Data Track
Technology Inc

sales.us@dtrack.com
1-201-404-2248
website: us.dtrack.com

Smart Grid Networks
Securing Cyber Assets

THE CHALLENGES OF SECURE SMART GRID NETWORKS

TCP/IP technology has extended into every aspect of data, voice, and control networks. The benefits of standards-based solutions being integrated into the legacy networks of utilities far outweigh the expense of the engineering and maintenance efforts. They start with the ease of evolving scalable and secure solutions as the needs of a Smart Grid utility grow, and extend onward to reduced costs and increased productivity right from the start of deployment. Data Track Technology has solutions that utilities are using today for complying with NERC CIP and NIST cyber security requirements.
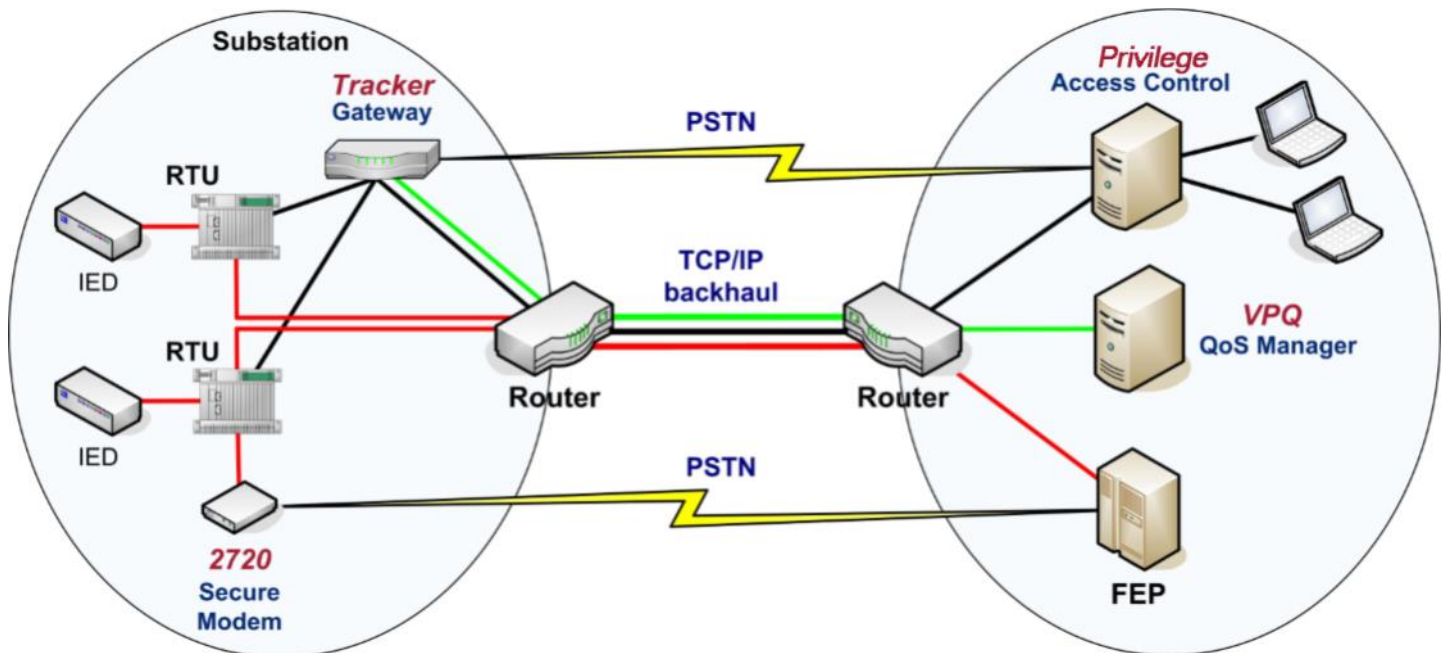
Secure maintenance access, event notification, and network QoS for
SCADA, AMI, VoIP, and other substation TCP/IP traffic

DATA TRACK'S SOLUTION

Tracker Access Gateway	Privilege Access Control	Management Applications
Routing, firewalling, VPN server/client	Authentication, authorization, access	Tracker access gateway management
Serial to TCP/IP Ethernet conversion	In-band access to managed devices	Device alarm management console
Out-of-band access, AES authentication	Out-of-band access, AES authentication	Authentication credential management
Device event capture / filter / forward	Multi-protocol support for audit log-	QoS compliance assessment
Extensive, automated audit generation	Automated audit collection, reporting	QoS performance, utilization monitor-
Physical security gateway with alarm-ing	Automated password management	QoS configuration management
Environmental monitoring and alarm-ing	Browser-based interface	Browser-based interfaces

Mapping Data Track's Solution to NERC CIP Standards

Since 1979, Data Track Technology has been developing secure communications management solutions for service providers and enterprises, including electric power utilities. The following table summarizes where Data Track's Secure Access solution lines up with NERC CIP requirements regarding Smart Grid infrastructure cyber security. For more details, see our web site for a series of white papers on securing administrative access, and managing TCP/IP Quality of

NERC Requirement	Data Track Solution Feature
CIP-005 Electronic Security Perimeter	
R2. Electronic Access Controls	
R2.1 – Deny access by default	Access to all features and ports within the Tracker denied as default.
R2.2 – Enable only necessary ports	Tracker administrator enables serial, Ethernet, and TCP/IP ports needed.
R2.3 – Secure dial-up access	Secured by: restricted answering, two factor authentication, firewall, VPN, login, etc.
R2.4 – Strong technical controls	Tracker employs secure lock and key model out-of-band using AES technology.
R2.6 – Appropriate use banner	Tracker administrator creates and maintains an "appropriate use" banner as required.
R3. Monitoring Electronic Access	
R3.1 – Dial-up access monitoring	Tracker access control is monitored, logged, and alerted as configured by administrator.
R3.2 – Unauthorized access attempts	Unauthorized and failed access attempts are automatically detected, logged, and alerted.
CIP-007 Systems Security Management	
R2. Ports and Services	
R2.1 – Enable only necessary ports	Tracker administrator enables serial, Ethernet, and TCP/IP ports needed.
R2.2 – Disable unnecessary ports	Tracker administrator disables unneeded serial, Ethernet, and TCP/IP ports.
R5. Account Management	
R5.1 – Limit permissions	Multi-level user profiles within Privilege, and Tracker user profiles limit permissions.
R5.1.2 – Access audit trail	Audit facilities within Privilege and Tracker give multiple levels of audit logging.
R5.2 – Manage scope of system accounts	Privilege allows for centralized management of system accounts, including on Tracker.
R5.2.3 – Auditing system accounts	Privilege has automated auditing facilities on per Privilege and per Tracker user bases.
R6. Security Status Monitoring	
R6.2 – Security status alerting	Unauthorized activity is detected, logged, and alerted as configured by administrator.
R6.3 – Security status logging	Access logs within Privilege and Tracker are maintained and forwarded automatically.

D a t a   T r a c k   T e c h n o l o g y   i s   a n   I S O   9 0 0 1 : 2 0 0 8   q u a l i t y   c e r t i f i e d   c o m p a n y