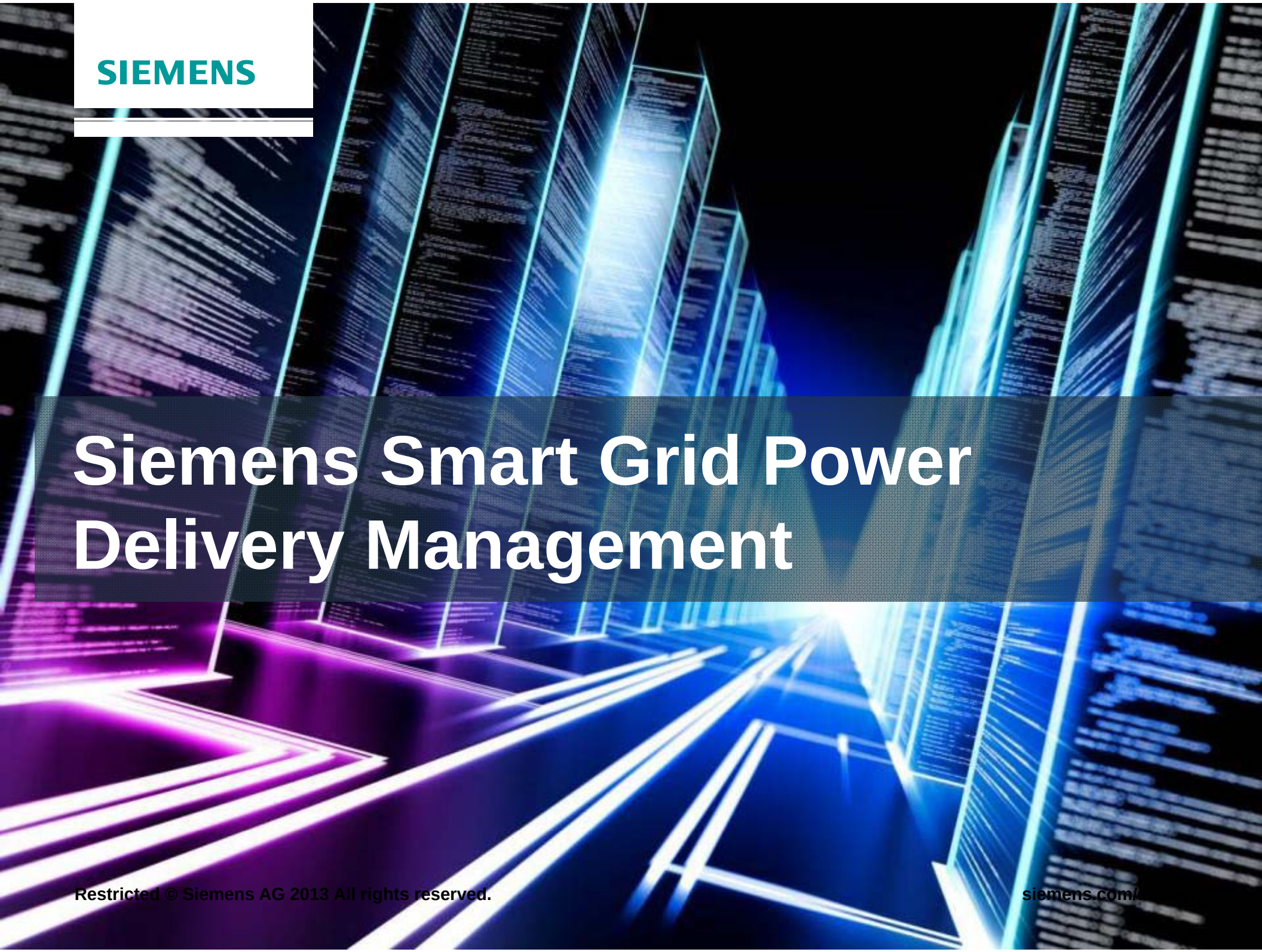

Problem at hand

Today's Data Center Challenges

- U.S. Federal Government Data Centers require robust cyber-security for required services, including facility electric power, cooling and networks.
- Other critical data centers either must already meet stringent cyber-security requirements or this will be mandated in the future.
- Other data centers should have robust cyber-security as part of due diligence, and to avoid extended downtime after an attack.

Power demands of today's and future data centers are radically different and are in a constant state of change.

Solution

Siemens has been a leader in cyber-security for many years.

All of the Smart Grid Division's SCADA, Energy Automation and Energy Management Systems have industry-leading cyber-security protection.

Basic cyber security functions for Data Centers:

- Establish a clearly-defined and well-managed security perimeter.
- Defense-in-depth places multiple barriers between threats and assets.
- Patch management assures assets always have the most current protection.
- User authentication, password management, automatic privilege assignment and fine access granularity assures users only have required system access.
- We offer many cyber-security options for the most sensitive systems.

Smart Grid Standard Cyber-Security Features:
User authentication with definition of password, log-on and log-off policies
Detailed privilege management
Recording all user activities including log-on and log-off events

Best Practice

- **Proven Technology**
- Over 50 systems delivered that are designed to meet DHS/FERC Critical Infrastructure Protection requirements
- Cyber-security leadership: Siemens will provide secure systems today that can expand to meet future requirements.
- Many standard and optional cyber - security applications and services: get what you need when you need it.