte für alle Punkte des Automatisierungssystems, während das Management nur Zugriff auf Leistungsberichte hat.	MatrikonOPC Security Gateway: • Setzt Schutzmaßnahmen bis auf die granularste Ebene durch: pro Anwender und Tag. Die umfassendste Anwendung der OPC-Sicherheitsspezifikation. • Kontrolliert, was Anwender auf sämtlichen OPC-Servern sehen können, und erlaubt ihnen nur die Aktionen, die für sie freigegeben wurden.

Abbildung 4: Vergleich der Maßnahmen zur tiefgestaffelten Verteidigung bei Banken und Industriesystemen.

11. SICHERHEITSLÖSUNGEN, AUF DIE SIE ZÄHLEN KÖNNEN

Mit dem steigenden Bedarf an OPC-Konnektivität werden die Auswirkungen fehlender OPC-Sicherheit schnell größer. Die Vergangenheit hat gezeigt, dass viele öffentlich bekannt gewordenen Sicherheitsprobleme die unsachgemäße Anwendung von IT-Sicherheitsmaßnahmen oder deren vollständiges Fehlen zur Ursache hatten.

Sicherheitsbewusste Fachleute für Steuerungs- und Automatisierungssysteme setzen eine Kombination aus speziell auf Steuerungssysteme ausgelegten Netzwerksicherheitspraktiken, ordnungsgemäß entworfenen OPC-Architekturen und OPC-orientierten Sicherheitsprodukten ein. Durch den Einsatz der richtigen Produkte lässt sich der Schutz bestehender Systeme bedeutend verbessern, ohne dass Geräte ausgetauscht werden müssen oder eingehende IT-Erfahrung notwendig wäre. Das MatrikonOPC Security Gateway und der Tofino OPC Enforcer sind gebrauchsfertige Komponenten, mit denen die OPC-basierte Kommunikation schnell und einfach geschützt werden kann.

Denn Sicherheitszwischenfälle passieren nun einmal nicht nur „den Anderen". Clevere Unternehmen sorgen daher vor und überprüfen ihre OPC-Sicherheitsarchitektur, bevor es zu einem kostspieligen Sicherheitszwischenfall kommt.

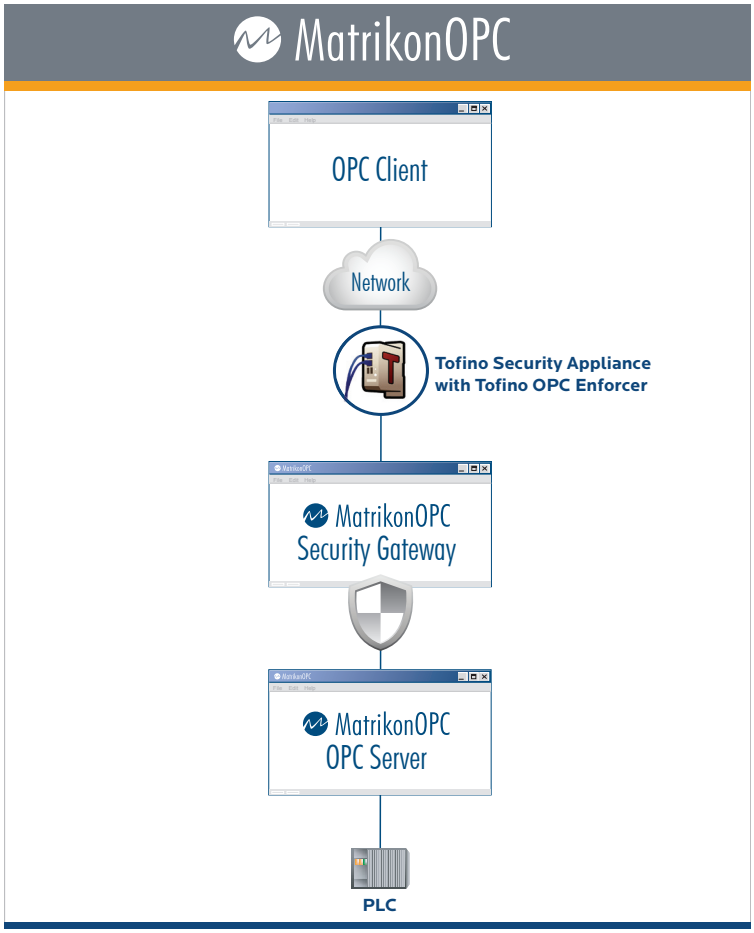


Abbildung 5 – Tofino und MatrikonOPC Security Gateway

DER NÄCHSTE SCHRITT: PROBIEREN SIE DIESE LÖSUNGEN SELBST AUS!

12. MATRIKONOPC SECURITY GATEWAY

MatrikonOPC Security Gateway unterstützt alle herstellerkonformen OPC-Server und schließt somit Sicherheitslücken in allen bestehenden OPC-Architekturen. Security Gateway ermöglicht einen konfigurierbaren Zugriff auf die OPC-Architekturen und uneingeschränkte Kontrolle für den Anwender. Der Anwender kann für jeden Tag kontrollieren, wer diesen durchsuchen, etwas hinzufügen, ihn auslesen oder beschreiben darf.

Download Security Gateway

13. DIE AUTOREN

13.1 Über Byers Security Inc.

Die Tofino-Lösung für Industriesicherheit der Byres Security Inc. schützt industrielle Steuerungssysteme und SCADA-Systeme praktisch und effektiv, ist einfach zu implementieren und erfordert keinen Anlagenstillstand. Das Modul Tofino OPC Enforcer bietet allen Systemen, die OPC Klassik anwenden, robuste Sicherheit und Stabilität. Im Gegensatz zu anderen Firewalls überprüft, verfolgt und sichert dieses Produkt jede von einer OPC-Anwendung hergestellte Verbindung und gibt nur genau den TCP-Port frei, der für den Verbindungsaufbau zwischen OPC-Client und OPC-Server benötigt wird.

Weitere Informationen finden Sie unter www.tofinosecurity.com.

„Tofino" ist ein eingetragenes Warenzeichen von Byres Security Inc.

13.2 Über MatrikonOPC

MatrikonOPC ist ein herstellerunabhängiger Anbieter von Kommunikationssoftware zur Integration von Daten auf der Basis des OPC-Standards. MatrikonOPC sichert Anwendern einen zuverlässigen Zugang zu den Prozess- und Gerätedaten aller relevanten Automationssysteme, bietet praxisnahe OPC-Schulung und liefert anspruchsvolle Kundenunterstützung. Die enge Beziehung von MatrikonOPC mit den Anwendern ermöglicht es, deren wirtschaftliche und technologische Anforderungen optimal zu adressieren. Mit seinen Niederlassungen in Nordamerika, Europa, der Asien-Pazifik-Region und im Mittleren Osten bietet MatrikonOPC lokale Präsenz auf weltweiter Basis. Für den deutschsprachigen Raum ist Köln der Hauptsitz von MatrikonOPC.

Weitere Informationen: www.MatrikonOPC.de

Tel.: +49 (221) 96977-0
Fax: +49 (221) 96977-22
Web: www.MatrikonOPC.de
E-Mail: europe@matrikonopc.com