SANDIA REPORT
SAND2021-0977
Printed January 2021

Recommendations for Distributed Energy Resource Access Control

Jay Johnson

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico
87185 and Livermore,
California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@osti.gov
Online ordering:	http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.gov
Online order:	https://classic.ntis.gov/help/order-methods/

ABSTRACT

Cybersecurity for internet-connected Distributed Energy Resources (DER) is essential for the safe and reliable operation of the US power system. Many facets of DER cybersecurity are currently being investigated within different standards development organizations, research communities, and industry committees to address this critical need. This report covers DER access control guidance compiled by the Access Controls Subgroup of the SunSpec/Sandia DER Cybersecurity Workgroup. The goal of the group was to create a consensus-based technical framework to minimize the risk of unauthorized access to DER systems. The subgroup set out to define a strict control environment where users are authorized to access DER monitoring and control features through three steps: (a) user is identified using a proof-of-identity, (b) the user is authenticated by a managed database, (c) and the user is authorized for a specific level of access. DER access control also provides accountability and nonrepudiation within the power system control environment that can be used for forensic analysis and attribution in the event of a cyber-attack. This paper covers foundational requirements for a DER access control environment as well as offering a collection of possible policy, model, and mechanism implementation approaches for IEEE 1547-mandated communication protocols.

ACKNOWLEDGEMENTS

The author would like to thank to the SunSpec/Sandia DER Cybersecurity Workgroup subgroup on access control and additional industry reviewers. Contributors included many industry experts: Georgios Fragkos, Pietro Calo, Tom Tansy, Ravi Sandhu, Robby Simpson, Suzanne Martinez, Aegir Jonsson, AJ Rossman, Alexander Miranda, Alfred Tom, Allyson Ugarte, Andrew Levy, Assaf Ben Or, Assaf Harel, Bob Fox, Bob White, Bret Young, Brian Noel, Candace Suh-Lee, Cuong Nguyen, Daniel Sylawa, Donald Coffin, Dylan Tansy, Dzung Nguyen, Emily Hwang, Gordon Lum, Graham Watson, Hassan Mohammed, Ifeoma Onunkwo, Ingo Hanke, Ioannis Zografopoulos, Jeremiah Miller, Jessie Deot, John Drummond, Jon Bichel, Jorg Brakensiek, Jules LaPrairie, Keith Brown, Keith Rose, Kemal Celik, Kevin Harnett, Kirk Rosener, Kyle Song, Leon-Gerard Vandenberg, Limin Huang, Matthew Hyde, Mehmet Cintuglu, Michael Cowan, Nate Diamond, Nicholas Manka, Nir Hasson, Prasanth Gopalakrishnan, Randy King, Roger Alexander, Ron Ih, Shuo Chen, Stephen Wurmlinger, Steve Peters, Tanner Kural, and Todd Davis.

This work was partially completed under the "DER Cyber Security Standards Development" project, funded by the Solar Energy Technologies Office (SETO) at the US Department of Energy (DOE).

CONTENTS

LIST OF FIGURES

This page left blank

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
ABAC	Attribute Based Access Control
AC	Access Control
Access	A specific type of interaction between a subject and an object that results in the flow of information from one to the other.
Access Control	The process of limiting access to the resources of a system only to authorized programs, processes, or other systems
ACL	Access Control List
Administrative role	A role that includes permission to modify the set of users, roles, or permission or to modify the user assignment of permission assignment relations.
AGLP	account, global, local, permission
AGUDLP	account, global, universal, domain local, permission
AI	Analog Input
AMI	Advanced Metering Infrastructure
AMP	Authorization Management Protocol
ANSI	American National Standards Institute
AO	Analog Output
API	Application Programming Interface
CIP	Critical Infrastructure Protection
DAC	Discretionary Access Control
DBMS	Database Management Systems
DER	Distributed Energy Resource
DERMS	Distributed Energy Resource Management System
DI	Digital Input
DNP	Distributed Network Protocol
DNP3-SA	Distributed Network Protocol 3 Secure Authentication
DO	Digital Output
DoD	Department of Defense
DSD	Dynamic Separation of Duty
GBAC	Graph-Based Access Control
HGABAC	Hierarchical Group and Attribute Based Access Control
HTTP	Hypertext Transfer Protocol
IBAC	Identity Based Access Control
Identity provider	An entity that creates, maintains, and manages identity information.
IEC	International Electrotechnical Committee
IEEE	Institute of Electrical and Electronics Engineers

Abbreviation	Definition
INCITS	International Committee for Information Technology Standards
IT	Information Technology
JSON	JavaScript Object Notation
JWS	JSON Web Signing
JWT	JSON Web Token
LaBAC	Label-Based Access Control
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control
MLS	Multilevel Security
NGAC	Next Generation Access Control
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
Object	A passive entity or system resource, subject to access control, that contains or receives information.
OEM	Original Equipment Manufacturer
OrBAC	Organization-Based Access Control
OT	Operational Technology
P-RBAC	Privacy-Aware Role-Based Access Control
PKI	Public Key Cryptography
PKINIT	Public Key Cryptography for Initial Authentication
PV	Photovoltaic
QoS	Quality of Service
RBAC	Role-Based Access Control
REST	Representational State Transfer
Right	A set of accessing privileges assigned to an object
Role	A job function with assigned authority and responsibility
RSBAC	Ruleset Based Access Control
RTO	Regional Transmission Organization
RuBAC	Rule-Based Access Control
SAML	Security Assertion Markup Language
SASL	Simple Authentication and Security Layer
SCRAM	Salted Challenge Response Authentication Mechanism
SC-RBAC	Smart Contract based Role-Based Access Control
SDO	Standards Development Organization

Abbreviation	Definition
SLA	Service Level Agreement
SP	Special Publication (from NIST)
SPNEGO	Simple and Protected GSS-API Negotiation Mechanism
SSD	Static Separation of Duty
SSO	Single Sign On
Subject	An active entity, person, user, machine or system interested in gaining access to an object.
SQL	Structured Query Language
TBAC	Task-Based Access Control
TCSEC	Trusted Computer System Evaluation Criteria
TLS	Transport Layer Security
TMAC	Team-Based Access Control
Token	A physical instance of “access token” (evidence of one’s right to credit, confidence, or authority)
TSO	Transmission System Operator
UCON	Usage Control
User	A human subject.
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

1. INTRODUCTION

There are approximately 2.5 million DER installations in the US now with more than 80% being smaller customer-owned systems.[1,2,3,4] These distributed, internet-connected devices play a critical role in the operation of the power system but are not subject to the same rigorous cybersecurity requirements of larger generating plants. For this reason, industry stakeholders have been working over the last few years to create several DER security recommendations, best practices, and reference solutions that can be codified by standards development organizations (SDOs).[5] This work is challenging because there are multiple entities within this ecosystem with varying roles and responsibilities and they need differing levels of access to DER data and/or DER control modes. For example, DER vendors and aggregators monitor production to advise maintenance schedules, DER-owners track their solar generation, and grid operators track production and push control setpoints to the equipment for DER-based grid services.

With so many users needing access to the equipment control settings or data, there is a need to establish robust access control security policies and technologies. Access control (AC) restricts access to resource functionality unless the user is authorized. This prevents unauthorized users from changing power system control settings—e.g., voltage/frequency ride-through and trip settings—that could compromise DER equipment or the power system.

Fundamentally, an effective access control system provides three cybersecurity functions:[6]

1. Authentication – Users must provide one or more proofs of identity to ensure they are who they claim to be. Legitimate users are either required to *know* something (username/password, key code, etc.), *have* something (access card), *be* something (fingerprints, biometric scans, etc.), or—in the case of multifactor authentication—use a combination of these items to prove their identity. Recent implementations are also incorporating geolocation techniques to authenticate legitimate users based on *where* they are.
2. Authorization – Users are permitted to access data, services, resources, or objects granted by the security policy.
3. Accountability and non-repudiation – Effective access control implementations include logging of all user activities so adversary actions can be traced or audited.

In this work, the subgroup assumed installations needed turnkey solutions and determined active management of endpoint devices was infeasible due to lack of clarity on who was responsible for cybersecurity of homeowner systems. By devising solutions for AC protections for small systems—believed to the hardest use case—workable solutions could be established for the entire DER ecosystem. Clear system requirements are needed in order to design a robust and effective DER access control ecosystem. These requirements would be documented in three abstraction levels (security

[1] T. Tansy, "Securing Distributed Energy Resources in California", S4x20, Miami South Beach, Jan 20-23, 2020.

[2] SEIA/Wood Mackenzie Power & Renewables U.S. Solar Market Insight 2020 Q2, June 11, 2020.

[3] W. Palz, The Triumph of the Sun in 2000–2020: How Solar Energy Conquered the World, CRC Press, 2019.

[4] G. Barbose, N. Darghouth, "Tracking the Sun: Pricing and Design Trends for Distributed Photovoltaic Systems in the United States, 2019 Edition," Oct 2019.

[5] J. Johnson, I. Onunkwo, D. Saleem, "DER Cybersecurity Standards Development," 2020 DOE SETO Peer Review, 6 Apr. 2020.

[6] Rescorla, E., Lebovitz, G.: A survey of authentication mechanisms version 7. Internet-draft, Internet Engineering Task Force, February 2010, URL: http://tools.ietf.org/search/draft-iab-auth-mech-07

policy, security model, and security mechanism) with specifics agreed upon by the stakeholders. They are defined as:[7]

- **Security policy** defines the high-level rules according to which access control must be regulated. Often, the term "policy" is also used to refer to particular instances of a policy—actual authorizations and access restrictions to be enforced (e.g., "DER owners can read DER measurement data").
- **Security model** provides a formal (mathematical) representation of the access control security policy and its working principals. The formalization permits the proof of properties on the security provided by the access control system being designed.
- **Security mechanism** defines the low-level (software and hardware) functions that implement the controls imposed by the policy and is formally stated in the model.

Each of these topics is covered in this paper. The types of security models are presented in Chapter 2. Constraints and considerations for a DER access control security policy are presented in Chapter 3. Security mechanisms are covered in Chapter 4 for a RBAC implementation along with proposed networking architectures for the IEEE 1547 protocols. Lastly, Chapter 5 presents unanswered issues and conclusions.

[7] S. De Capitani di Vimercati, "Access Control Policies, Models, and Mechanisms," in: H.C.A. van Tilborg, S. Jajodia, (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA, 2011.

2. ACCESS CONTROL MODELS

There are many different access control models. While each is designed to protect access to information or equipment in collaborative ecosystems, they vary in implementation complexity, management requirements, and control fidelity.[8] In this section, multiple access control models are presented that may be applicable to DER communication environments.

2.1. Mandatory Access Control (MAC) & Discretionary Access Control (DAC)

MAC and DAC were developed in the 1960s and 1970s for DoD applications. These logical access control mechanisms were documented in the DoD Trusted Computer System Evaluation Criteria (TCSEC) and defined in NIST SP 800-53 Rev 4[9]. MAC is a uniformly enforced policy for all subjects and objects within an IT boundary, e.g., a classified database. A subject that has been explicitly granted access by an administrator has the organization-defined permissions to perform operations on objects within the system boundary. This access control methodology, like Multilevel Security (MLS), uses administrators to establish organization-wide trusted subjects.

DAC is much like MAC except that it does not use a security policy administrator to universally control access and subjects can override permissions. DAC subjects can override permissions for objects they own but not change the access type for data owned by someone else. This ability to grant privileges to other subjects is not present in a MAC model. DAC uses subject identities and groups to restrict access to objects. DAC is common in Unix/Linux systems where users/groups have associated read-write-execute permissions. Unfortunately, both MAC and DAC suffer from high overhead costs when there are regular changes to the AC policy. A representation of these models is shown in Figure 1.

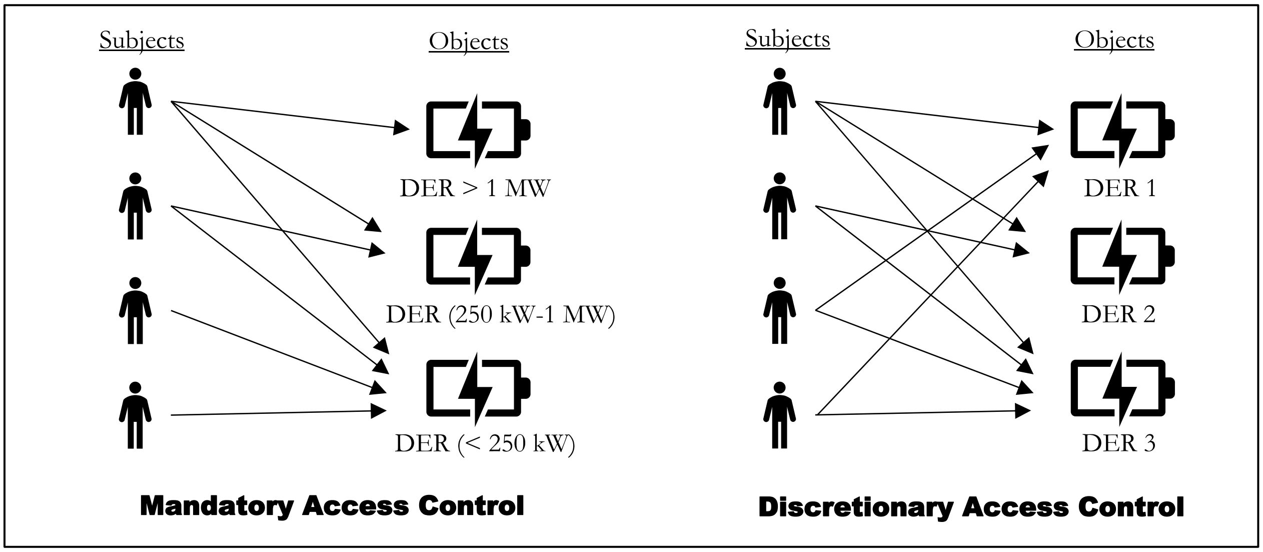


Figure 1: MAC and DAC Model Representations.

[8] V. Suhendra, A Survey on Access Control Deployment. In: Kim T., Adeli H., Fang W., Villalba J.G., Arnett K.P., Khan M.K. (eds) Security Technology. SecTech 2011. Communications in Computer and Information Science, vol 259. Springer, Berlin, Heidelberg.

[9] NIST SP 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

2.2. Identity Based Access Control (IBAC)

Identity Based Access Control—often represented with Access Control Lists (ACLs)—are an AC model where permissions are applied at the discretion of the owner and typically represent a direct mapping from user to permissions. Individual privileges allow the subject/user to read, write, edit, delete, other otherwise operate on the object. This approach places substantial workload on the object owner because they must create the rules for each user based on the access control policy, and update these rules whenever there is a change in the subject, object, policy, etc. Notably, MAC and DAC are a form of IBAC, and DAC often uses ACLs to store access permissions.

2.3. Role-Based Access Control (RBAC)

Formalized by NIST researchers in 1992 and standardized in ANSI INCITS 359-2012,[10] Role-Based Access Control places a role abstraction between subjects and objects.[11] RBAC greatly simplifies access control administration in large organizations and has been shown to reduce access control implementation costs.[12] In RBAC, each subject is assigned one or more roles (e.g., "DER installer", "utility engineer", etc.), and each role is assigned a collection of privileges. A simple "flat" RBAC system is shown in Figure 2 where the utility engineers can access all three of the DER, the DER vendor only can access two DER, and the DER owner can only access their own equipment.

It is also possible to create Hierarchical RBAC, Constrained RBAC, and Symmetric RBAC environments as well.[13] In Hierarchical RBAC, there are supporting roles (junior and senior staff) where the senior members inherit the permissions of the juniors, but not vice versa. In Constrained RBAC, conflict of interest issues and the risk of fraud or malfeasance are reduced by creating an explicit separation of duties that spread authority to take actions over multiple subjects. Symmetric RBAC provides additional organizational oversight by identifying and reviewing roles-to-rights assignments. INCITS 359 provides options for Static Separation of Duty (SSD) based on subject-role assignments and Dynamic Separation of Duty (DSD) based on role activation.

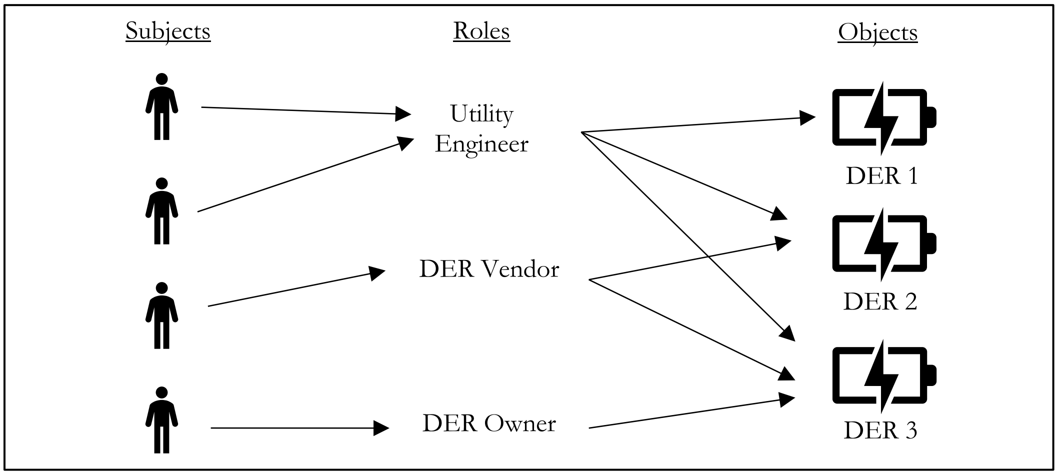


Figure 2: RBAC Model Representation.

[10] INCITS 359-2012, "Information Technology - Role Based Access Control," 2012.

[11] D. Ferraiolo (NIST), R. Kuhn (NIST), "Role-Based Access Controls," Proceedings of the 15th National Computer Security Conference, pp. 554-563, Baltimore, Oct 13-16, 1992.

[12] M.P. Gallaher, A.C. O'Connor, N. Kropp, "The Economic Impact of Role-Based Access Control," RTI Report, March 2002.

[13] R. Sandhu, D. Ferraiolo, R. Kuhn, "The NIST Model for Role-Based Access Control: Towards A Unified Standard,"

2.4. Attribute Based Access Control (ABAC)

ABAC defines access control policies with logical relationships between subjects, objects, requested operations, and other environmental conditions. NIST Special Publication (SP) 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations,[14] defines ABAC mechanisms in detail. In short, the advantage of ABAC is the administrators can create control policies without knowing the users and adding new users is more straightforward. Each of the operation/object pairs for each subject or role do not need to be created *a priori* and the ABAC engine can grant or deny permission based on the assigned attributes, the access control policy, and environment conditions, as shown in Figure 3. There are two primary types of ABAC definitions—logical formulas and relations—as described below.

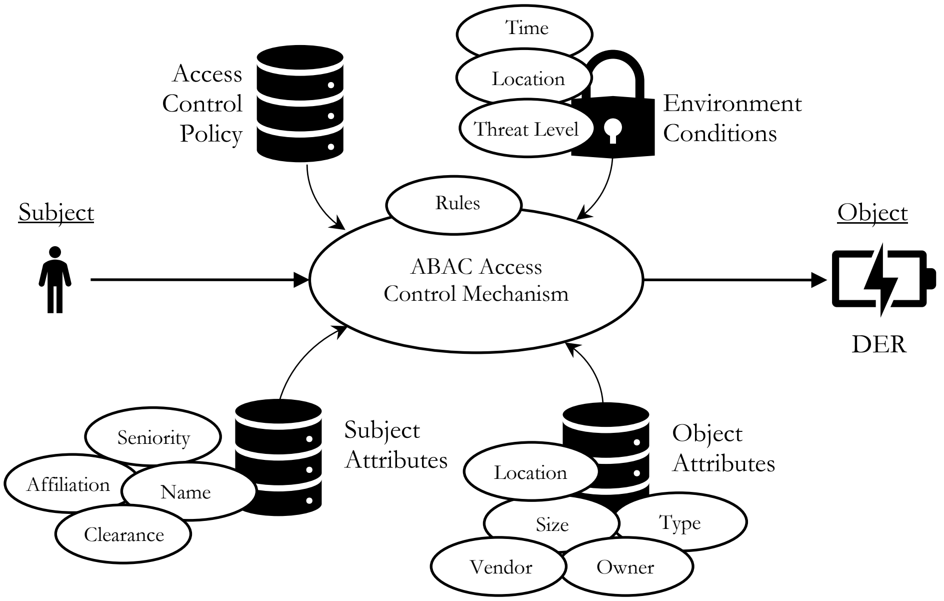


Figure 3: ABAC Model Representation.

2.4.1. Logical Formulas

ABAC can be defined using logical formulas. For instance, Role(u) = "INSTALLER" AND Region(u) = Region(o) AND (a = read OR a = write) indicates that any user (u) with a role of installer can read or write to any object (o) where the region of the user is the same as the region of the object. These logical building blocks can be encoded using eXtensible Access Control Markup Language (XACML). Some access control models of this type include Hierarchical Group and Attribute Based Access Control (HGABAC) and ABAC$_\alpha$.

2.4.2. Relations

Another type of ABAC is one that builds rules from configurations of relations of assignments, associations, prohibitions, and obligations. Access is granted to certain operations through

[14] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone, "NIST Special Publication 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, Jan 2014 with updates from Aug 2019.

associations defined by user attributes, object attributes, and access rights sets. Each user has a set of attributes that are created based on their job (e.g., John Smith is a protection engineer with Southern California Edison). Objects also have attributes assigned by the owner (e.g., the 3 kW inverter at 123 Main St is on Feeder 2034 and compliant to IEEE 1547-2018). To be granted access there must exist a mapping from an operation and argument sequence pair to a set of access rights and policy element pairs.[15] As an example, one rule may be that all utility protection engineers can configure the voltage trip setpoints on IEEE 1547-2018-compliant DER on Feeders 2000-3000. Some examples of these models include Next Generation Access Control (NGAC) and Label-Based Access Control (LaBAC).

2.4.3. Encoding

ABAC has two common encoding formats: OASIS eXtensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC). The XACML architecture is shown in Figure 4. XACML subject, resource, action, and environment attributes are defined as name-value pairs. Whereas NGAC defines ABAC expressions and policy enforcement rules using standardized and generic sets of reusable relations/functions. Both are discussed in detail by Ferraiolo et al.[16] Notably, these encodings are highly versatile and could be used for other models, including RBAC, and reference XACML and NGAC models could be established for DER environments.

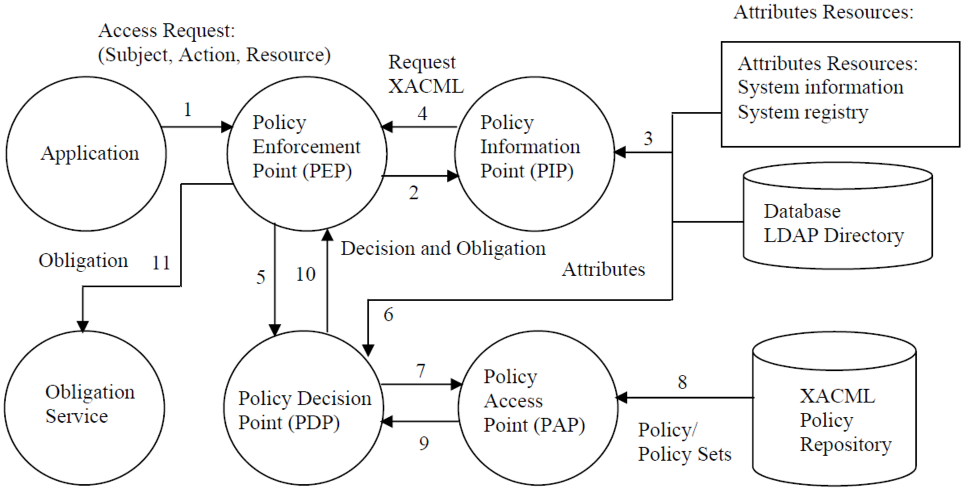


Figure 4: XACML Architecture.[17]

2.5. Other Access Control Models

There are many other access control models presented in the literature—most of which extend well known MAC, DAC, RBAC, or ABAC models in some way.[18] They span from conceptual to

[15] D. Ferraiolo, R. Chandramouli, V. Hu, R. Kuhn, "NIST Special Publication 800-178, A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC)," Oct 2016.

[16] D. Ferraiolo, R. Chandramouli, R. Kuhn, V. Hu, Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC), Proceedings of the 2016 ACM International Workshop on Attribute Based Access Control, New Orleans, Louisiana, pp. 13-24, March 11, 2016.

[17] V. Hu, D. Ferraiolo, R. Kuhn, NISTIR 7316, Assessment of Access Control Systems, Sept 2006.

[18] R. Sandhu, "Attribute-Based Access Control (ABAC)," University of Texas at San Antonio CS 5323 Lecture 5 Class Notes, URL: https://profsandhu.com/cs5323_s17/L5.pdf

rigorously-defined implantations. A noncomprehensive list of additional models is included here to illustrate the variety of AC models:

- **AGUDLP** ("account, global, universal, domain local, permission") – Windows Active Directory RBAC implementation. **AGLP** ("account, global, local, permission") is the Window NT domain equivalent.
- **Rule-Based Access Control (RuBAC)** – a generic model applied to systems with organization-defined rules, typically using a security label system which dynamically creates rules defined in a security policy. Label are attached to all objects, e.g., files, directories, devices.
- **Graph-Based Access Control (GBAC)** – organizational graphs are used with organizational query languages to define permissions on accounts, files, documents, or other objects.
- **Context-Based Access Control** – used in firewalls to filter TCP/UDP traffic using protocol information and deep packet analysis.
- **Content-Based Access Control** – applicable to digital libraries and distributed systems, dynamic user rights change with each login based on their qualifications and characteristics.
- **Organization-Based Access Control (OrBAC)** – a form of RBAC where security policy is defined per organization.
- **Team-Based Access Control (TMAC)** – RBAC where subjects with different roles form teams to collaborate on objects.
- **Ruleset Based Access Control (RSBAC)** – An open-source RBAC implementation for Linux kernels.
- **Task-Based Access Control (TBAC)** – Sequential steps or tasks are used to define access control. The permissions dynamically change with each step state.
- **Lattice-Based Access Control** – Label-based MAC where a lattice defines the security levels of objects and subject rights. Mathematically identical to **Label-Based Access Control (LaBAC)** or RuBAC.
- **Cryptography-Based Access Control** – relies completely on cryptography for access. Subjects are provided with the object key for data access. There are many forms of Cryptography-Based Access Control.[19]
- **Privacy Preserving-Based Access Control** – Tokens are generated that do not uniquely identify the subject but authorize a set of rights.
- **Privacy-Aware Role-Based Access Control (P-RBAC)** – RBAC that protects personally identifiable information or other sensitive information.[20]
- **Usage Control (UCON$_{ABC}$)** – An access control methodology that is applied after the object is distributed. The Authorizations (A), oBligations (B), and Conditions (C) represent the inputs into the decision process. UCON provides a means to provide Digital Rights Management (DRM).[21]
- **Hierarchical Group and Attribute-Based Access Control (HGABAC)** – ABAC with hierarchical user and object attribute groups.

[19] H. A. Maw, H. Xiao, B. Christianson and J. A. Malcolm, "A Survey of Access Control Models in Wireless Sensor Networks," J. Sens. Actuator Netw, Vol. 3, No. 2, pp. 150-180, 2014.

[20] Qun Ni, Elisa Bertino, Jorge Lobo, Carolyn Brodie, Clare-Marie Karat, John Karat, and Alberto Trombeta. 2010. Privacy-aware role-based access control. ACM Trans. Inf. Syst. Secur. Vol. 13, No. 3, Article 24, July 2010.

[21] J. Park, and R. S. Sandhu, The UCON$_{ABC}$ usage control model. ACM Trans. Inform. Syst. Secur. Vol. 7, No. 1, pp. 128—174, 2004.

- **Role-Based Access Control Areas of Responsibility ($RBAC_{AOR}$)** – Flat RBAC model for smart grid applications with regional division of critical assets.[22]
- **Smart Contract based RBAC (SC-RBAC)** – A decentralized RBAC model for Decentralized Applications (DApps) that minimizes the risk of a single point of failure.[23]

[22] D. Rosic, U. Novak, S. Vukmirovic, "Role-Based Access Control Model Supporting Regional Division in Smart Grid System," 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks, Madrid, 2013, pp. 197-201.

[23] Yi Ding, "SC-RBAC: A Smart Contract based RBAC Model for DApps." International Conference on Human Centered Computing. Springer, Cham, 2019.

3. DER ACCESS CONTROL POLICY REQUIREMENTS

It is difficult to define a concise AC policy for DER because there are many permutations of subjects, objects, and communication paths that may exist—even simultaneously. Data connections run from several users and roles to DER equipment, DER gateways, DER site controllers, aggregators, DER vendors, etc. and each of these endpoints must support the AC mechanisms. Additionally, the diversity in device endpoints (utility-owned DER, residential systems, commercial DER with site controllers, etc.) and interfaces (supporting IEEE 2030.5, IEEE 1815, SunSpec Modbus, proprietary protocols, local DER communications, site controllers, AMI routed traffic, etc.) each have their own operating constraints.

An DER AC security policy needs to be established in order to select the AC model and build the rules into hardware and software (via security mechanisms). The primary element of this policy would include permissions each subject/user/role has on the objects. In order to better define these policy constraints, an investigation of stakeholder roles and responsibilities, rights, and permission administration considerations was conducted to precipitate implementation requirements and constraints. These parameters were used to establish recommendations in Chapters 4 and 5. Additionally, supporting policies should be established for a broader DER cybersecurity defense-in-depth strategy, including:

- identification of critical AC assets and requirements for securing these assets
- limitations on passwords and other cyber hygiene requirements based on the criticality of the asset
- identification of any monitoring technologies employed on the access control system
- security requirements preventing unauthorized physical access of AC equipment

3.1. Roles and Responsibilities

Establishing requirements for access control is challenging because the interactions and roles of many of these users, organizations, and regulators are changing rapidly. Futureproofing an AC implementation requires the ability to adjust AC policy and AC rules dynamically. Here we list many players in the DER AC ecosystem with their assets, DER access points, and grid, cyber, and other responsibilities. By mapping roles to ownership and responsibilities to access control roles, certain patterns emerge in the communication network. This can be used to help answer big questions about who should act as the arbiter for access and be responsible for managing the AC ruleset.

- DER Owners (Homeowners)
    - Ownership: DER equipment
    - DER Access: through local interfaces (Wi-Fi, Zigbee, Ethernet, Front Panels, etc.) or DER vendor/aggregator portals
    - Grid Responsibility: none
    - Cyber Responsibility: they pass cybersecurity responsibilities to DER vendor/aggregator through formal agreement
    - Other: maintain DER equipment, keep DER connected to the internet (as required in certain jurisdictions)
- DER Owners (Corporations)
    - Ownership: DER equipment

  - DER Access: DER vendor/aggregator portals or separate cellular connections (4G/5G)
  - Grid Responsibility: none
  - Cyber Responsibility: DER management
  - Other: maintain DER equipment
- DER Vendor (Original Equipment Manufacturer)
  - Ownership: none, after sale
  - DER Access: often direct proprietary communications
  - Grid Responsibility: none
  - Cyber Responsibility: patch firmware in DER (as contracted by the DER owner)
  - Other Responsibilities: maintenance of vendor-owned DER systems (as contracted by the DER owner)
- Gateway Vendor
  - Ownership: none, after sale of gateway
  - DER Access: none
  - Grid Responsibility: none
  - Cyber Responsibility: provide users/operators with patches for gateway
  - Other Responsibilities: none
- DER Service Provider (maintainer or operator of the equipment)
  - Ownership: owner/aggregator/utility APIs, DER control servers
  - DER Access: direct proprietary communications or standardized interfaces
  - Grid Responsibility: none
  - Cyber Responsibility: patch firmware in DER/gateway, establish access control mechanisms for DER devices/gateways
  - Other Responsibilities: maintenance of vendor-owned systems (as contracted by a single home- or business owner)
- DER/Gateway Installer (typically either the OEM or service provider)
  - Ownership: none, after sale
  - DER Access: direct access to the devices through local interfaces (Wi-Fi, Zigbee, Ethernet, Front Panels, etc.) to configure them for local interconnection standards and communications backhaul protocols
  - Grid Responsibility: none
  - Cyber Responsibility: patch equipment and secure equipment in accordance with OEM/service provider
  - Other Responsibilities: none
- Utilities/Grid Operators
  - Ownership: power and networking equipment, DERMS, IEEE 2030.5 servers
  - DER Access: they (will) have legislated access to DER control features through interconnection standards and grid codes. Access is provided through SunSpec Modbus masters, DNP3 masters, IEEE 2030.5 servers, or DER vendor/aggregator portals
  - Grid Responsibility: responsible for power system operations—of which DER are a growing component
  - Cyber Responsibility: cybersecurity responsibilities are defined in North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)

    regulations but utilities have indicated they will not take responsibility for assets they do not own
  - Other Responsibilities: maintenance of utility-owned systems
- Aggregators (grid service providers, virtual power plant operators)
  - Ownership: control servers, utility- and DER-facing interfaces/APIs
  - DER Access: either directly through standardized communication interfaces or DER vendor portals
  - Grid Responsibility: as delegated by the utility to manage/control DER assets
  - Cyber Responsibility: protection of their equipment (servers), utility- and DER-facing interfaces/APIs, etc.
  - Other Responsibilities: none
- ISO/RTOs
  - Ownership: bulk system control equipment
  - DER Access: indirectly through utilities or DER vendors/aggregators. They require DER monitoring to measure and forecast renewable and DER generation/load for bulk power balancing.
  - Grid Responsibility: management and control of the transmission grid
  - Cyber Responsibility: per NERC CIP
  - Other Responsibilities: none

As exposed in the above list, many subjects establish their connections via DER service providers, who may double as the DER vendor or DER aggregator. As a central point for many communication pathways to DER equipment, and with utilities disinterested in creating security solutions for assets they do not own, it is natural to consider AC solutions that place the identity server or other access control mechanisms within the jurisdiction/domain of the DER service provider.

3.2. Rights

Rights for DER devices and servers are less complicated than, e.g., operating systems, because there is limited functionality exposed to the subject. For instance, IEC 62351-8 includes rights for dataset management and manipulation, reporting, file reads and writes, file management, object control, object configuration, creating/editing/deleting settings groups, and adjusting server or service security settings. Cybersecurity requirements in IEEE Std. 1686 for Intelligent Electronic Devices include AC password requirements, minimum numbers for individual users, and a list of rights that include viewing data/configuration files, modifying data/configurations, changing firmware, and RBAC managements and audit rights. In the case of SunSpec Modbus and IEEE 1815, much of this functionality does not exist natively in the protocol, so defining those rights are not necessary. In the case of IEEE 2030.5, because profiles can be established in the server, a more sophisticated breakdown of rights could be necessary for the user-interface to the server. Suggested rights for the IEEE 1547 protocols are shown below:

- SunSpec Modbus
  - Read – read Modbus holding register
  - Write – write value to Modbus holding register
- IEEE 1815
  - Read – read analog input (AI) or digital input (DI) outstation point
  - Write – write to analog output (AO) or digital input (DO) outstation point
- IEEE 2030.5

- Read – the RESTful protocol allows GET HTTP actions
- Write – the RESTful protocol allows PUT/POST/DELETE HTTP actions

Again, note that in the case of IEEE 2030.5, the AC mechanism is likely applied on the backend server API. This is a non-standardized configuration interface so the range of rights available for the subject will vary between server vendors. By definition, RESTful protocols like IEEE 2030.5 may allow POST (create) and DELETE (remove) HTTP actions. These are commonly used to create or remove DER EndDevice, DERControls, etc. in the DER service provider client/utility server interactions. Details are provided in the Common Smart Inverter Profile.[24] Beyond the IEEE 2030.5 DER function set, AC policies should also be defined for IEEE 2030.5 group management functions. The grouping functions are not considered in this report.

In some cases, it may be possible to add a "view" right so that the subject cannot discover or see what objects are present in the DER. Ideally, this would be applied to all DER objects for which a subject does not have read access. Further, an "Execute" right could be added for these protocols, which would be the same as a write, but to a holding register, digital output, or server interface that enables or disables a DER control mode.

A suggested Roles-to-Rights map for IEEE 1547-2018 DER functionality is included in Appendix A. This mapping covers read and write permissions.

3.3. Permission Administration

In most AC implementations, subject privileges are assigned by a centralized access control system. This system may have rules established by a single administrator for smaller organizations, but as the size of the organization grows, AC rules can be created through administration delegation to additional administrators.

DER access control administration is challenging because there are many organizations that need access to DER controls or data. It is likely that some organizations will have separate connections to the DER equipment with their own AC mechanisms. For instance, utilities may connect to DER equipment directly, while DER vendors connect to patch their firmware, while a homeowner inspects production data locally. In other cases, it may be possible to create a federated AC system where access is granted from a single server/service. This would likely be implemented by routing all utility/aggregator DER control and monitoring requests through a DER vendor and having DER owners access their production data through the same authentication mechanism.

In either scenario, there is a large administrative burden placed on each of these organizations to manage the configuration of users, roles, and rights. To help with this overhead, delegated administration can be used to assign users roles. As an example, Figure 5 illustrates a federated AC system where rules are created and managed by administrators for each organization. By creating one or more administrator roles for each of the organizations or sub-organizations (e.g., West Coast DER Service Provider Branch), a single entity is not required for maintaining the entire access control ruleset. Unfortunately, this does increase the risk of bad actors in these organizations compromising the entire system. However, by limiting the authority of each of the administrators to a subset of the

[24] Common Smart Inverter Profile: IEEE 2030.5 Implementation Guide for Smart Inverters. Version 2. Technical Report, 2018.

AC administrative control functions (e.g., they can only enroll/remove users in their organization's roles), this risk is minimized.

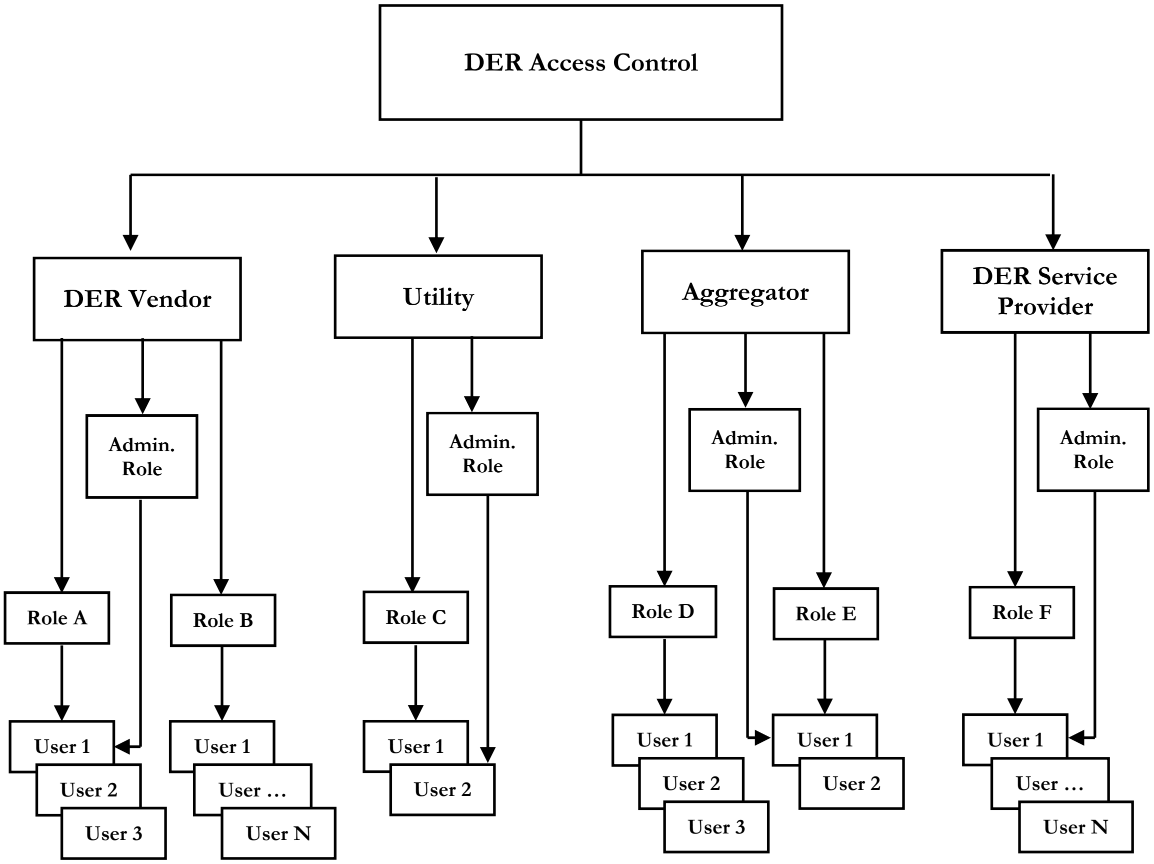


Figure 5. DER Access Control with Administration Delegation.

It seems possible that administrator roles could be configured for stakeholder groups or organizations (utilities, RTO/ISOs, DER vendors, homeowners, etc.), who would be responsible for enrolling and dis-enrolling users with permissions associated with their role. These administrative roles would be limited to assign roles for which they oversee in order to minimize insider threats. For especially large organization, the administrative role may be further disseminated. For instance, a DER service provider may have one administrator that enrolls new DER owners as their PV systems come online for a given region, while another person in the organization is responsible for enrolling DER installers or maintenance personnel.

4. ROLE-BASED ACCESS CONTROL MECHANISMS FOR DER

Role-Based Access Control is a natural choice for DER communication environments because there are clear roles for subjects based their company of employment, job position, and responsibilities. RBAC has also been used and standardized (IEC 62351-8) for AC of power system equipment so there is precedence for using that model for other grid-connected resources. That said, alternative AC models should be explored in the future to determine if other approaches reduce management overhead or provide greater security or versatility.

Establishing an RBAC mechanism for DER, required detailed information on the hardware and software required for the deployment. This would include a list of applicable access control standards (e.g., database formats, communication protocols, etc.) and permitted access control mechanisms/algorithms for identification, authentication, and authorization. Allowable interfaces for each element in the AC trust chain must be defined with clear requirements around acceptable operating systems, APIs, and AC tools/software/firmware. These requirements, based largely on the IEC 62351-8 RBAC implementation, are covered below.

4.1. Authentication and Authorization Mechanisms

Authentication is used to verify the identity of a subject. There are a few different options for authentication in AC environments including:

- Challenge-response authentication protocols, where the resource/object owner issues a challenge and the response must match a known pattern. A simple example is a CAPTCHA, through most use cryptographic techniques like the Salted Challenge Response Authentication Mechanism (SCRAM).
- Kerberos is a mutual client-server authentication mechanism for large, heterogeneous networks that is like challenge-response authentication except that is uses a third party for authentication ticket verification. The Kerberos security server acts as a trusted third party that enables hardware or software (principals) to trust other principals on the network. Kerberos is typically used in enterprise/local LANs, but Kerberos-based HTTP/HTTPS alternatives are available like Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) or Apache Kerby. An extension to Kerberos v5 supports Public Key Cryptography for Initial Authentication (PKINIT) mechanism where the authentication step between the subject and the Authentication Server uses public key cryptography, but then the subject uses software tokens for additional authenticated communications.[25]
- Digital signatures can bind personal authentication information to a message. By "signing" the message using the secret key of the subject, the receiver can verify the information originated from the object by decrypting the data using the subject's public key. There are many implementations of digital signatures for authentication, such as:
    - Security Assertion Markup Language (SAML) is an XML-based exchange of authentication information between a client, identity provider, and the service provider. SAML is a Single Sign On (SSO) interoperability standard, typically using a username and password combination to give access to a software environment via web browser.

[25] IETF RFC 4556, Public Key Cryptography for Initial Authentication in Kerberos (PKINIT), June 2006.

- OpenID Connect is an authentication extension on top of the OAuth 2.0 security protocol that uses a JSON Web Token (JWT) signed according to JSON Web Signing (JWS) specifications.

There are multiple authorization mechanisms that take authentication data (e.g., username/password, multifactor authentication information, cryptographic security tokens) and decide on access. In the case of administrators, once authorized, these users can adjust AC rules. Two types of authorization mechanisms are SQL and LDAP:

- Structured Query Language (SQL) is a standard language for defining, storing, retrieving, and manipulating data in relational database management systems (DBMSs). SQL authorization privileges can be granted, revoked, or adjusted for users/roles when the administrator role is enabled in the DBMS.
- Lightweight Directory Access Protocol (LDAP) is an authentication and/or an authorization mechanism, common for distributed AC systems with many users. It provides a modular, single sign-on solution for multiple applications in an information system. Microsoft's Active Directory Domain Service, which authenticates and authorizes users as system administrators or normal users when they log in to a computer on a Windows Domain, uses LDAP. LDAP is also the required AC mechanism in IEC 62351-8. LDAPS (LDAP over TLS) could be used if clear text authorization data is a concern.

AC implementations must select the authentication and authorization mechanisms. For instance, it is common to use Kerberos for authentication and LDAP for authorization. Though LDAP v3 uses the Simple Authentication and Security Layer (SASL) authentication framework[26] which permits different authentication mechanisms, including DIGEST-MD5, CRAM-MD5, and Kerberos v4.

When selecting these mechanisms for the DER AC implementation, the administrative overhead and ease of implementing administration delegation are important. Kerberos and LDAP groups are one combination for establishing AC delegated administration. Microsoft Active Directory also includes delegated administration tools for expanding administrative permissions, which may be useful for standalone AC implementations at utilities, DER vendors, aggregators, etc.

4.2. Session vs Message-Based RBAC and Separation of Duties

As defined in ANSI INCITS 359-2011 and supported in IEC 62351-8, subjects may interact with objects using either session-based or message-based access control. Session-based access control is established at transport layer via TLS. Message-based RBAC uses the access token in every message. Message-based RBAC is preferred in situations where multiple connections are made to a single object (e.g., IEEE 2030.5 server) that map to a single outbound connection (to DER devices).

There are different mechanisms for conflict of interest mitigations for session-based and message-based approaches. Separation of duty is critical for DER control environments to restrict a single user from gaining too much control of system resources. For instance, a DER vendor may limit users from having permissions to edit firmware source code, code sign firmware, and push firmware updates at the same time so there is at least two people required to push updated firmware. In the case of session-based AC, dynamic separation of duty is enforced; conflicts of interest are addressed when the user

[26] IETF RFC 4752, The Kerberos V5 ("GSSAPI") Simple Authentication and Security Layer (SASL) Mechanism), Nov 2006.

assumes a role. In message-based AC, static separation of duty is implemented; a single user cannot be assigned multiple roles deemed to have a conflict of interest. In the DER application space, static separation of duties is likely to cover most of the use cases because a single user should not be assigned to multiple roles that could produce a conflict of interest.

4.3. Push and Pull Models

It is possible to implement RBAC using two different data flow models. The push model requires the subject to fetch the token from the identity provider before sending it to the object. Whereas the pull model requires the object to fetch the token from the identity provider. The push model is shown in Figure 6 and the pull model is shown in Figure 7. Depending on the type of operational environment and object, the use of either the push or pull models may be appropriate. For instance, when multiple organizations are communicating to a DER via IEEE 1815, the push model may be best, because the tokens can be retrieved from the identity provider and then passed to the DER in a message-based connection. In the case of communicating to a single entity that has an IEEE 2030.5 server, it may be best to have the identity provided at the same entity; the authentication information can be sent to the server and the role authorized internally.

There are important considerations when selecting the model. In the case of push models, the access token must be secured with a short lifetime to prevent replay attacks. The access token must be validated by the object and the token exchange must be encrypted. For the pull model, the identity provider repository must be accessible by all users, there must be trust communications between the object and repository, the authentication information is always current, but there is a delay from the authentication communications. Careful analysis of these pros and cons must be undertaken to select the best approach for the DER RBAC implementation.

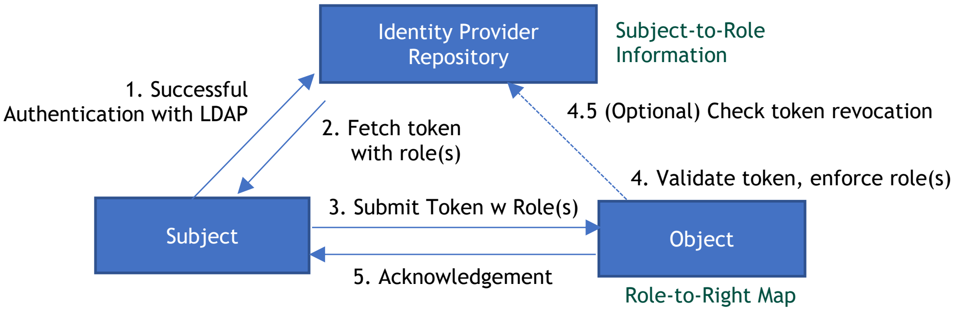

Identity Provider Repository
Subject-to-Role Information
1. Successful Authentication with LDAP
2. Fetch token with role(s)
4.5 (Optional) Check token revocation
4. Validate token, enforce role(s)
3. Submit Token w Role(s)
Subject
Object
5. Acknowledgement
Role-to-Right Map

Figure 6. Push RBAC Model

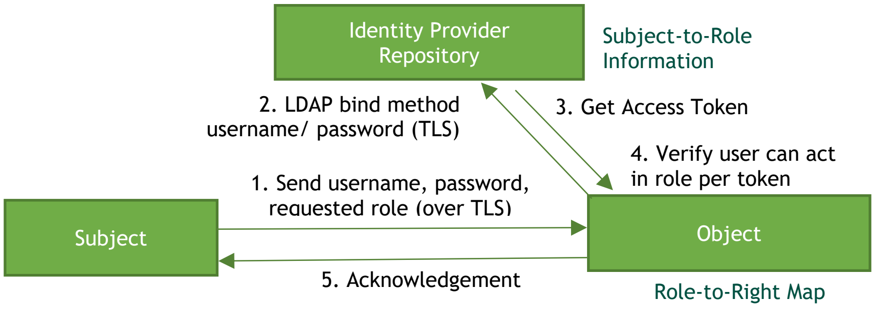

Identity Provider Repository
Subject-to-Role Information
2. LDAP bind method username/ password (TLS)
3. Get Access Token
4. Verify user can act in role per token
1. Send username, password, requested role (over TLS)
Subject
Object
5. Acknowledgement
Role-to-Right Map

Figure 7. Pull RBAC Model

4.4. Tokens

Access tokens are used to transport roles. IEC 62351-8 provides multiple options for defining access tokens. All profiles are identified as compliant with IEC 62351-8 with a unique OID (1.2.840.10070.8.1). Distributing the tokens is provided by an LDAP-enabled repository/server/device. When communicating with the repository, LDAP v3 with SSL/TLS should be used with unique user identifier, authentication information, and access token entries. For the IEC 62351-8 profiles, the type, tokens distribution, and optional revocation methods include:

- Profile A
  - **Token**: X.509 ID certificates with extensions using PKI
  - **Profile Distribution**: After the subject has been enrolled with a private key (e.g., using PKCS#10), the subject authenticates to the LDAP server and receives the access token (ID certificate). The private key is needed to apply the ID certificate.
  - **Token Authentication**: Subject proves the right to use the access token using a digital signature in the TLS handshake to the object, or challenge-response mechanism using authentication credential bound to access token.
  - **Token Integrity**: Access token signature verification through PKI chain.
  - **Revocation**: Use certificate revocation list (CRL) is permitted (per IEC 62351-3), though limited ID certificate lifetimes is preferred.
- Profile B
  - **Token**: X.509 attribute certificates using Privilege Management Infrastructure (PMI)
  - **Profile Distribution**: subject authenticates to the LDAP server with an ID certificate and receives the access token (attribute certificate tied to the ID certificate).
  - **Token Authentication**: Subject proves the right to use the access token using a digital signature in the TLS handshake to the object, or challenge-response mechanism using authentication credential bound to access token.
  - **Token Integrity**: Access token signature verification through PKI chain.
  - **Revocation**: Attribute Certificate Revocation List (ACRL) is supported but limited attribute certificate lifetimes should be used.
- Profile C
  - **Token**: Software token (similar to Kerberos)
  - **Profile Distribution**: Subject authenticates to the LDAP server with an ID certificate and receives a software token.
  - **Token Authentication**: Challenge-response mechanism uses authentication credential bound to access token.

    - **Token Integrity**: Checked with pre-shared key.
    - **Revocation**: Revocation lists based on access token serial number and issuer; limited token lifetimes are preferred.

Per IEC 62351-8, tokens must include the following fields:

- serial number of the access token
- name of the subject and access token holder
- role assigned to the subject and access token holder
- issuer of the access token
- timestamp of the issuing moment
- time-period during which the access token and thus the role assignment is valid
- revision number of the subject-to-role assignment
- signature algorithm (Profile A or B)
- signature value of the issuing instance (Profile A or B)
- Hash algorithm (Profile C)
- Key length (Profile C)
- Hash value (Profile C)

and optionally include,

- revision number for role assignment
- area of responsibility (geographical or organizational)
- issuing instance of access token
- revocation list
- role definition
- operation field for attribute-related operations, where the access token is applied to an administrative user at the object; This is used to change permissions of roles on the object.
- dedicated sequence number for replay protection in environments without time synchronization

4.5. Potential DER RBAC Implementations

It would be preferred to establish protocol-agnostic AC requirements. However, due to the unique characteristics of each of the IEEE 1547-2018 protocols (IEEE 2030.5, IEEE 1815, and SunSpec Modbus), there are specific considerations needed when building an AC system for each of these protocols. This is primarily because IEEE 2030.5 client/server implementations naturally make the IEEE 2030.5 server the AC object; while DNP3 and Modbus implementations work best with the DER acting as the object.

It is possible the IEEE 1547-compliant interfaces will only be used by utilities because DER service providers and/or DER vendors will route all their traffic through the proprietary interface(s). Therefore, in the sections below, proprietary and front-panel interfaces are also included to show alternative access paths.

Applying centrally-coordinated AC mechanisms for all DER access points is possible with a federated approach, but it may not provide significantly greater security than a non-federated approach—and comes with substantially more management/administration complexity. For instance, it may be simpler to have the utility connection to DER through their own IEEE 2030.5 server. They would then manage their own access control system internally, likely using Windows Active Directory or some other integrated, internally managed system. In the non-federated case, the DER service provider could manage the access control for many of the other stakeholders. These questions remain unresolved, so multiple implementation options are presented below for IEEE 2030.5, IEEE 1815, and SunSpec Modbus communications—though many combinations of these examples could provide the desired level of access protection.

4.5.1. Utility Communicating IEEE 2030.5

For client-server protocols, the access control object is the server. Anyone with access to the servers can invoke RESTful exchanges. DER clients will pull down IEEE 2030.5 messages associated with them so the access protections must be placed on the server as opposed to the DER equipment itself.

Furthermore, IEEE 2030.5 does not support embedding roles in IEEE 2030.5 exchanges. IEEE 2030.5-2018 is silent on RBAC implementation but does include ACL attributes. For authentication, the client-server access authentication is applied using certificates over TLS. All hosts shall present their certificate as part of the TLS handshake. Authorization is performed on a request-by-request basis determined by the ACL settings for the object, which may be set up at the end of the authentication based on the level of client authentication. It is also mentioned that the Local Registration List can be also used to authorize a device-by-device basis. The AuthType attribute is used to control the required authentication types in the HTTPS request:

- 0x1: No authentication
- 0x2: User Authentication
- 0x4: Self-signed certificate
- 0x8: Device certificate

Within the DER Cybersecurity Workgroup, utility participants indicated they would not like to be the owner of the identity server and did not want to be responsible for the cybersecurity of assets that they did not own. Therefore, there are a couple potential implementation options for access control when the utility is communicating IEEE 2030.5. In these cases, the utility may communicate directly to the DER equipment or to DER service providers (or a combination).

In the first exemplar, shown in Figure 8, the utility domain is shown at the top of the figure, the DER service provider domain is in the middle, and the DER is at the bottom. In this case, it is assumed that the utility does not interact with a central identity provider or access control database to adjust settings in its IEEE 2030.5 server. Instead the utility has its own authorization service. Any utility user seeking to change settings on the IEEE 2030.5 server will either change the settings directly on the server or via a DER management system (DERMS) gateway application, which will relay user's log in credentials to the access control service to authenticate and authorize the user. Once authorized to make changes to the server, the user may change the IEEE 2030.5 profiles that will be pulled down by the DER clients or the DER service provider client. The steps in the process in Figure 8 are:

1. The utility user logs into the DERMS (AC object) with their credentials. In the case this is done remotely, this connection will use TLS mechanisms to verify the identity of the object.
2. The DERMS uses LDAP bind to pass user credentials to the AC service.
3. The DERMS uses LDAP query to retrieve the user access token.
4. The DERMS verifies the access token to determine if the utility user is authorized to act in the selected role.

In some instantiations of the utility system, steps two and three may be omitted because the DERMS contains a replica of the LDAP repository.

In this example, the DER service provider exposes an application programming interface (API) or other webservice for stakeholders to access DER devices or data. Users will enroll in a particular role with the DER service provider (or other authorized) administrator, and the IEEE 2030.5 or proprietary protocol server will use the pull model to authenticate and authorize the user to the identity provider. The steps in this process are:

1. The subject opens a TLS protected connection through the API to the DER communication server. The TLS cryptographic mechanisms will be used to verify the identity of the object (likely the DER communication server, but possibly the API) being accessed.
2. Once the object is verified, the subject transmits their authentication credentials to the DER service provider object.
3. The object uses the LDAP bind method and user credentials to authenticate the subject to the identity provider repository.
4. The object uses the LDAP query to retrieve the access token for the subject from the LDAP repository. The object verifies the user can act in the specified role and then acknowledges or rejects the authentication of the subject.
5. If authorized, the user may make changes to the IEEE 2030.5 profile, and the DER or gateway client will pull down the new profile.

In many cases, users will be requesting current or historical monitoring data that is likely to be stored in a separate database at the DER service provider. Those requests will need to be directed to the appropriate AC-protected objects at the DER service provider.

The DER equipment often includes a local interface that can be accessed with a front panel, Wi-Fi, Zigbee, browser, or some other connection. This interface should also be protected with AC mechanisms. While fallback operating modes should exist for communication failures, commissioning/maintenance, etc., access to this equipment should be governed by the identity provider as well. In this case the DER or front panel is the object and it will use the pull model to get the user's token from the LDAP repository to authorize access or changes to the equipment.

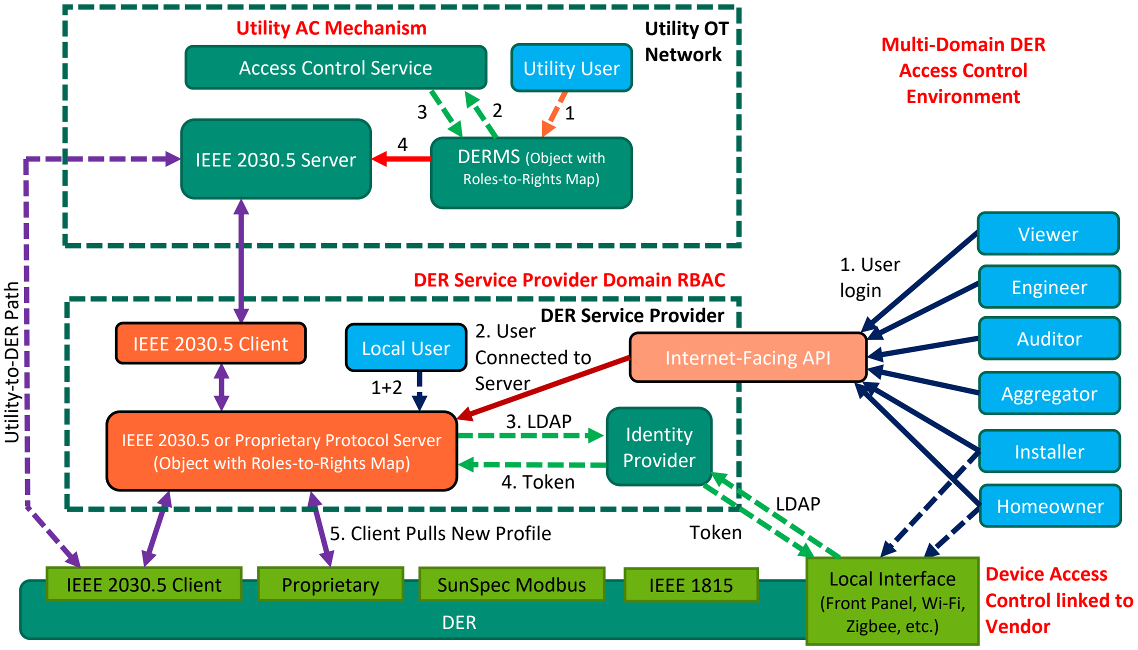


Figure 8. IEEE 2030.5 Access Control with DER Service Provider-Owned Identity Provider

In a slightly different configuration shown in Figure 9, the AC identity provider is owned by a 3rd party. This system could be managed by this entity or that management role could be delegated to each of the appropriate stakeholders. This AC environment will work the same as the previous, except that the LDAP connection from the DER service provider object to the identity provider (Step 3) must use TLS in order to verify the identity of the LDAP repository since it is no co-located with the object.

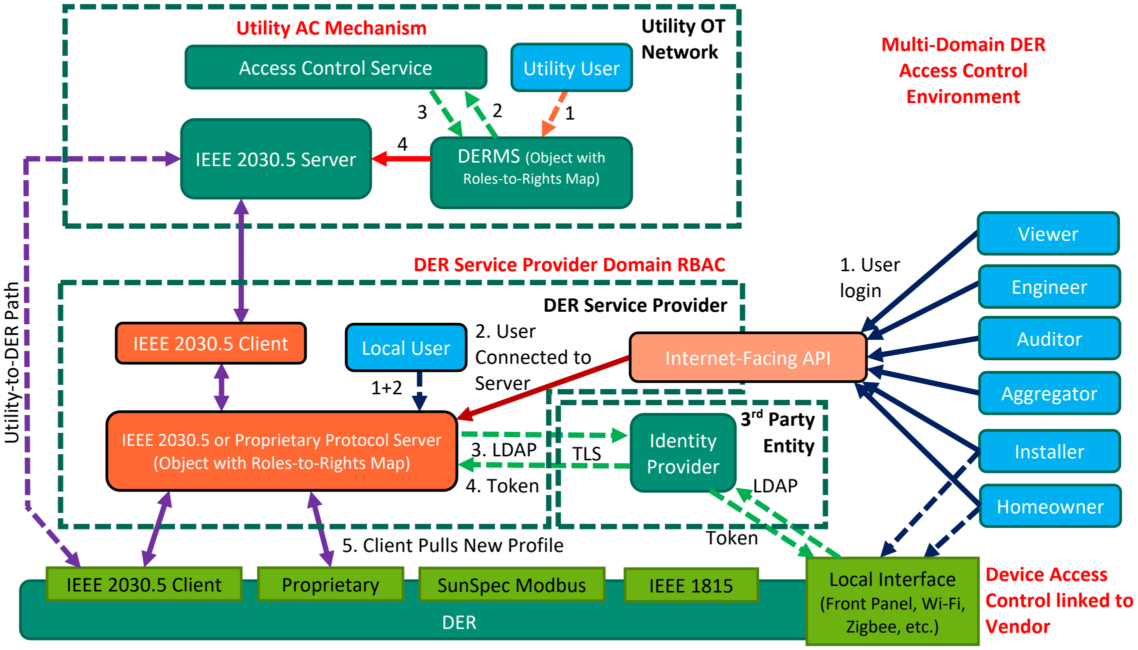


Figure 9. IEEE 2030.5 Access Control with 3rd Party-Owned Identity Provider

The Pull Model approach to would look like the exchange shown in Figure 10.

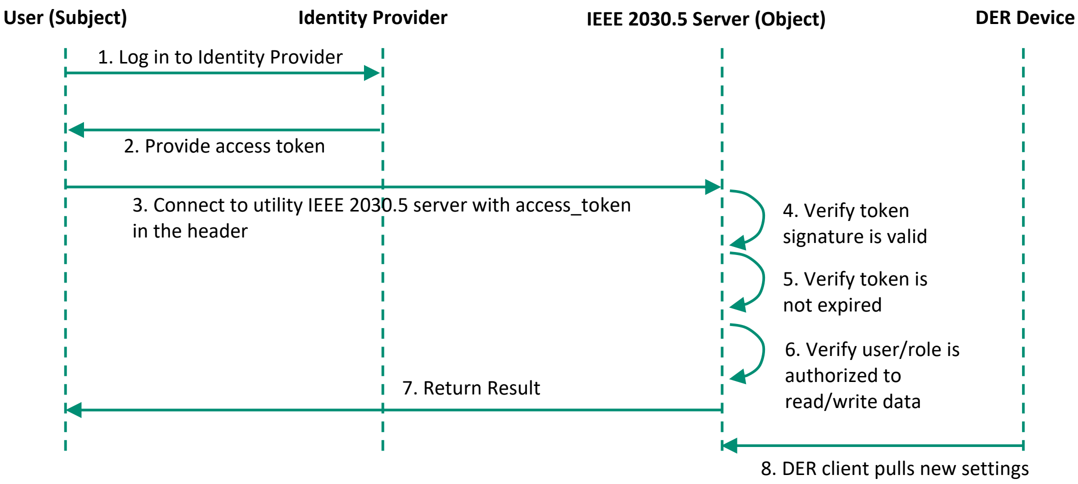

User (Subject)
Identity Provider
IEEE 2030.5 Server (Object)
DER Device
1. Log in to Identity Provider
2. Provide access token
3. Connect to utility IEEE 2030.5 server with access_token in the header
4. Verify token signature is valid
5. Verify token is not expired
6. Verify user/role is authorized to read/write data
7. Return Result
8. DER client pulls new settings

Figure 10. RBAC Push Model for IEEE 2030.5.

It is good practice to associate the IEEE 2030.5 messages passed through the utility-to-DER service provider connection to the "utility" role in the AC ecosystem. Unfortunately, as shown in Figure 11, there are multiple utilities which will have connections to each DER Service Provider because multiple companies operate within utility jurisdictional regions. Therefore, it is necessary to subdivide utility roles based on the DER equipment in their territories. In the example in Figure 11, assuming each of these utilities is issuing DER setpoints through the DER service providers, the DER service providers will each have three IEEE 2030.5 clients associated with the utility's IEEE servers. The IEEE 2030.5 endpoints are authenticated using the TLS handshake, so commands from each server can be safely assigned to the correct utility role with associated DER privileges. Therefore, regardless of where the identity provider is located, each utility must have the utility role mapped to the DER equipment in its territory. This is also the case for ISO/RTOs, installers, etc. in order to preserve the principle of least privilege. Likewise, any DER service provider or DER should only be able to access information from the server associated with their assets (e.g., a DER cannot GET, PUT, POST, or DELETE control settings for other DER equipment). These jurisdictional relationships may make ABAC more appealing in certain DER AC implementations.

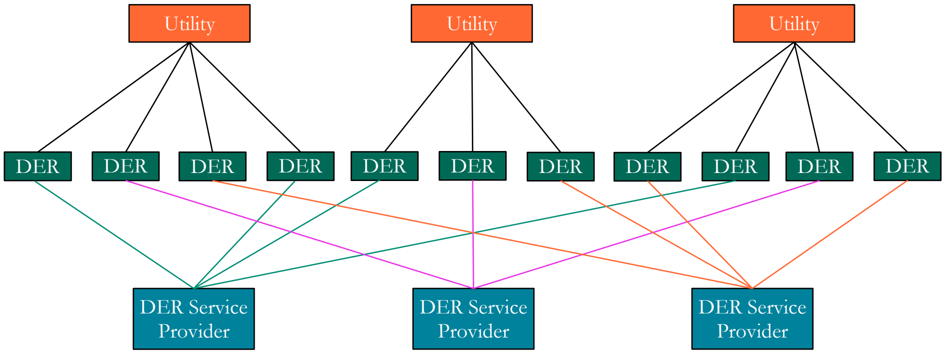


Figure 11. Utility Jurisdictional Ownership and DER Service Provider Mappings

4.5.2. Utility Communicating IEEE 1815 and SunSpec Modbus

In the case of IEEE 1815 (DNP3) and SunSpec Modbus, the master commands device changes and reads setpoints, nameplate, monitoring, and other data. In the DNP3 case, the master can read outstation digital input (DI) and analog input (AI) points and write outstation digital output (DO) and analog output (AO) points. For SunSpec Modbus, holding registers representing nameplate/measurement data and control settings can be read and written in the Modbus slave. DNP3/Modbus masters may be located within the ownership domains of multiple stakeholders. So, in these cases, push models are more appropriate because the object that contains the role-to-right map will be the DER.

DNP3/Modbus communications can be protected using TLS, per DNP3 Secure Authentication (DNP3-SA)[27] or Modbus TCP Security[28], down to the devices in order to protect the token. Currently, few—if any—DER devices or gateways contain access control functionality beyond simple passwords. Therefore, to implement RBAC, a few different options would need to be explored.

When the DER equipment is the object, the need for a federated AC environment is more crucial because the device should authorize access based on a token tied back cryptographically to a single server. Otherwise, a DER device would need to accept RBAC tokens from multiple AC ecosystems, which makes the administration more challenging and the potential for cyber weaknesses much greater. As shown in Figure 12, the utility operators will communicate DNP3/Modbus to the DER equipment in one of the following methods.

Utility communicates to DER directly using Push Model:

1. The utility user/subject connects to the DER service provider through a utility API or potentially directly to an internet-addressable identity provider.
2. The API will communicate with the LDAP identity server to authenticate the utility.
3. The API will retrieve the utility's access token and roles from the LDAP-enable service (identity provider).
4. The API returns the token to the utility user.
5. The user submits the access token containing the role information to the DER with the DNP3/Modbus read/write/execute request.
6. The DER verifies the access token of the subject and gives the utility subject authorized access to DER object(s) according to the utility rights in the token.
7. The DER acknowledges authentication and, as appropriate, provides a response to the utility request.

Utility communicates to DER via DER Service Provider using Pull Model:

1. Utility subject logs into DER Service Provider system with their credentials.
2. From the DER service provider API/web service/other DERMS interface, the utility user requests a set of read/write/execute operations.
3. The DER Service Provider DERMS will communicate the utility-specified commands to the DER using the provided credentials (e.g., username, password, requested role) with their internal DNP3 Master, Modbus Master, or proprietary protocol.

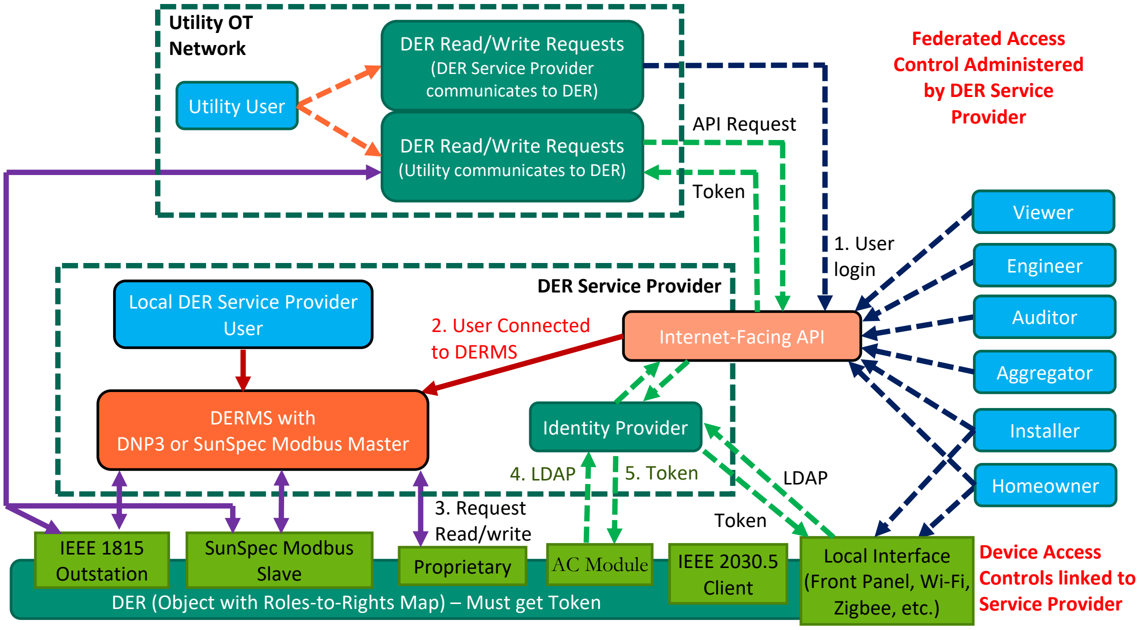
[27] IEEE 1815-2012, "IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)," 10 Oct 2012.

[28] Modbus.org, "MODBUS/TCP Security Protocol Specification," MB TCP Security v21, 7/24/2018.

4. The DER uses LDAP bind method to supply utility authentication credentials to verify the authentication information with the identity provider server. This connection will use TLS to verify the identity of the identity provider repository and protect the exchange.
5. The DER uses an LDAP query to retrieve the utility-specific access token from the LDAP repository.
6. The DER verifies the access token to ensure the user is allowed access in the provided role.
7. The DER acknowledges or rejects the authentication and then proceeds with the requested read/write/execute actions.

Note that the TLS connection from the utility does not reach the object in this scenario and is instead composed of two protected links: one from the utility to DER Service Provider and another TLS connection between the DER Service Provider and the DER/gateway. Normally the utility would want to verify the identity of the object that it is communicating with, but instead this is done piecemeal: the utility has the responsibility to verify the identity of the DER Service Provider and the DER Service Provider has the responsibility to verify the identity of the DER.

For DER communications from other external stakeholders, the pattern would be the same as the utility Pull Model above. In the situation that subjects are communicating with the equipment via a front panel, the DER will use the entered credentials to authenticate their role with the identity server, in the same way that the requests originated from the DER Service Provider DERMS. Similar RBAC implementations could be designed where the Identity Provider is owned by a 3rd party or other organization.



Utility OT Network
Utility User
DER Read/Write Requests (DER Service Provider communicates to DER)
DER Read/Write Requests (Utility communicates to DER)
API Request
Token
Federated Access Control Administered by DER Service Provider
1. User login
Viewer
Engineer
Auditor
Aggregator
Installer
Homeowner
DER Service Provider
Local DER Service Provider User
2. User Connected to DERMS
Internet-Facing API
DERMS with DNP3 or SunSpec Modbus Master
Identity Provider
4. LDAP
5. Token
LDAP
Token
3. Request Read/write
IEEE 1815 Outstation
SunSpec Modbus Slave
Proprietary
AC Module
IEEE 2030.5 Client
Local Interface (Front Panel, Wi-Fi, Zigbee, etc.)
Device Access Controls linked to Service Provider
DER (Object with Roles-to-Rights Map) – Must get Token

Figure 12. Federated IEEE 1815/SunSpec Modbus Access Control with DER Service Provider-Owned Identity Provider

Modbus, by design, is limited in its security features. To apply RBAC principals, it is likely a higher-level gateway, co-located with the DER, would handle authorization steps, roles-to-rights mapping, and only read/write permitted registers. For example, some researchers have created a centralized model to implement the functionality.[29] In their approach, a pull model is used where the Modbus slave is upgraded with a Modbus Application Protocol Secure Handler and Access Control Module to handle the RBAC operations before reading or writing to holding registers. Similar implementations could be created for DER devices. Since this type of control module or gateway acts as a bridge between encrypted, external networks and local ones that operate in the clear, additional physical security requirements are necessary for these networking devices. In the case of DNP3-SAv6, recent proposed changes may establish a new, separate protocol layer between the DNP3 Application Layer and the DNP3 Transport function.[30,31] Additionally, an Authorization Management Protocol (AMP) may manage authorization by directing messages between masters, outstations, and a central Authority (which could act like a RBAC identity provider). An illustration of this data exchange is included in Figure 13. Unfortunately, AMP only informs the outstation of which roles and permission the Authority assigns to a given master. ACLs would be needed for access control at a per-point level. This approach—like that described above for IEEE 2030.5—offloads the role-to-rights mapping to the master (or server) and there is no logic at the DER for how to handle a given role. Further analysis of DNP3-SAv6 will be necessary to determine if this approach would be effective for DER communication systems.

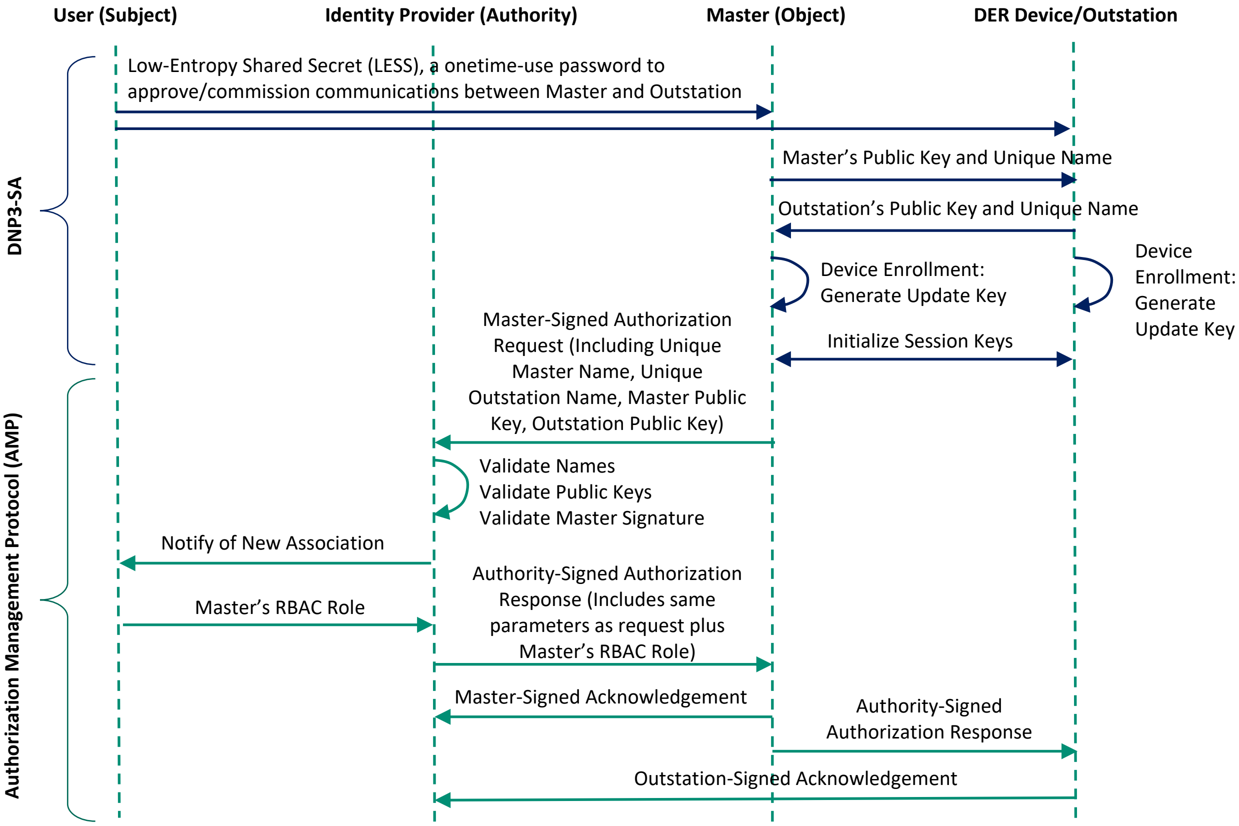

User (Subject)
Identity Provider (Authority)
Master (Object)
DER Device/Outstation
DNP3-SA
Authorization Management Protocol (AMP)
Low-Entropy Shared Secret (LESS), a onetime-use password to approve/commission communications between Master and Outstation
Master's Public Key and Unique Name
Outstation's Public Key and Unique Name
Device Enrollment: Generate Update Key
Device Enrollment: Generate Update Key
Initialize Session Keys
Master-Signed Authorization Request (Including Unique Master Name, Unique Outstation Name, Master Public Key, Outstation Public Key)
Validate Names
Validate Public Keys
Validate Master Signature
Notify of New Association
Master's RBAC Role
Authority-Signed Authorization Response (Includes same parameters as request plus Master's RBAC Role)
Master-Signed Acknowledgement
Authority-Signed Authorization Response
Outstation-Signed Acknowledgement

Figure 13. Proposed DNP3-SAv6 Enrollment and RBAC Authorization. Adapted from "Overview of DNP3 Security Version 6".

[29] S. Figueroa-Lorenzo, J. Añorga, S. Arrizabalaga, "A Role-Based Access Control Model in Modbus SCADA Systems. A Centralized Model Approach." Sensors (Basel, Switzerland), vol. 19, no. 20, pp. 4455, 14 Oct. 2019.

[30] DNP Users Group Member Update, December 2019.

[31] DNP, Overview of DNP3 Security Version 6.

5. PATH FORWARD

There are several critical issues that must be addressed by the DER industry before an access control solution can be deployed. As described above, the industry should work together to create an access control policy. This can be used to select an appropriate access control model and mechanisms. There are historical and technical reasons role-based access control may be the most appropriate model for the DER communication environment, e.g., RBAC has been vetted and standardized for power systems applications. Roles are naturally represented by user employers (this user works for ABC Utility), ownership (DER owners), or legal agreements (DER service providers). There are options for implementing RBAC or other access control policies for DER for each of the IEEE 1547-2018-specified protocols. While this functionality is not imbedded in the protocols naturally, RBAC for IEEE 2030.5 can be applied at the configuration interface of the server, IEEE 1815 RBAC may be included using the proposed DNP3-SAv6 additions, and additional gateway services can be added to DER to manage Modbus RBAC. Example communication relationships between organizations/entities, subjects/stakeholders, and DER equipment were provided above, but selection of an implementation approach for the industry must be determined through consensus-based standards development processes. These could be created under IEEE, IEC, or other standards development processes or as directed by public utility commissions.

5.1. Suggested Normative Language for DER Equipment

To provide IEEE, IEC, or other SDOs with a starting place for normative DER AC language, we outline suggested recommendations for DER equipment in this section. We focus on DER device requirements because AC requirements will likely be first incorporated into interconnection standards. If an RBAC model is adopted, supporting requirements would need to be established for DER Service Providers, utilities, and other stakeholders for the ecosystem to function, but those could be built on top of these device-level requirements. Another reason to start with DER device RBAC requirements is that few communicate IEEE 2030.5 natively, so most DER will need to have a local roles-to-rights map. The following RBAC requirements are not applicable for DER that only support an IEEE 2030.5 interface.

Using IEEE Std. 1686 as a reference, the following requirements are recommended.

General requirements

- All electronic access to DER, whether locally through a control panel or diagnostic port, or remotely through communications media, shall be protected with an authentication mechanism that identifies a subject with a unique user identification (ID) and password combination. Further use of authentication mechanisms (e.g., Smart Cards, USB tokens, geolocation technologies, biometrics, etc.) for multifactor authentication is permitted.
- The DER shall have no undisclosed means whereby the access control can be defeated or circumvented.
- User-created passwords shall follow a set of rules that shall be adhered to in the creation of each password. Passwords must be at least eight characters in length and shall be case sensitive. When encoding passwords in plain text, the password characters shall contain the following:
    - At least one uppercase and one lower case letter
    - At least one number
    - At least one non-alphanumeric character (e.g., @, %, &, *)

- Any attempt to create a password that violates these rules shall be captured at the time of attempted creation, and the user shall be notified and prompted to choose another password that conforms to the rules.
- The DER shall support adjustable account lockout thresholds and durations.[32]
- Only user IDs shall be displayed in screens, audit trails, the memory area or files, and other records and configuration files. It shall not be possible to cause passwords to be displayed through any means, including local display panel, configuration software (local or remote; offline or online), web browser, and terminal access.
- The DER shall have a timeout feature that automatically logs out a user who has logged in after a period of user inactivity. Inactivity shall be defined as the absence of input from local or remote DER ports. The period of time before the timeout feature activates shall be settable by an authorized user in the DER configuration.[33]
- The DER shall either support access control lists or role-based access control. Any DER device that supports an IEEE 1815 or SunSpec Modbus interface must support the RBAC requirements.

Access Control List (ACL) requirements

- DER shall have an open and documented interface to change user accounts and passwords.
- The minimum number of individual users supported by the DER shall be 20.[34]
- The DER shall support the ability to assign authorization to utilize one or more DER rights based on individual user-created ID/password combinations. At minimum, rights should include:
    - Reading DER nameplate or configuration information, measurement data (voltage, current, power, energy, status, alarms, etc.), and control mode settings.
    - Writing control mode settings that alter the operational characteristics of the DER.

  Additional functionality shall be documented.

Role-Based Access Control (RBAC) requirements

- The DER shall have the capability of defining at least 10 user-defined roles.[35] Each role shall have the capability of having any combination of rights including:
    - Reading DER nameplate or configuration information, measurement data (voltage, current, power, energy, status, alarms, etc.), and control mode settings.
    - Writing control mode settings that alter the operational characteristics of the DER.

  Additional functionality shall be documented.
- The DER must support the "push" RBAC model and accept valid role tokens.
- A role shall be assignable in the DER using an IEC 62351-8 Profile A token. Additional methods of assigning roles to subjects/users are permitted.

5.2. Unanswered Questions

There are many unanswered questions surrounding an AC implementation strategy. Some of the biggest issues raised in the DER Access Control Subgroup include:

[32] These can be selected based on the AC policy.

[33] The interval can be selected based on the policy.

[34] The number of the subjects can be further refined in a DER access control standard or consensus-based policy.

[35] Roles should be defined by a DER access control standard or consensus-based policy.

- **Who writes the DER access control policy?**
  - While high-level access control recommendations will likely be provided in national guides such as the forthcoming IEEE 1547.3 revision, a national standard for DER access control is unlikely for many years. So, it may be better to create jurisdictional implementations through state public utility commissions in the short term. These could be adopted relatively quickly by utilities, DER vendors, and other stakeholders by writing the formal AC policy into interconnection handbooks/regulations. This document and the above language may act as a template for those interconnection regulations.
- **Who arbitrates access and manages the identity provider?**
  - As discussed earlier in the management delegation section, it is unreasonable for a single entity to manage the entire DER access control administration task. The user-to-role mapping should be delegated to administrators in each stakeholder organization (e.g., each utility/DER vendor/DER service provider/etc. is responsible for updating their users and roles). The precise mechanism surrounding the delegation of authority and safety mechanisms to prevent insider threats needs to be established.
- **Could AC mechanisms and role-to-rights maps be mandated for all DER? Is AC more likely to be handled in proprietary gateways?**
  - Given DER equipment is only required to include one of the three IEEE 1547 protocols, the simplest path to creating robust RBAC implementations may be to employ gateways that translate RBAC-supported protocols to local DNP3/Modbus DER messages. Also, DER equipment/interconnection standards, like IEEE 1547, take a substantial amount of time to be updated, so these device-level regulations are not likely to be seen for 3-5 years at the earliest. One of the advantages of the proprietary gateway approach is communication protocols can be patched at the rate that vulnerabilities are discovered.
- **At a national level, will one of the proposed implementations emerge as the predominant approach? Or will all the interoperability topologies (representing the different IEEE 1547 protocols) exist simultaneously?**
  - It is uncertain how US utilities will communicate to DER equipment within their service territories. This will drive much of the decision making around AC policy and mechanism selection and implementation.
- **How can the AC policy be designed to be scalable but prevent the proliferation of fine-grained roles (e.g., the "role explosion" problem)?**
  - Industry standardization would be best for designing the system with an appropriate number of roles, size of the role hierarchy, administrative implementation constraints, etc. This would provide boundaries on the number/type of roles; however, it does limit the expansion of new roles that may be required based on geographical locations of subjects, working hours, or other pertinent attributes.
- **If access control was required in the US, how many RBAC systems would be created? Could a single identity provider database exist for the entire country?**
  - Utilities have their interests geographically constrained, but DER service providers have equipment spread across the country. Therefore, if multiple RBAC systems are stood up based on traditional utility or balancing authority jurisdictions, DER service providers will likely need to configure their roles for each of these jurisdictions—adding significant overhead. However, a nation-wide AC service provides a single point-of-failure. If it became corrupted through malicious or unintentional actions,

communications to all DER equipment may be temporarily terminated. A single database would also be much larger than jurisdictional implementations, which would reduce performance (e.g., require longer query times, etc.). This same challenge is present for establishing certificate authorities (CAs) for IEEE 2030.5 PKI implementations. It may be logical for AC identity servers to mirror the locations and owners of the PKI CAs. So, if a utility chooses to act as the IEEE 2030.5 PKI CA for their jurisdiction, they could also establish the a RBAC identity server as well.

- **What happens with the temporary or permanent loss of the identity provider?**
  - While generally solved in many computing environments, contingency modes must be established if the identity provider server is offline. If the utility loses the ability to communicate with the equipment it could impact power system operations. Ensuring DER availability for a range of failure modes should be built into the AC system, while also protecting these fallback or cached operating modes from exploitation. Development of Quality of Service (QoS) requirements are necessary for the identity provider owner to select appropriate service level agreements (SLAs) for critical resources.
  - A major concern is if the organization that owns the identity provider goes out of business or stops supporting the service. For instance, if a large DER service provider went bankrupt and all RBAC tokens for the utility, homeowner, etc. were provided by this organization, the AC system would break, and no one could communicate with the DER equipment. Third-party implementations are also vulnerability to this problem. Designing security policy and mechanism portability and mandating independent offline backups may minimize the risk from this scenario, but still not eliminate it.

5.3. Closing Thoughts

Access control is a necessary component of a national defense-in-depth cybersecurity strategy for DER equipment. Currently, there is no clear path to adding access control requirements to the DER communication systems. In order to move forward, detailed access control policies must be drafted. From there, the access control mechanism can be selected, and specific implementation mechanisms can be put into place. The diversity and number of stakeholders, DER devices, and DER service provider business models make these choices especially difficult. The brief discussion of potential implementations provided in this report is a starting place for standards development organizations to understand the complexity of the communication ecosystem and begin drafting guidance for the industry. Example normative language for a DER cybersecurity standard is provided as a starting place for the DER AC requirements.

APPENDIX A. RBAC ROLES AND ROLES-TO-RIGHTS MAPS FOR IEEE 1547 DATA PARAMETERS

This section outlines the basic principles of a RBAC implementation for IEC 61850-7-420, IEEE 1815, IEEE 2030.5, and SunSpec Modbus. The roles-to-rights/permissions map is provided for multiple generic user roles below. This mapping would also be effective for other access control implementations including access control lists, etc. The roles and associated read (r) and write (w) permissions are defined, using the principle of least privilege, based on the following:

- DER Owner – The owner of the system may read the nameplate information, configuration data, and monitoring data points.
- Installer – The system installer may be required to configure the DER for a particular jurisdiction with a given grid code/interconnection standard that includes updates to the ride-through/trip settings, and other parameters.
- DER Vendor or DER Service Provider – The vendor or service provider is likely to have their own proprietary communication interface with the DER equipment to monitor additional operating details and push firmware updates. However, if a DER Vendor user is accessing the equipment with the standardize communication interface, they will have substantially fewer permissions as the control functionality will be assigned to the grid operators or an area electric power system (EPS) operator-designated aggregator. So, unless authorized as one of those roles, vendors and service providers will have privileges limited to those of a DER owner.
- 3rd Party Aggregator – The role of the aggregator is to relay grid operator commands to the DER or communicate pre-determined controls to the end devices. As such, their scope will match that of the utility. This role should not exist is utilities are directly controlling their equipment.
- Utility/DSO – While traditionally distribution system operators (DSOs) would be primarily responsible with maintaining feeder voltages and likely be limited to reactive power support functions, US utilities often operate at the transmission and distribution levels. Therefore, utilities will have access to read and write all the control points and execute any of the grid-support functions.
- ISO/RTO/TSO - Independent System Operators (ISOs), Regional Transmission Organizations (RTOs), and Transmission System Operators (TSOs) are concerned about bulk system operations, but distributed resources now have a large enough percentage of total generation that they monitor these systems. Often this data is used to advise short term forecasts and support security constrained economic dispatch scheduling. They will have the same access to the DER as a utility.
- Security Administrator – The security administrator can change subject-to-role assignments (outside the object), role-to-right assignment (inside the object), change security settings (e.g., certificates for subject authentication, access token verification, certificate validity periods). Therefore, this user can change many of the backend control of the system, but has no need to read, write, or execute any of the DER IEEE 1547 functionality.
- Security Auditor – The Security Auditor can view audit logs in the object. Like the Security Administrator they have no need to read, write, or execute any of the DER IEEE 1547 functionality.
- RBAC Manager – The RBAC Manager can change the role-to-right assignments. They should not access any of the IEEE 1547 functionality.

It should be noted that if the DER RBAC implementation would like to align with IEC standards, IEC 62351-8 provides the following mandatory roles that would need to be included:

- VIEWER: can view what objects are present within a Logical-Device by presenting the type ID of those objects.
- OPERATOR: An operator can view what objects and values are present within a Logical-Device by presenting the type ID of those objects as well as perform control actions.
- ENGINEER: An engineer can view what objects and values are present within a Logical-Device by presenting the type ID of those objects. Moreover, an engineer has full access to Date Sets and Files and can configure the server locally or remotely.
- INSTALLER: An installer can view what objects and values are present within a Logical-Device by presenting the type ID of those objects. Moreover, an installer can write files and can configure the server locally or remotely.
- SECADM: Security administrator can change subject-to-role assignments (outside the device) and role-to-right assignment (inside the device) and validity periods; change security setting such as certificates for subject authentication and access token verification.
- SECAUD: Security auditor can view audit logs.
- RBACMNT: RBAC management can change role-to-right assignment.

Table A-1. RBAC Roles-to-Rights Map for IEC 61850, IEEE 1815, IEEE 2030.5, and SunSpec Modbus

IEEE 1547 Data Requirements	Communication Protocol				Role								
	IEC 61850 Data Objects (LN.DO)	IEEE 1815 (DNP3) Uses IEC 61850 names	IEEE 2030.5	SunSpec Modbus	DER Owner	Installer	DER Vendor/ Service Provider	3rd Party Aggregator	Utility/DSO	ISO/RTO/ TSO	Security Administrator	Security Auditor	RBAC Manager
IEEE 1547 Nameplate data objects													
Active power rating at unity power factor (nameplate active power rating)	DGEN.WMaxRtg	AI4	DERCapability::rtgMaxW	702.WMaxRtg	r--	r--	r--	r--	r--	r--	---	---	---
Active power rating at specified over-excited power factor	DGEN.WGnOvPFRtg	AI6 - AI7	DERCapability::rtgOverExcitedW	702.WOvrExtRtg	r--	r--	r--	r--	r--	r--	---	---	---
Specified over-excited power factor	DGEN.OvPFRtg	AI8	DERCapability::rtgOverExcitedPF	702.WOvrExtRtgPF	r--	r--	r--	r--	r--	r--	---	---	---
Active power rating at specified under-excited power factor	DGEN.WGnUnPFRtg	AI9 - AI10	DERCapability::rtgUnderExcitedW	702.WUndExtRtg	r--	r--	r--	r--	r--	r--	---	---	---
Specified under-excited power factor	DGEN.UnPFRtg	AI11	DERCapability::rtgUnderExcitedPF	702.WUndExtRtgPF	r--	r--	r--	r--	r--	r--	---	---	---
Apparent Power Maximum Rating	DGEN.VAMaxRtg		DERCapability::rtgMaxVA	702.VAMaxRtg	r--	r--	r--	r--	r--	r--	---	---	---
Normal operating performance category	DGEN.Ieee1547Cat1	AI22	DERCapability::rtgNormalCategory	702.NorOpCatRtg	r--	r--	r--	r--	r--	r--	---	---	---
Abnormal Operating Performance Category	DGEN.Ieee1547Cat2	AI23	DERCapability::rtgAbnormalCategory	702.AbnOpCatRtg	r--	r--	r--	r--	r--	r--	---	---	---
Reactive Power Injected Maximum Rating	DGEN.VarMaxSupRtg	AI12	DERCapability::rtgMaxVar	702.VarMaxInjRtg	r--	r--	r--	r--	r--	r--	---	---	---
Reactive Power Absorbed Maximum Rating	DGEN.VarMaxAbgRtg	AI13	DERCapability::rtgMaxVarNeg	702.VarMaxAbsRtg	r--	r--	r--	r--	r--	r--	---	---	---
Active Power Charge Maximum Rating	DSTO.WChaUnPFRtg	AI5	DERCapability::rtgMaxChargeRateW	702.WChaRteMaxRtg	r--	r--	r--	r--	r--	r--	---	---	---
Apparent Power Charge Maximum Rating	DSTO.VAMaxChaRtg	AI15	DERCapability::rtgMaxChargeRateVA	702.VAChaRteMaxRtg	r--	r--	r--	r--	r--	r--	---	---	---
AC voltage nominal rating	DECP.VRef	AI29 - AI30	DERCapability::rtgVNom	702.VNomRtg	r--	r--	r--	r--	r--	r--	---	---	---
AC voltage maximum rating	DGEN.VMaxRtg	AI3	DERCapability::rtgMaxV	702.VMaxRtg	r--	r--	r--	r--	r--	r--	---	---	---
AC voltage minimum rating	DGEN.VMinRtg	AI2	DERCapability::rtgMinV	702.VMinRtg	r--	r--	r--	r--	r--	r--	---	---	---
Supported Control Mode Functions	DVRT, DFRT, DFWP, DWLM, DVWC, DFWC, DVAR, DFPF, DVVC, DWVR	BI31 - BI51	DERCapability::modesSupported	702.CtrlModes	r--	r--	r--	r--	r--	r--	---	---	---

IEEE 1547 Data Requirements	Communication Protocol				Role								
	IEC 61850 Data Objects (LN.DO)	IEEE 1815 (DNP3) Uses IEC 61850 names	IEEE 2030.5	SunSpec Modbus	DER Owner	Installer	DER Vendor/ Service Provider	3rd Party Aggregator	Utility/DSO	ISO/RTO/ TSO	Security Administrator	Security Auditor	RBAC Manager
Reactive susceptance that remains connected to the Area EPS in the cease-to-energize and trip state	DGEN.SuscRtg	AI21	DERCapability::rtgReactive Susceptance	702.ReactSusceptRtg	r--	r--	r--	r--	r--	r--	---	---	---
Manufacturer	LPHD.PhyNam.vendor		DeviceInformation::mfID	1.Mn	r--	r--	r--	r--	r--	r--	---	---	---
Model	LPHD.PhyNam.model		DeviceInformation::mfModel	1.Md	r--	r--	r--	r--	r--	r--	---	---	---
Serial Number	LPHD.PhyNam.serNum		DeviceInformation::mfSerNum	1.SN	r--	r--	r--	r--	r--	r--	---	---	---
Version	LPHD.PhyNam.swRev		DeviceInformation::mfHwVer DeviceInformation::swVer	1.Vr	r--	r--	r--	r--	r--	r--	---	---	---
Nameplate Storage Actual Capacity	DSTO.WhRtg	AI16	DERCapability::rtgOverExcitedW	713.WHRtg	r--	r--	r--	r--	r--	r--	---	---	---
IEEE 1547 Configuration data objects													
Active power rating at unity power factor (nameplate active power rating)	DGEN.WMax	AI4	DERCapability::rtgMaxW	702.WMax	r--	rw-	r--	r--	r--	r--	---	---	---
Active power rating at specified over-excited power factor	DGEN.WGnOvPFRtg	AI6 - AI7	DERCapability::rtgOverExcitedW	702.WMaxOvrExt	r--	rw-	r--	r--	r--	r--	---	---	---
Specified over-excited power factor	DGEN.OvPFRtg	AI8	DERCapability::rtgOverExcitedPF	702.WOvrExtPF	r--	rw-	r--	r--	r--	r--	---	---	---
Active power rating at specified under-excited power factor	DGEN.WGnUnPFRtg	AI9 - AI10	DERCapability::rtgUnderExcitedW	702.WMaxUndExt	r--	rw-	r--	r--	r--	r--	---	---	---
Specified under-excited power factor	DGEN.UnPFRtg	AI11	DERCapability::rtgUnderExcitedPF	702.WUndExtPF	r--	rw-	r--	r--	r--	r--	---	---	---
Apparent Power Maximum Rating	DGEN.VAMax		DERCapability::rtgMaxVA	702.VAMax	r--	rw-	r--	r--	r--	r--	---	---	---
Normal Operating Performance Category	DGEN.RegCap	AI22	DERCapability::rtgNormalCategory	702.NorOpCatRtg	r--	rw-	r--	r--	r--	r--	---	---	---
Abnormal Operating Performance Category	DGEN.RegCap	AI23	DERCapability::rtgAbnormalCategory	702.AbnOpCatRtg	r--	rw-	r--	r--	r--	r--	---	---	---
Reactive Power Injected Maximum Rating	DGEN.VarMaxSupRtg	AI12	DERCapability::rtgMaxVar	702.VarMaxInj	r--	rw-	r--	r--	r--	r--	---	---	---
Reactive Power Absorbed Maximum Rating	DGEN.VarMaxAbgRtg	AI13	DERCapability::rtgMaxVarNeg	702.VarMaxAbs	r--	rw-	r--	r--	r--	r--	---	---	---
Active Power Charge Maximum Rating	DSTO.WChaUnPFRtg	AI5	DERCapability::rtgMaxChargeRateW	702.WChaRteMax	r--	rw-	r--	r--	r--	r--	---	---	---

IEEE 1547 Data Requirements	Communication Protocol				Role								
	IEC 61850 Data Objects (LN.DO)	IEEE 1815 (DNP3) Uses IEC 61850 names	IEEE 2030.5	SunSpec Modbus	DER Owner	Installer	DER Vendor/ Service Provider	3rd Party Aggregator	Utility/DSO	ISO/RTO/ TSO	Security Administrator	Security Auditor	RBAC Manager
Apparent Power Charge Maximum Rating	DSTO.VAMaxChaRtg	AI15	DERCapability::rtgMaxChargeRateVA	702.VAChaRteMax	r--	rw-	r--	r--	r--	r--	---	---	---
AC voltage nominal rating	DECP.VRef	AI29 - AI30	DERCapability::rtgVNom	702.VNom	r--	rw-	r--	r--	r--	r--	---	---	---
AC voltage maximum rating	DGEN.VMax	AI3	DERCapability::rtgMaxV	702.VMax	r--	rw-	r--	r--	r--	r--	---	---	---
AC voltage minimum rating	DGEN.VMin	AI2	DERCapability::rtgMinV	702.VMin	r--	rw-	r--	r--	r--	r--	---	---	---
Supported Control Mode Functions	DVRT, DFRT, DFWP, DWLM, DVWC, DFWC, DVAR, DFPF, DVVC, DWVR	BI31 - BI51	DERCapability::modesSupported	702.CtrlModes	r--	rw-	r--	r--	r--	r--	---	---	---
Reactive susceptance that remains connected to the Area EPS in the cease-to-energize and trip state	DGEN.SuscRtg	AI21	DERCapability::rtgReactiveSusceptance	702.ReactSusceptRtg	r--	rw-	r--	r--	r--	r--	---	---	---
Manufacturer	LPHD.PhyNam.vendor		DeviceInformation::mfID	1.Mn	r--	rw-	r--	r--	r--	r--	---	---	---
Model	LPHD.PhyNam.model		DeviceInformation::mfModel	1.Md	r--	rw-	r--	r--	r--	r--	---	---	---
Serial Number	LPHD.PhyNam.serNum		DeviceInformation::mfSerNum	1.SN	r--	rw-	r--	r--	r--	r--	---	---	---
Version	LPHD.PhyNam.swRev		DeviceInformation::mfHwVer DeviceInformation::swVer	1.Vr	r--	rw-	r--	r--	r--	r--	---	---	---
Storage Actual Capacity	DSTO.WhRtg	AI16	DERCapability::rtgOverExcitedW	713.WHRtg	r--	rw-	r--	r--	r--	r--	---	---	---
Monitoring information requirement													
Active Power	DECP.MMXU.TotW	AI537	ReadingType::accumulationBehaviour = 12 ReadingType::commodity = 1 ReadingType::flowDirection = 19 ReadingType::kind = 37 ReadingType::uom = 38	701.W	r--	r--	r--	r--	r--	r--	---	---	---

IEEE 1547 Data Requirements	Communication Protocol				Role								
	IEC 61850 Data Objects (LN.DO)	IEEE 1815 (DNP3) Uses IEC 61850 names	IEEE 2030.5	SunSpec Modbus	DER Owner	Installer	DER Vendor/ Service Provider	3rd Party Aggregator	Utility/DSO	ISO/RTO/ TSO	Security Administrator	Security Auditor	RBAC Manager
Reactive Power	DECP.MMXU.TotVAr	AI541	ReadingType::accumulationBehaviour = 12 ReadingType::commodity = 1 ReadingType::flowDirection = 19 ReadingType::kind = 37 ReadingType::uom = 63	701.Var	r--	r--	r--	r--	r--	r--	---	---	---
Voltage(s)	DECP.MMXU.PhV.phsA.mag DECP.MMXU.PhV.phsB.mag DECP.MMXU.PhV.phsC.mag	AI547 - AI553	ReadingType::accumulationBehaviour = 12 ReadingType::commodity = 1 ReadingType::flowDirection = 1 ReadingType::phase = {phase} ReadingType::uom = 29	701.LLV 701.LNV 701.VL1 701.VL2 701.VL3	r--	r--	r--	r--	r--	r--	---	---	---
Frequency	DECP.MMXU.Hz	AI536	ReadingType::accumulationBehaviour = 12 ReadingType::commodity = 1 ReadingType::flowDirection = 1 ReadingType::uom = 33	701.Hz	r--	r--	r--	r--	r--	r--	---	---	---
Operational State	DGEN.DERState	BI10 - BI24	DERStatus::operationalModeStatus	701.St	r--	r--	r--	r--	r--	r--	---	---	---
Connection Status	DSTO.DERState.1	BI10 - BI24	DERStatus::genConnectStatus DERStatus::storConnectStatus	701.ConnSt	r--	r--	r--	r--	r--	r--	---	---	---
Alarm Status	CALH.GrAlm	BI0 - BI9	DERStatus::alarmStatus	701.Alrm	r--	r--	r--	r--	r--	r--	---	---	---
Operational State of Charge	DSTO.SocUsePct	AI48	DERStatus::stateOfChargeStatus	713.SoC	r--	r--	r--	r--	r--	r--	---	---	---
Constant power factor function													
Constant power factor mode enable	DFPF.ModEna	BI80	Active Event	704.PFWInjEna 704.PFWAbsEna	---	r--	r--	rw-	rw-	r--	---	---	---
Constant power factor setting	DFPF.PFGnTgt DFPF.PFLodTgt	AI288 - AI289	DERControl::opModFixedPFInjectW	704.DERCtlAC.PFWInj.PF 704.DERCtlAC.PFWAbs.PF	---	r--	r--	rw-	rw-	r--	---	---	---

IEEE 1547 Data Requirements	Communication Protocol				Role								
	IEC 61850 Data Objects (LN.DO)	IEEE 1815 (DNP3) Uses IEC 61850 names	IEEE 2030.5	SunSpec Modbus	DER Owner	Installer	DER Vendor/ Service Provider	3rd Party Aggregator	Utility/DSO	ISO/RTO/ TSO	Security Administrator	Security Auditor	RBAC Manager
Constant power factor excitation setting	DFPF.PFExtSet	BI29 - BI30	DERControl::opModFixedPFInjectW.excitation	704.DERCtlAC.PFWInj.Ext 704.DERCtlAC.PFWAbs.Ext	---	r--	r--	rw-	rw-	r--	---	---	---
Voltage-reactive power (volt-var) function													
Voltage-Reactive Power Mode Enable	DVVR.ModEna	BI81	Active Event	705.Ena	---	r--	r--	rw-	rw-	r--	---	---	---
V_{Ref} Reference Voltage	DECP.VRef	AI29 - AI30	DERCurve::vRef	705.DERVoltVar.Crv.VRef	---	r--	r--	rw-	rw-	r--	---	---	---
Autonomous V_{Ref} Adjustment Enable	DECP.VRefOfs	BI93	DERCurve::autonomousVRefEnable	705.DERVoltVar.Crv.VRefAuto	---	r--	r--	rw-	rw-	r--	---	---	---
V_{Ref} Adjustment Time Constant		AI300	DERCurve::autonomousVRefTime Constant	705.DERVoltVar.Crv.VRefAutoTms	---	r--	r--	rw-	rw-	r--	---	---	---
V/Q Curve Points	DVVR.VVArCrv	AI303	DERControl::opModVoltVar::CurveData	705.DERVoltVar.Crv.Pt.V/Var	---	r--	r--	rw-	rw-	r--	---	---	---
Open Loop Response Time	DVVR.OpnLoopMax	AI298 - AI299	DERControl::opModVoltVar::openLoopTms	705.DERVoltVar.Crv.RspTms	---	r--	r--	rw-	rw-	r--	---	---	---
Active power-reactive power (watt-var) function													
Active-Reactive Power Mode Enable	DWVR.ModEna	BI82	Active Event	712.Ena	---	r--	r--	rw-	rw-	r--	---	---	---
P/Q Curve Points	DWVR.WVArCrv	AI308, AI328 - AI532	DERControl::opModWattVar::CurveData	712.DERWattVar.Crv.Pt.W/Var	---	r--	r--	rw-	rw-	r--	---	---	---
Constant reactive power (fixed var) function													
Constant Reactive Power Mode Enable	DVAR.ModEna	BI79	Active Event	704.VarSetEna	---	r--	r--	rw-	rw-	r--	---	---	---
Constant Reactive Power	DVAR.VArTgt	AI281	DERControl::opModFixedVar DERControl::opModTargetVar	704.VarSet	---	r--	r--	rw-	rw-	r--	---	---	---
Voltage-active power (volt-watt) function													

IEEE 1547 Data Requirements	Communication Protocol				Role								
	IEC 61850 Data Objects (LN.DO)	IEEE 1815 (DNP3) Uses IEC 61850 names	IEEE 2030.5	SunSpec Modbus	DER Owner	Installer	DER Vendor/ Service Provider	3rd Party Aggregator	Utility/DSO	ISO/RTO/ TSO	Security Administrator	Security Auditor	RBAC Manager
Voltage-Active Power Mode Enable	DVWC.ModEna	BI77	Active Event	706.Ena	---	r--	r--	rw-	rw-	r--	---	---	---
V/P Curve Points	DVWC.VWCrv	AI248, AI328 - AI532	DERControl::opModVoltWatt::CurveData	706.DERVoltWatt.Crv.Pt.V/W	---	r--	r--	rw-	rw-	r--	---	---	---
Open Loop Response Time	DVWC.OpnLoopMax	AI251 - AI252	DERControl::opModVoltWatt::openLoopTms	706.DERVoltWatt.RspTms	---	r--	r--	rw-	rw-	r--	---	---	---
Voltage trip function													
HV Trip Curve Points	DHVT.TrZnSt PTOV.TmVCrv	AI73 AI328 - AI532	DERControl::opModHVRTMustTrip::CurveData	708.DERTripHF.Crv.MustTrip.Pt.V/Tms	---	rw-	r--	rw-	rw-	r--	---	---	---
LV Trip Curve Points	DLVT.TrZnSt PTUV.TmVCrv	AI74, AI328 - AI532	DERControl::opModLVRTMustTrip::CurveData	707.DERTripLV.Crv.MustTrip.Pt.V/Tms	---	rw-	r--	rw-	rw-	r--	---	---	---
Voltage momentary cessation function													
HV Momentary Cessation Curve Points	DHVT.CeaZnSt PTOV.TmVCrv	AI75, AI328 - AI532	DERControl::opModHVRTMomentaryCessation::CurveData	708.DERTripHF.Crv.MomCess.Pt.V/Tms	---	rw-	r--	rw-	rw-	r--	---	---	---
LV Momentary Cessation Curve Points	DLVT.CeaZnSt PTUV.TmVCrv	AI76, AI328 - AI532	DERControl::opModLVRTMomentaryCessation::CurveData	707.DERTripLV.Crv.MomCess.Pt.V/Tms	---	rw-	r--	rw-	rw-	r--	---	---	---
Frequency-trip function													
HF Trip Curve Points	DHFT.TrZnSt PTOF.StrVal	AI79, AI328 - AI532	DERControl::opModHFRTMustTrip::CurveData	710.DERTripHF.Crv.MustTrip.Pt.Hz/Tms	---	rw-	r--	rw-	rw-	r--	---	---	---
LF Trip Curve Points	DLFT.TrZnSt PTUF.StrVal	AI80, AI328 - AI532	DERControl::opModLFRTMustTrip::CurveData	709.DERTripLF.Crv.MustTrip.Pt.Hz/Tms	---	rw-	r--	rw-	rw-	r--	---	---	---
Frequency droop function													
Overfrequency Droop *db*OF	DHFW.HzStr	AI121 - AI122	DERControl::opModFreqDroop::dBOF	711.Ctl.DbOf	---	rw-	r--	rw-	rw-	r--	---	---	---
Underfrequency Droop *db*UF	DLFW.HzStr	AI125 - AI126	DERControl::opModFreqDroop::dBUF	711.Ctl.DbUf	---	rw-	r--	rw-	rw-	r--	---	---	---
Overfrequency Droop *k*OF	DHFW.WGra	AI123 - AI124	DERControl::opModFreqDroop::kOF	711.Ctl.KOf	---	rw-	r--	rw-	rw-	r--	---	---	---
Underfrequency Droop *k*UF	DLFW.WGra	AI127 - AI128	DERControl::opModFreqDroop::kUF	711.Ctl.KUf	---	rw-	r--	rw-	rw-	r--	---	---	---

IEEE 1547 Data Requirements	Communication Protocol				Role								
	IEC 61850 Data Objects (LN.DO)	IEEE 1815 (DNP3) Uses IEC 61850 names	IEEE 2030.5	SunSpec Modbus	DER Owner	Installer	DER Vendor/ Service Provider	3rd Party Aggregator	Utility/DSO	ISO/RTO/ TSO	Security Administrator	Security Auditor	RBAC Manager
Open Loop Response Time	DHFW.OpnLoopMax DLFW.OpnLoopMax	AI131 - AI132	DERControl::opModFreqDroop::openLoopTms	711.Ctl.RspTms	---	rw-	r--	rw-	rw-	r--	---	---	---
Enter service function													
Permit service	DCTE.RtnSrvAuto DCTE.RtnSrvAuth	BI16	DERControl::opModEnergize	703.ES	r--	rw-	r--	rw-	rw-	r--	---	---	---
ES Voltage High	DCTE.VHiLim	AI50	DERSettings::setESHighVolt DefaultDERControl::setESHighVolt	703.ESVHi	---	rw-	r--	rw-	rw-	r--	---	---	---
ES Voltage Low	DCTE.VLoLim	AI51	DERSettings::setESLowVolt DefaultDERControl::setESLowVolt	703.ESVLo	---	rw-	r--	rw-	rw-	r--	---	---	---
ES Frequency High	DCTE.HzHiLim	AI52	DERSettings::setESHighFreq DefaultDERControl::setESHighFreq	703.ESHzHi	---	rw-	r--	rw-	rw-	r--	---	---	---
ES Frequency Low	DCTE.HzLoLim	AI53	DERSettings::setESLowFreq DefaultDERControl::setESLowFreq	703.ESHzLo	---	rw-	r--	rw-	rw-	r--	---	---	---
ES Delay	DCTE.RtnSrvDlyTim	AI54	DERSettings::setESDelay DefaultDERControl::setESDelay	703.ESDlyTms	---	rw-	r--	rw-	rw-	r--	---	---	---
ES Randomized Delay	DCTE.RtnSrvDlyTim	AI55	DERSettings::setESRandomDelay DefaultDERControl::setESRandom Delay	703.ESRndTms	---	rw-	r--	rw-	rw-	r--	---	---	---
ES Ramp Time	DCTE.RtnSrvRmpTim	AI56	DERSettings::setESRampTms DefaultDERControl::setESRampTms	703.ESRmpTms	---	rw-	r--	rw-	rw-	r--	---	---	---
Limit active power													
Limit Active Power Enable	DWMX.ModEna DWMN.ModEna	BI69	Active Event	704.WMaxLimPctEna	r--	rw-	r--	rw-	rw-	r--	---	---	---
Maximum Active Power	DWMX.LimW DWMN.LimW	AI148 - AI149	DERControl::opModMaxLimW	704.WMaxLimPct	r--	rw-	r--	rw-	rw-	r--	---	---	---

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Charles Hanley	08810	cjhanle@sandia.gov
Jennifer Depoy	05620	depoy@sandia.gov
Summer Ferreira	08812	srferre@sandia.gov
Brian Gaines	09366	bgaines@sandia.gov
Jay Johnson	08812	jjohns2@sandia.gov
Ifeoma Onunkwo	09366	ionunkw@sandia.gov
Technical Library	01977	sanddocs@sandia.gov

Email—External

Name	Company Email Address	Company Name
Jeremiah Miller	jeremiah.miller@ee.doe.gov	U.S. Department of Energy
Guohui Yuan	guohui.yuan@ee.doe.gov	U.S. Department of Energy

This page left blank

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.