IT-Sicherheit

# Rollenbasierte Zugriffssteuerung in Stromnetzen

Role-based Access Control (RBAC) oder rollenbasierte Zugriffssteuerung ist ein bewährtes Konzept in IT-Systemen, das von vielen (Betriebs-)Systemen zur Steuerung des Zugriffs auf die Systemressourcen genutzt wird. Es ist eine Verbesserung gegenüber dem weit verbreiteten, aber unsicheren Einzeladministrator-Gast-Modell. Statt Nutzern spezielle Zugriffsrechte zu gewähren, unterstützt RBAC das Prinzip der geringsten Rechte (Least Privilege). Dies ermöglicht die Zuordnung eines Subjekts (Nutzers) zu einer Rolle, die nur die zur Ausführung einer bestimmten Aufgabe notwendigen Rechte hat. So kann eine Organisation durch RBAC dedizierte Rechte festlegen und in bestimmten zuweisbaren Rollen zusammenfassen.

Eine rollenbasierte Zugriffssteuerung (RBAC) für die Energieautomatisierung wird bereits in mehreren Lastenheften, Standards, Richtlinien sowie in regulatorischen Anforderungen für den zuverlässigen Betrieb von Netzen berücksichtigt. Außer den Anforderungen für diese Funktionen sind auch technische Standards zur Gewährleistung der Interoperabilität entwickelt worden.

## Grundkonzept

RBAC verringert Komplexität und Kosten der Sicherheitsadministration in Netzen mit einer großen Zahl von Subjekten. Subjekte können Nutzer, Anwendungen oder Geräte sein. Die Grundidee besteht darin, Subjekten Rollen zuzuweisen, um die Zuweisung individueller Rechte zu vermeiden. In *Bild 1* ist das allgemeine Konzept von RBAC mit der Zuordnung der Subjekt-Rolle-Rechte dargestellt. Dabei ist Tom die Rolle Ingenieur zugewiesen. In dieser Rolle kann Tom Objekte anzeigen und steuern. Objekte können zum Beispiel Statuswerte oder Schaltobjekte sein.

Mit diesem Konzept kann die Verwaltung der Subjekte von der Zuweisung Rolle-zu-Rechte getrennt werden. Damit ist das flexible und zentrale Management einer eher dynamischen Zuweisung Subjekt-zu-Rolle möglich. Gleichzeitig ermöglicht es die Kombination mit einer klar definierten, eher statischen Zuweisung Rolle-zu-Rechten.

In *Bild 1* sind auch die dynamischen und statischen Zuweisungen zwischen Subjekten, Rollen und Rechten zu sehen. Wie das Beispiel zeigt, kann »anzeigen« zu den Rechten von Mary hinzugefügt werden durch Zuweisung der Rolle Ingenieur an Mary, ohne dass sich die damit verbundenen Rechte in Bezug auf Objekte dadurch ändern.

Die Sicherheitsadministration wird vereinfacht durch die Nutzung von Rollen und Vorgaben zur Organisation von Zugriffsebenen für Subjekte. Vorgaben können in diesem Zusammenhang direkt mit einer bestimmten Rolle verknüpft werden, zum Beispiel mit einer Gültigkeitsdauer oder einem bestimmten Ort, an dem die Rolle genutzt werden kann. Andere Vorgaben können sich durch die Betriebsumgebung ergeben und gegebenenfalls die Wirksamkeit einer Rolle ändern, zum Beispiel in Notfällen. Allgemein gesprochen kann RBAC die administrativen Kosten in einer Organisation senken, weil es dem Umstand Rechnung trägt, dass sich Rechte und Verantwortungen von – vor allem – Mitarbeitern öfter ändern, als eine Änderung der Rechte innerhalb von Rollen und Verantwortungen nötig ist.

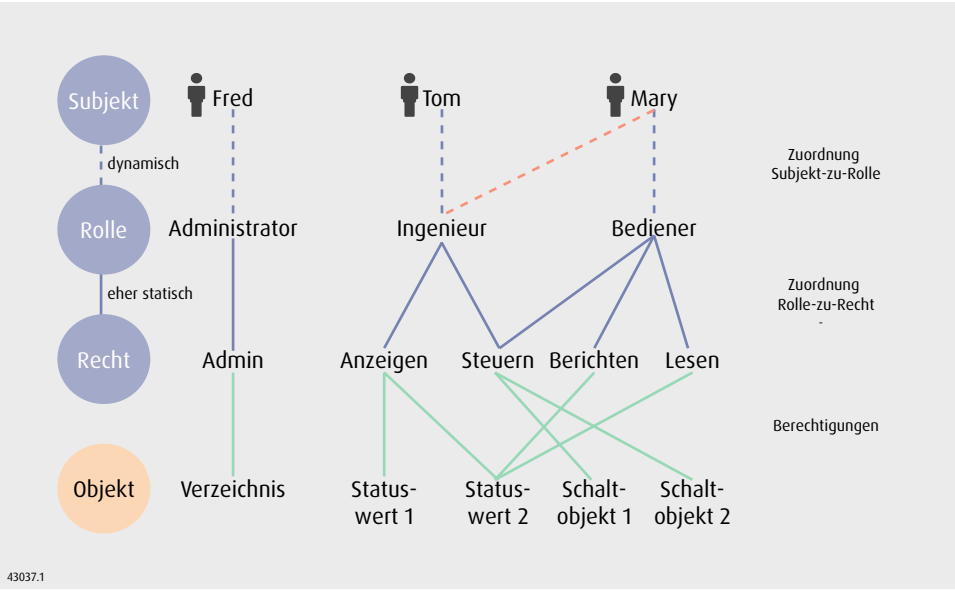


Bild 1. Zuordnung von Subjekten zu Rollen und den dazu gehörigen Rechten

## Anwendung von RBAC in der Energieautomatisierung

Um Stromnetze vor den immer häufiger auftretenden Cyberattacken zu schützen, müssen präventive, aufdeckende und korrigierende Kontrollen eingerichtet werden, die die Verantwortung und Rückverfolgbarkeit aller Handlungen beim Netzbetrieb – manuell oder automatisch, lokal oder ferngesteuert – sicherstellen. Hier kommen RBAC, Protokollierung von Sicherheitsereignissen und Nutzermanagement ins Spiel.

Damit Zugriffskontrolle, Sicherheitsprotokollierung und Nutzermanagement in der Energieindustrie wirksam werden können, müssen die besonderen Rahmenbedingungen der Branche berücksichtigt werden (*Bild 2*).

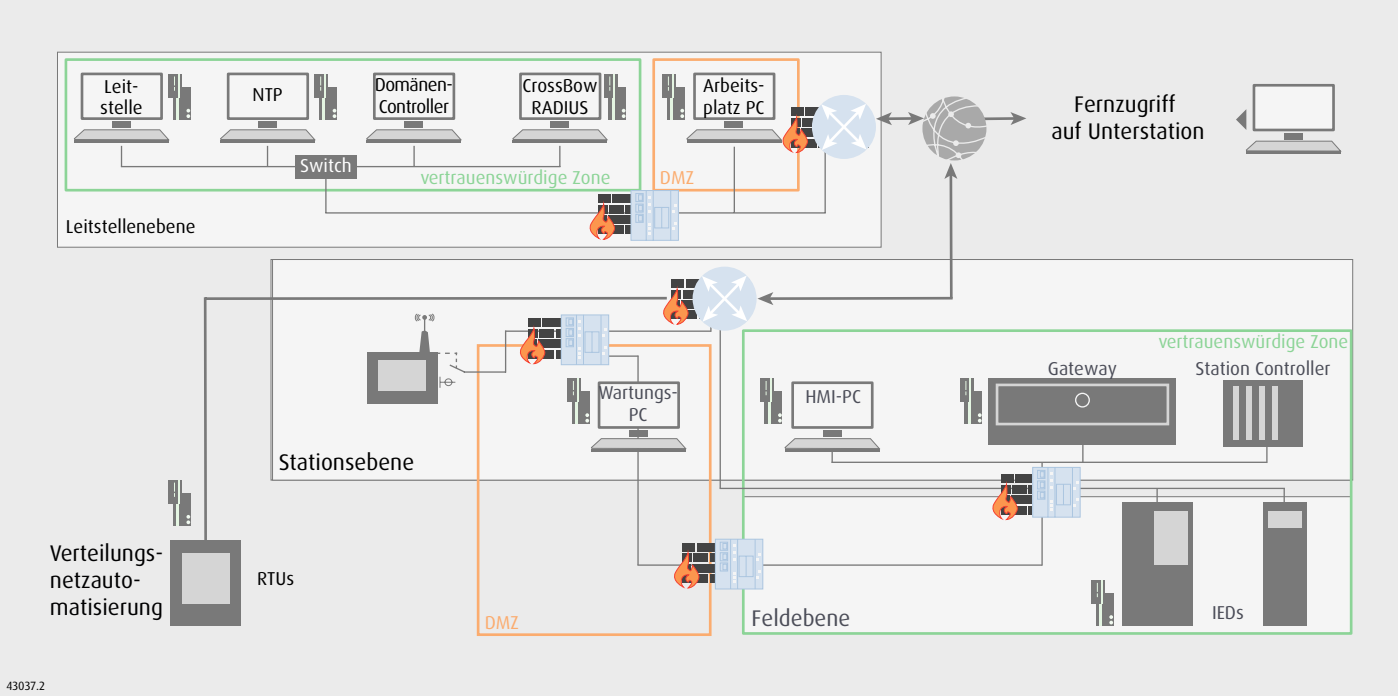


Bild 2. Beispielhafte Umsetzung von RBAC in der Energieindustrie

- große Zahl zu bedienender Unterstationen
- mehrere Rollen je Nutzer
- mehrere Anbieter von Sekundärtechnik je Unterstation
- externe Dienstleister sowie Fachpersonal des Systemintegrators brauchen Zugriff auf Betriebsmittel der Unterstation.

Obwohl RBAC in allen Phasen des Lebenszyklus einer digitalen Unterstation – von der Inbetriebnahme bis zur vollständigen Neugestaltung – eine Rolle spielt, ist die wichtigste zu beachtende Phase die Zugriffskontrolle im täglichen Betrieb. In diesem Abschnitt werden einige der gängigen Szenarios für Nutzerinteraktionen behandelt, die für den Betrieb digitaler Unterstationen typisch sind. Hervorzuheben ist, dass alle Nutzerhandlungen, die unter dem Aspekt der Systemsicherheit relevant sind, in allen Zugriffskontrollszenarien unbedingt protokolliert werden müssen. Einige der gängigen Szenarien werden hier beschrieben.

**Zugriff über HMI**

Beim normalen Betrieb in einer Unterstation wird die Prozessautomatisierung von einem Bediener mit einem PC-basierten Human Machine Interface (HMI) oder Bedien- und Beobachtungssystem überwacht und gesteuert, mit der die Zustände sowohl der primären Betriebsmitteln – zum Beispiel Leistungsschalter und Trenner – als auch der sekundären Betriebsmitteln – zum Beispiel Feldleitgerät und Schutzgerät – angezeigt und geändert werden können. Der unbefugte und anonyme Zugang zum HMI muss deshalb verhindert werden. Diese Überlegungen gelten auch für PC-basierte Runtime-Anwendungen zur Ausführung von Aufgaben der Kommunikationsschnittstelle und der Stationssteuerung und -automatisierung.

**Zugriff auf IED**

Um Einstellungen von IED – Intelligent Electronic Devices, zum Beispiel Schutzgeräten – in der Unterstation anzeigen und ändern zu können, wird normalerweise ein Engineeringwerkzeug verwendet, das mit dem IED meist über IP – bei älteren IED auch über serielle Verbindungen – verbunden ist. Dies ist auch über das im IED integrierte HMI-Bedienfeld möglich. Ein ähnliches Szenario mit Nutzerinteraktion ist das Management automatisierungs- und kommunikationsintensiver Sekundärgeräte wie Remote Terminal Units (RTU) und der dazu gehörigen Netzwerkbetriebsmittel in der Unterstation.

**Zugriff für den Abruf von Daten**

Die Erfassung von Daten für Offlinediagnosen und Netzoptimierung ist ein weiteres Szenario: Betriebsprotokolle und Abfolgen von Ereignissen sowie Abruf von Nicht-Betriebsprotokollen und Störschrieben. Heutige Power-Quality-Geräte erfassen sensible Informationen zur Netztopologie und zur Art der Einstellungen, die zum Fehler führten – zum Beispiel Transformatoreinstellungen, überwachte Abzweige und Leitungen. Alle werden im international anerkannten Comtrade-Format für Störschriebe gespeichert. Bei diesem Szenario kann der aktive Nutzer den Großteil seiner Aufgaben mit Nur-Lese-Zugriff auf die IED und die Datenarchivierungssysteme ausführen. Weitergehende, potenziell schädliche Zugriffsrechte sollten vermieden werden.

**Zugriff zum Ausführen der Updates**

Aufgrund nationaler Vorschriften sind die Betreiber von Stromnetzen verpflichtet, für alle eingesetzten Netzautomatisierungssysteme ein aktives Management der Sicherheitspatches zu betreiben. Die Zugriffsrechte, die ein Bediener vor Ort für die Durchführung von Firmware- und Softwareupdates benötigt, können von (anonymen) böswilligen Dritten missbraucht werden zur Installation korrupter, veralteter oder manipulierter Firm- und Software auf sekundären Betriebsmitteln.

**Zugriff zur Verwaltung der Datensicherung**

Die Zugriffskontrolle muss auch die regelmäßig wiederkehrende Sicherung der Einstellungen der sekundären Betriebsmittel erfassen. Bei diesem Szenario kann der aktive Nutzer den Großteil seiner Aufgaben mit Nur-Lese-Zugriff auf das System ausführen.

**Zeitweiliger Zugriff**

Besondere Überlegungen erfordert die Gewährung zeitweiliger Zugriffe auf sekundäre Betriebsmittel in der Unterstation für externe Techniker wie Dienstleister oder Fachpersonal des Sys-

**Übergreifende Zuordnung von Rollen und Rechten in IEEE 1686, BDEW-Whitepaper und IEC 62351-8**

| | | | Rollen in IEC 62351-8 und BDEW-Whitepaper sowie zusätzliche empirische Rollen | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Rechte in IEEE 1686 | Beschreibung der Rechte in IEEE 1686 | »GUEST« | [BDEW: Data display] LESER | OPERA-TOR | BDEW: BACKUP OPERA-TOR | ENGINEER | [BDEW: Operator] INSTAL-LER | [BDEW: Admin] SECADM | [BDEW: Auditor] SECAUD | RBAC-MGMT | »ADMIN« |
| IEEE-1686-Rechte | keine | allg. Inform. anzeigen | × | × | × | × | × | × | × | × | × | × |
| | view data | Betriebsdaten anzeigen | | × | × | × | × | × | | | | × |
| | view cfg settings | Konfigurationseinstel-lungen anzeigen | | × | × | × | × | × | | | | × |
| | force values | Werte setzen; Istdaten manuell übersteuern; Ausgaben veranlassen | | | × | | × | × | | | | × |
| | cfg change | Konfig. herunterladen/ ändern/hochladen | | | | ×[1] | × | × | | | | × |
| | fw change | Firmware ändern | | | | | | × | | | | × |
| | RBAC mgmt | RBAC-Management | | | | | | | × | | × | × |
| | security mgmt | Sicherheitsfkt. (außer RBAC) ausführen und managen | | | | | | | × | | | × |
| | audit trail | Audit Trail | | | | | | | × | × | | × |

[1] nur Download

Tafel 1. Übergreifende Zuordnung von Rollen und Rechten in internationalen Standards und Empfehlungen

temintegrators. Es sollte möglich sein, die Gültigkeit solcher Nutzerkonten einzuschränken und diese Konten erst zu aktivieren beziehungsweise anzulegen, wenn sie gebraucht werden.

**Rollenflexibilität**

Neben den genannten beispielhaften Szenarios gibt es weitere Szenarios mit Nutzerinteraktion, bei denen die Erstellung individueller Rollen und Rechte am besten für die Organisationsstrukturen der Netzbetreiber geeignet ist – vor allem bei vielen Mitarbeitern im Betrieb. Es ist abzusehen, dass die flexible, konsequent auf sekundäre Betriebsmittel verschiedener Hersteller anwendbare Unterstützung nutzerdefinierter Rollen unabdingbar werden wird.

**Verwaltung der Sicherheit**

Wie in den Anforderungen des BDEW-Whitepaper und in der Norm IEC 62351-8 behandelt, müssen bei Anwendung von Zugriffskontrolle und Nutzermanagement die dabei genutzten Infrastruktur und Richtlinien ständig verwaltet werden. Dazu sollte das Zugriffskontrollsystem Rollen unterstützen, die für die Verwaltung der Sicherheitseinstellungen in den sekundären Betriebsmitteln, die zentrale Nutzerverwaltung sowie das Management der genannten Betriebsszenarien mit erforderlichen Nutzerrollen und -rechte zuständig sind. Ein einfaches Beispiel für das Management der Rechte ist das Hinzufügen und Entfernen von Nutzerkonten. Ein zusätzliches Szenario ist der Abruf von Sicherheitsprotokollierungen aus sekundären Betriebsmitteln und zentralen Sicherheitsprotokollierungsservern für einen Audit Trail. Bei der Prüfung verdächtiger Aktivitäten können externe oder ausschließlich dafür vorgesehene Auditoren eingesetzt werden, die nur die Zugriffsberechtigung auf die Sicherheitsprotokollierung aus den entsprechenden Quellen und Archiven für Analysezwecke haben.

**Verfügbarkeit hat Vorrang – Zugriff in Notfällen**

Abschließend gilt, dass – auch nach Einrichtung einer Nutzerverwaltung und einer RBAC – die Bediener im Notfall Zugriff auf sekundäre Komponenten der Unterstation haben müssen, selbst wenn sie aus irgendeinem Grund nicht mit ihren Anmeldeinformationen auf die sekundären Betriebsmittel zugreifen können. Es ist nicht akzeptabel, dass die Sicherheit der Unterstation auf Kosten der Systemverfügbarkeit geht.

## RBAC mit Basisinteroperabilität

In den vergangenen zehn Jahren haben die Strommärkte weltweit, veranlasst durch Standards wie IEC 62351 und IEEE 1686 sowie regionale Organisationen von Energienetzbetreibern, wie die Nerc in Nordamerika und den BDEW in Deutschland, gemeinsam daran gearbeitet, mehr Bewusstsein für die Sicherheit der Kombination aus IT-Infrastruktur und operativer Infrastruktur (IT/OT) herzustellen.

Jedoch gibt es bei den Orientierungshilfen zu RBAC derzeit noch keine Abstimmung der Gruppen von Rollen, die von den hier genannten Standards und Empfehlungen gefordert werden. So können zum Beispiel – durch die vom Standard IEC 62351-8 derzeit festgelegten Mindestrollen, die ausschließlich auf die im Standard IEC 61850 berücksichtigten Vorgänge abgestimmt sind – einige oder sogar alle darin definierten Rechte nicht auf Betriebstätigkeiten außerhalb des Bereichs der IEC 61850 übertragen werden – zum Beispiel Berücksichtigung von Firmware-Updates. Wie in *Tafel 1* zu sehen ist, würde eine Zuordnung der in der IEC 62351-8 und im BDEW-Whitepaper festgelegten Rollen zu den verschiedenen Rechten nach IEEE 1686 diese Lücke schließen und es ermöglichen,

- eine Basisinteroperabilität von RBAC ganzheitlich zu behandeln und nicht nur aus der Sicht eines einzelnen Standards
- allen Märkten gerecht zu werden, die von den genannten Verbänden und Normenausschüssen abhängen.

Zusätzlich zu diesen obligatorischen Standardrollen ist zu beachten, dass sich die

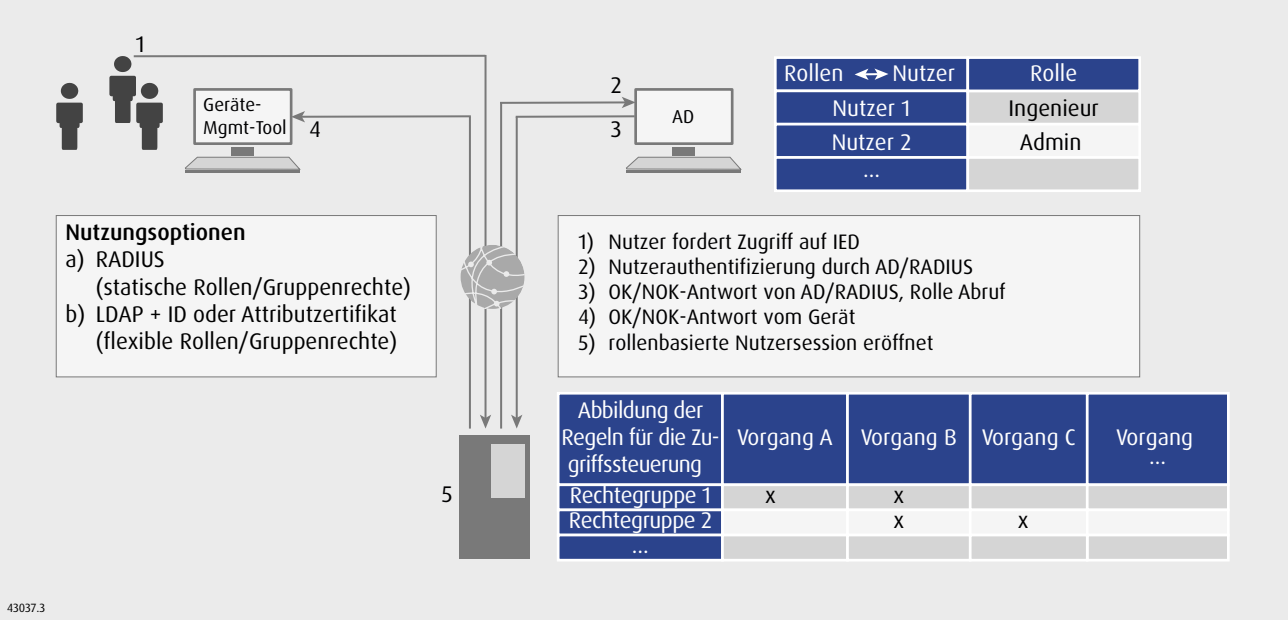


Bild 3. Verwendung von Nutzerauthentifizierung und Autorisierung auf der Grundlage offener Standards

Normungsgruppen derzeit mit der Interoperabilität nutzerdefinierter Rollen und Rechtedefinitionen beschäftigen, durch die sich Rollen besser auf eine Betriebsumgebung abstimmen lassen.

## Zukunftsperspektiven für RBAC

Mit der steigenden Zahl sekundärer Betriebsmittel, die RBAC direkt unterstützen, stellen sich auch Fragen zur Skalierbarkeit und Interoperabilität. Dazu ist es notwendig, eine interoperable, skalierbare und sichere Lösung zur übergreifenden Anwendung der RBAC bei sekundären Betriebsmitteln verschiedener Hersteller über mehrere Unterstationen zu entwickeln. Letztlich sollte es Netzbetreibern möglich sein, RBAC wirksam und mit angemessenem Betriebskostenaufwand umzusetzen und zu betreiben. Eine effektive und bewährte Methode der Realisierung ist die Verwendung von digitalen Zertifikaten.

Um Anforderungen zur Skalierbarkeit bei der IT-Betriebssicherheit gerecht zu werden, definiert der Standard IEC 62351-9 das nötige Management kryptografischer Schlüssel. Dieser Standard behandelt vor allem die Handhabung kryptografischer Schlüssel über eine Public-Key-Infrastruktur (PKI) für genau die genannten Szenarien und beruht auf dem Umgang mit X.509-basierten Zertifikaten.

Die Anwendung von Zertifikaten im Kontext der RBAC wird im Standard IEC 62351-8 definiert. Dabei werden durch eine zentrale Zertifizierungsstelle (Certification Authority – CA) X.509-Zertifikate ausgestellt, mit denen jeder Nutzer (Subjekt) identifiziert und die ihm zugeordneten Attribute wie Nutzerrolle und Verantwortungsbereiche angegeben werden. Diese Nutzerzertifikate werden bezogen auf die entsprechenden Nutzerkonten im zentralen LDAP-Server (Lightweight Directory Access Protocol) gespeichert – zum Beispiel im AD-Controller (Active Domain Controller). Beispielhaft ist hier ein Szenario für die Umsetzung dargestellt: Wenn ein Nutzer mit einem IED interagieren will, das Nutzerzertifikate verarbeiten kann, gibt er dem IED seinen Nutzernamen und sein Passwort an. Das IED stellt eine sichere Verbindung zum AD-Domänencontroller her und leitet die Anmeldeinformationen des Nutzers an den AD-Server weiter, um den Nutzer authentifizieren zu lassen. Ist das Nutzerkonto gültig, empfängt das IED das Attributszertifikat des Nutzers, in dem unter anderem dessen Rolle angegeben ist. Da die Nutzerrolle im IED vorliegt, erstellt das IED eine neue Nutzersitzung oder einen neuen Sitzungskontext, in dem die Rollenbeschränkungen angewandt werden, und ermöglicht schließlich dem Nutzer die entsprechenden Bedienoperationen. Mit diesem Ansatz wird auch die Migration von IED unterstützt, die keine Schnittstelle haben, über die der Nutzer sein eigenes Zertifikat direkt übertragen kann. Das wäre der konsequente nächste Schritt (*Bild 3*).

Die Zugriffskontrolle bleibt ein Eckpfeiler der Betriebssicherheit im Energiesektor. Präventive Maßnahmen basierend auf RBAC, Analysen des Auditierungspfads (Audit Trail), der von Nutzern ausgelösten Ereignisse und Alarme, sowie Korrekturmaßnahmen unterstützt durch eine effektive Verwaltung von Nutzerkonten verleihen dem Stromnetzbetreiber die nötigen Mittel zur Minimierung der Angriffsfläche für Cyberattacken und deren Auswirkungen – nach innen und nach außen, auf lokaler und auf Fernzugriffsebene. Anbieter sekundärer Betriebsmittel und Normenausschüsse müssen weiterhin mit den Netzbetreibern zusammenarbeiten und pragmatische, zukunftsfähige und interoperable Produkte entwickeln, die die vorhandene Technologien wirksam einsetzen. In der Zwischenzeit kommt es darauf an, Übergangstechnologien und -werkzeuge in Betracht zu ziehen, die den Einschränkungen sekundärer Betriebsmittel früherer Generationen gerecht werden, weil diese noch auf Jahre hinaus die Mehrheit des installierten Gerätebestands ausmachen werden.

Dipl.-Ing. **Steffen Fries**,
Principal Key Expert
IT-Security,
Corporate Technology,
Siemens AG, München

Dipl.-Inf. **Chaitanya Bisale**,
Product Manager, Senior Key
Expert Cyber Security,
Siemens-Division Energy
Management,
Business Unit Digital Grid,
Siemens AG, Nürnberg

>> chaitanya.b@siemens.com

>> www.siemens.com/gridsecurity

43037