WEAT Webinar

Who Goes There?
Access Control in Water/Wastewater

siemens.com/ruggedcom

ACCESS CONTROL WEBINAR
TABLE OF CONTENTS

TOPIC

- Why Access Control?
- Risks If Not Used
- Factors of Authentication
- Role-Based Access Control
- NIST & AWWA Guidelines for Access Control
- Ways to Enforce Access Control
- Summary

Why Access Control?

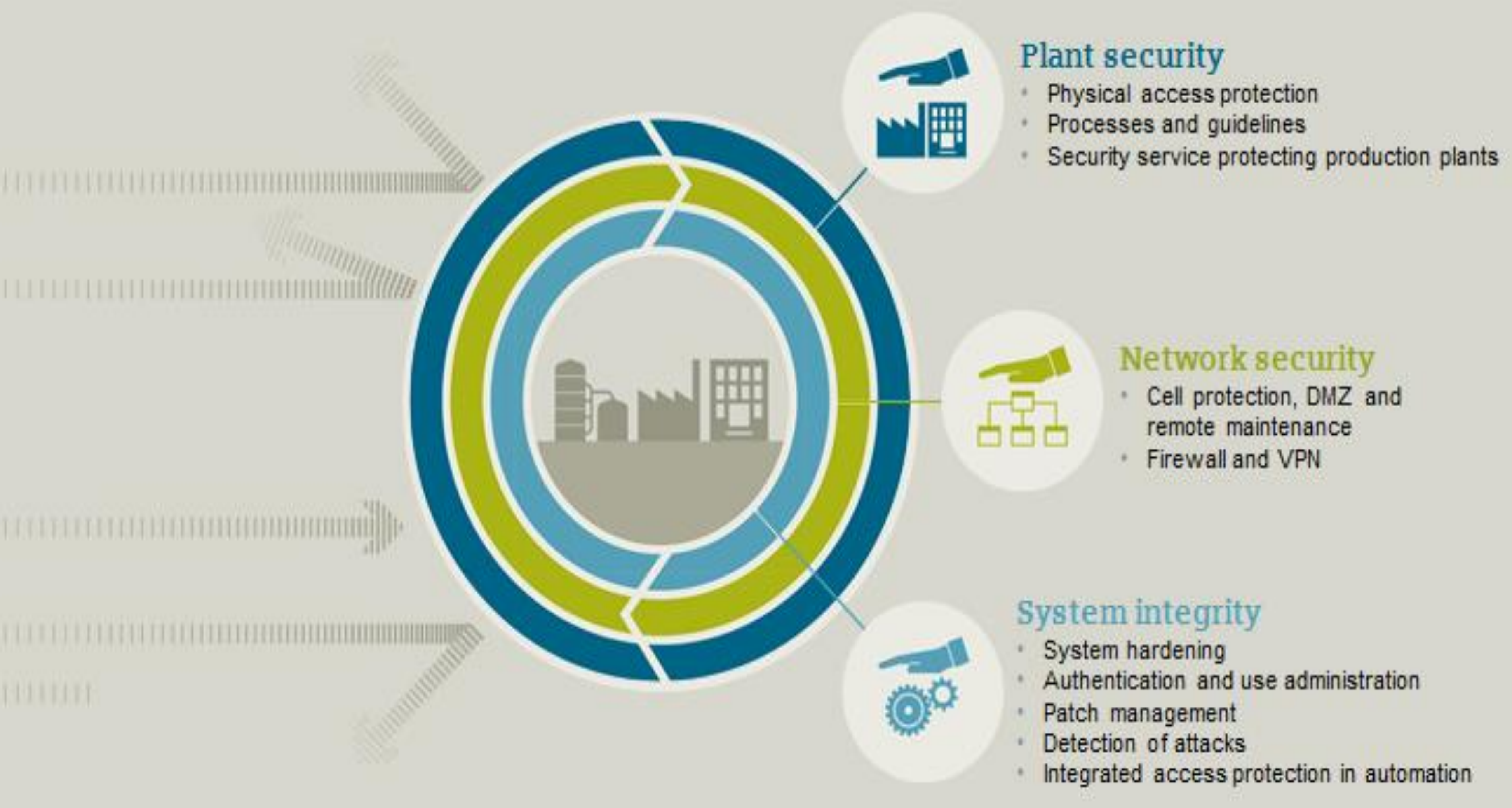
Access Control is a key component to a layered defense strategy. It's tough to hack something if you cannot get in.

Access control tries to ensure that no unauthorized parties can get into a system.

ACCESS CONTROL

The **principle of least privilege** (PoLP) is an information security term that refers to a user or program having the least authority possible to perform its job

DEFENSE IN DEPTH



Plant security

- Physical access protection
- Processes and guidelines
- Security service protecting production plants

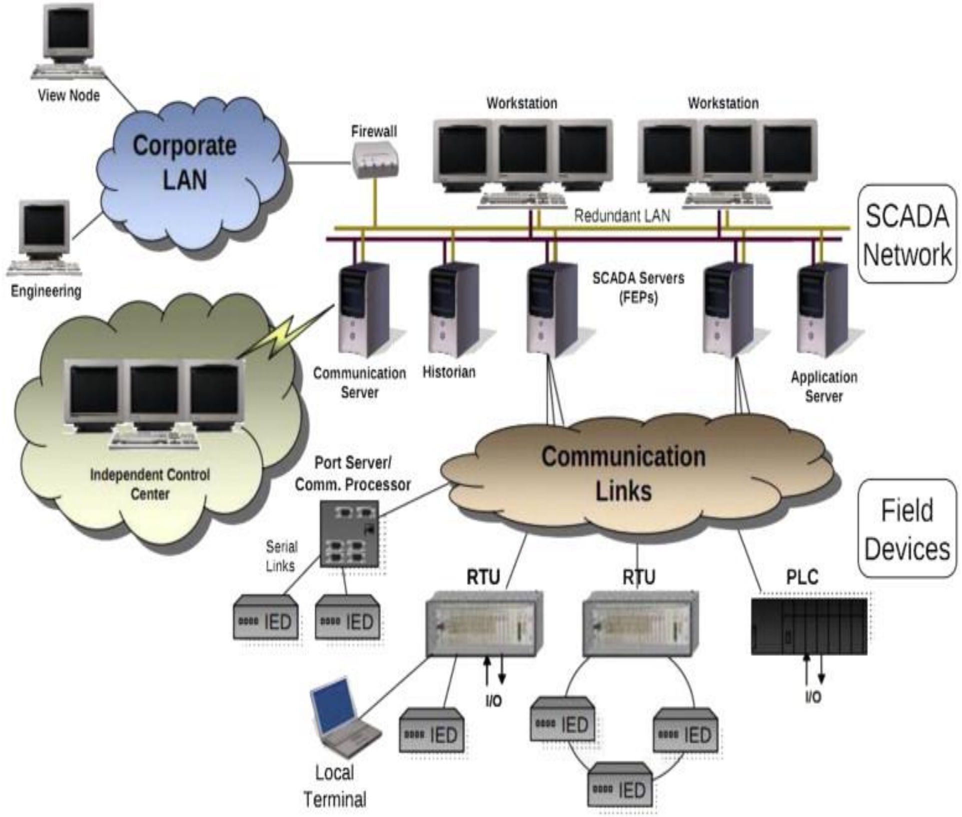
Network security

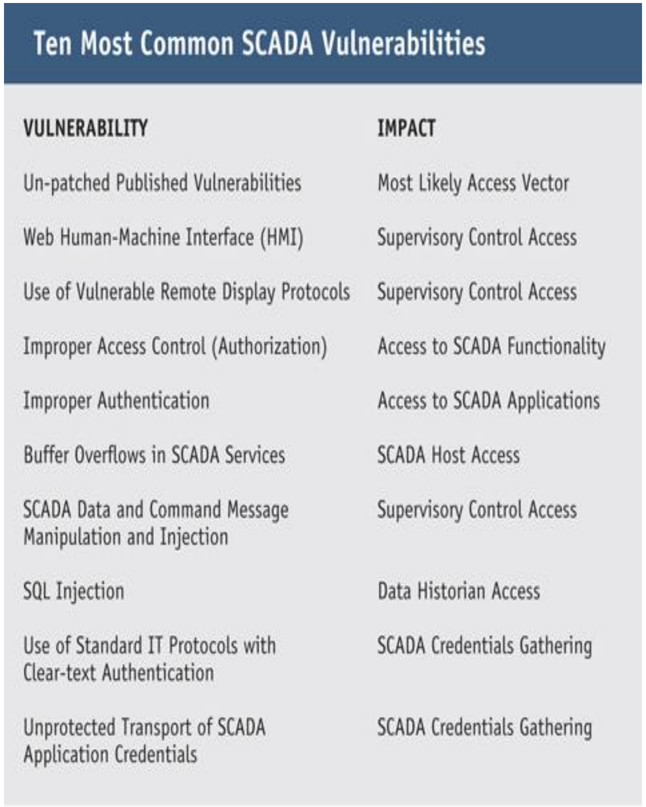
- Cell protection, DMZ and remote maintenance
- Firewall and VPN

System integrity

- System hardening
- Authentication and use administration
- Patch management
- Detection of attacks
- Integrated access protection in automation

SCADA VULNERABILITIES





Ten Most Common SCADA Vulnerabilities

VULNERABILITY	IMPACT
Un-patched Published Vulnerabilities	Most Likely Access Vector
Web Human-Machine Interface (HMI)	Supervisory Control Access
Use of Vulnerable Remote Display Protocols	Supervisory Control Access
Improper Access Control (Authorization)	Access to SCADA Functionality
Improper Authentication	Access to SCADA Applications
Buffer Overflows in SCADA Services	SCADA Host Access
SCADA Data and Command Message Manipulation and Injection	Supervisory Control Access
SQL Injection	Data Historian Access
Use of Standard IT Protocols with Clear-text Authentication	SCADA Credentials Gathering
Unprotected Transport of SCADA Application Credentials	SCADA Credentials Gathering

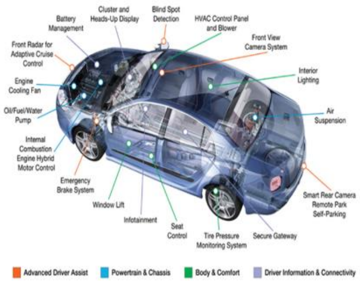
SECURITY PHASE CHANGE

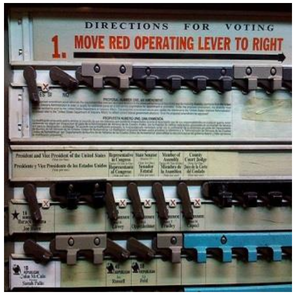
Security Phase Change describes devices that transition from electrical to computer-controlled to eventually networked.

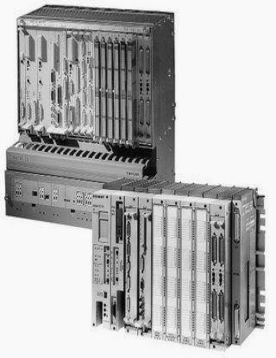
- Automobiles
- Voting machines
- Programmable Logic Controllers (PLCs)

LEGACY

MODERN

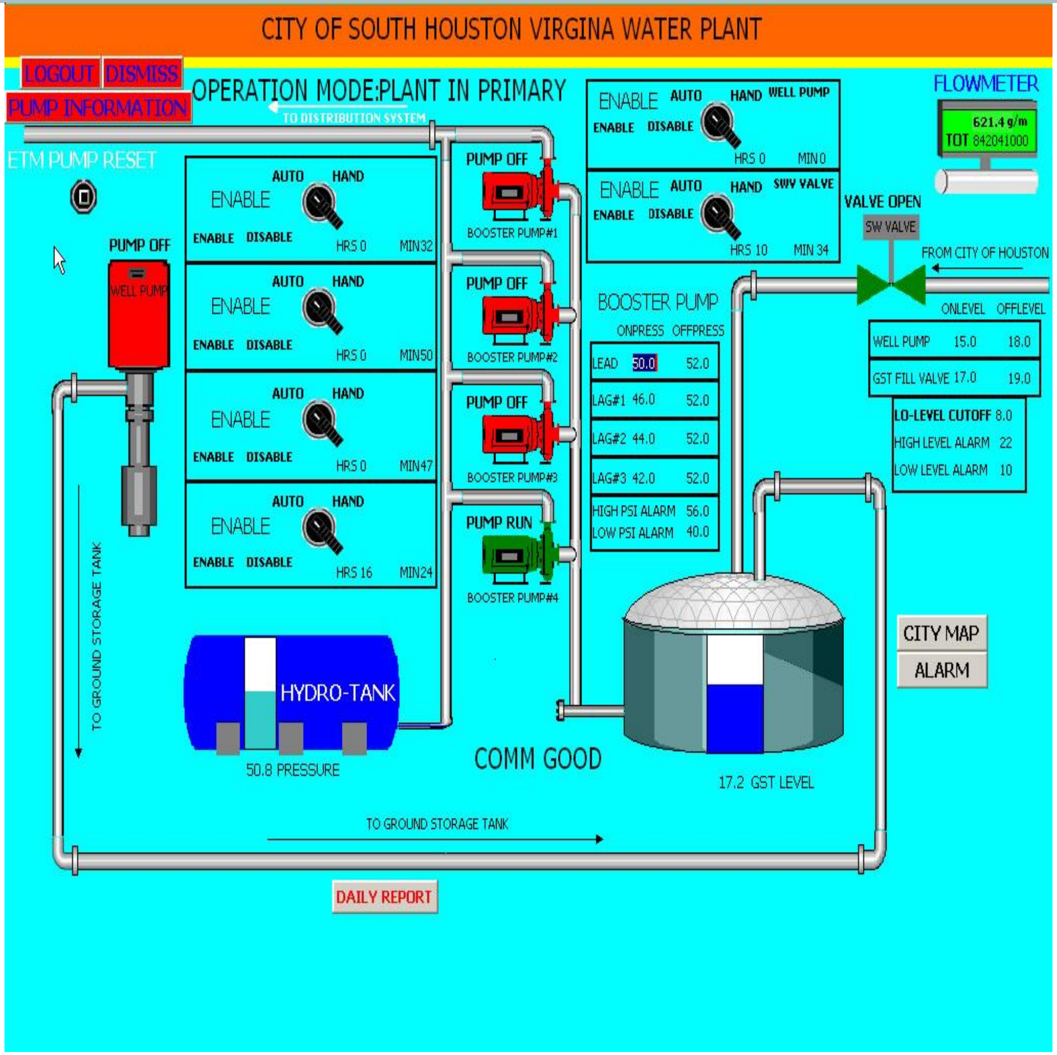






SOUTH HOUSTON WATER HACK

- In 2011, the City of South Houston Water Department was hacked
- The hacker provided documents from the plant as proof
- Poor configuration of services, bad passwords, and no access controls for SCADA interfaces were blamed



CYBER SECURITY STATISTICS

Can you name three of the top five countries where hacks originate?

China, USA (17%), Turkey, Brazil and Russia

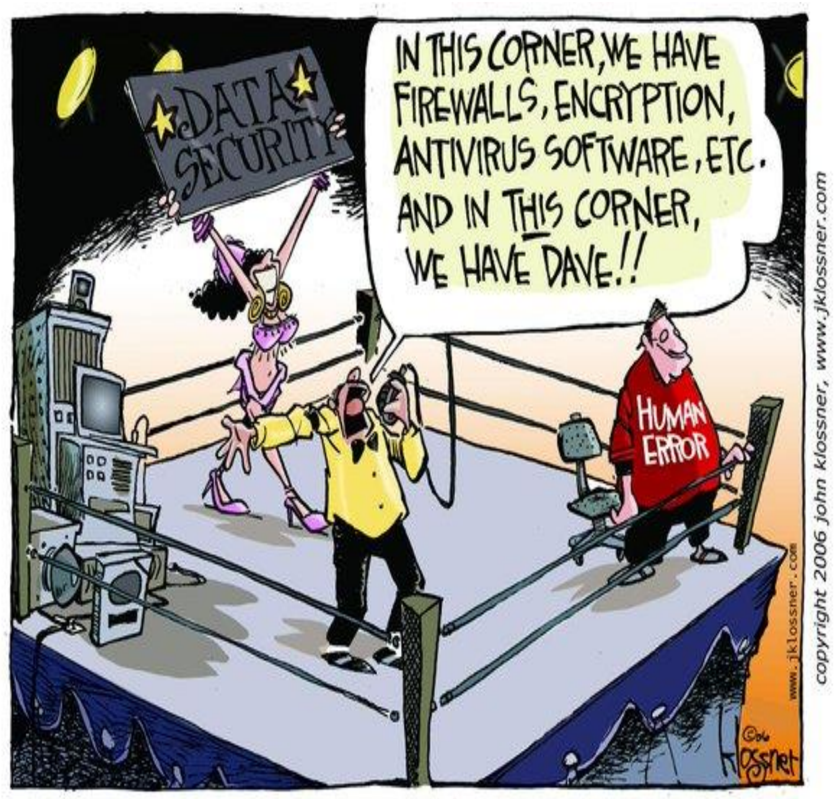
What famous billionaire said cyberattacks are the greatest threat to mankind – even more of a threat than nuclear weapons?

Warren Buffet

Which country has the highest number of malware-infected computers in the world?

China at 57%. Runner-up is Taiwan at 49% followed by Turkey at 42.5%.

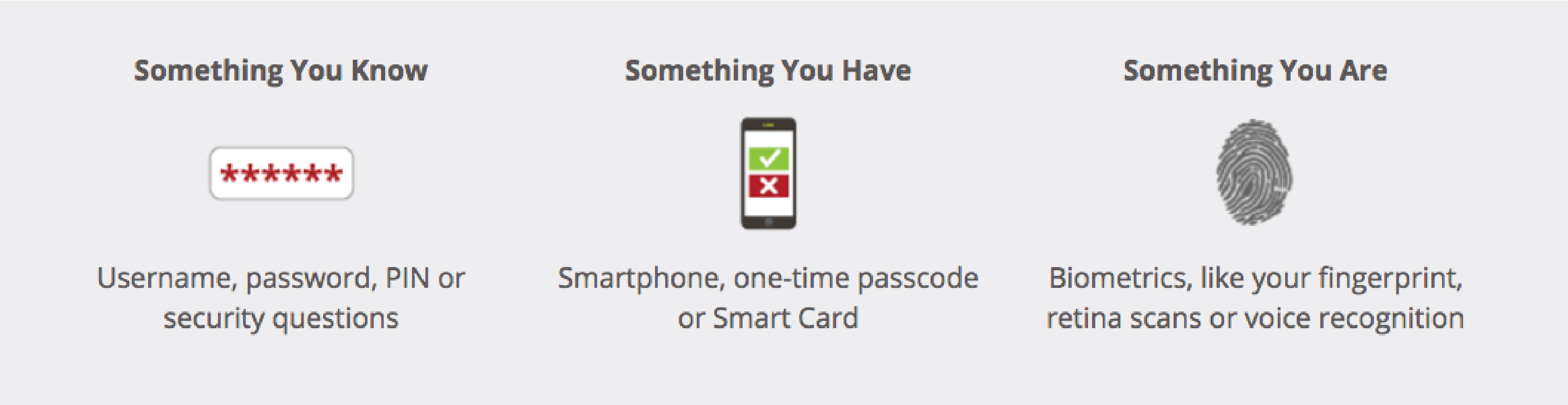
WHY PCS SECURITY IS DIFFICULT


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
copyright 2006 john klossner, www.jklossner.com
www.jklossner.com
©06 klossner

FACTORS OF AUTHENTICATION

What is a factor?

A factor is a type of authentication. When you claim to be someone, you need to provide further information to prove that you are who you say you are.



Something You Know

Username, password, PIN or security questions

Something You Have

Smartphone, one-time passcode or Smart Card

Something You Are

Biometrics, like your fingerprint, retina scans or voice recognition

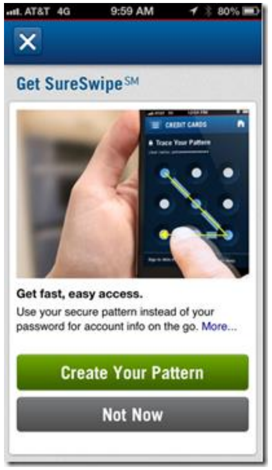
FACTORS OF AUTHENTICATION

Factor #4: Somewhere you are

- Internet Protocol (IP) address
- Media Access Control (MAC) address
- Geolocation services

Factor #5: Something you do

- Windows 8 Picture Password
- SureSwipe login from Capital One



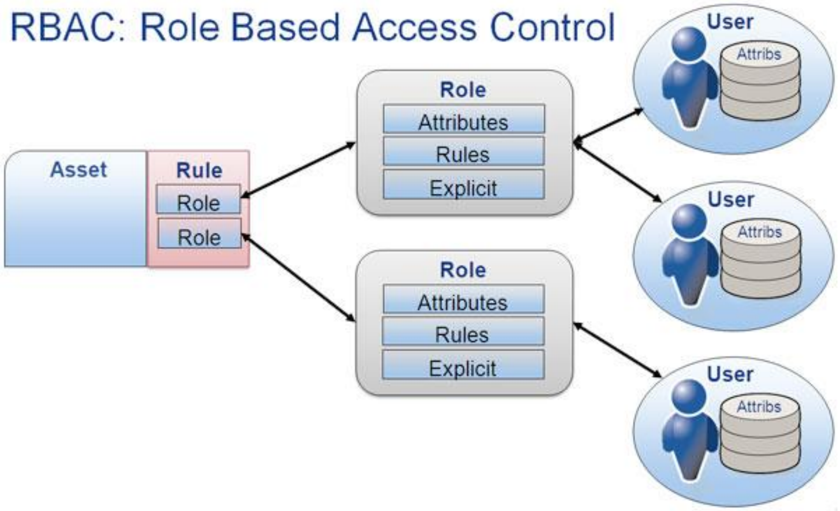
Get SureSwipe^{SM}

Get fast, easy access.

Use your secure pattern instead of your password for account info on the go. More...

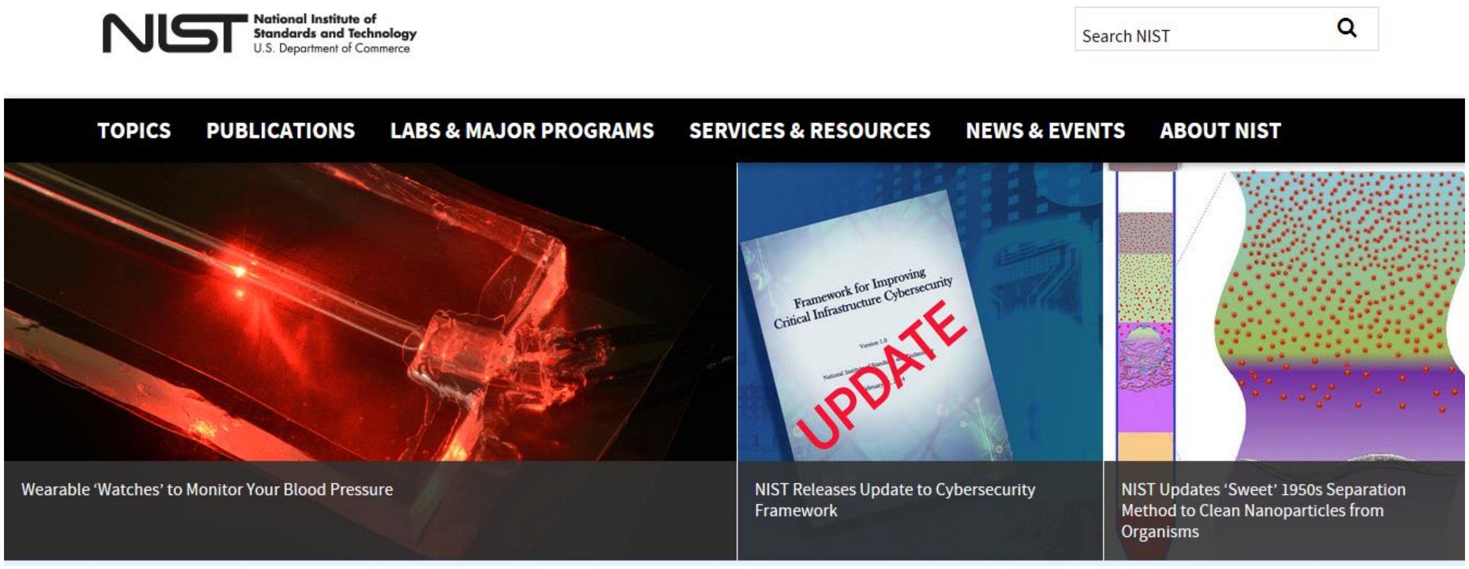
Role-Based Access Control

RBAC defines the users' security roles, permissions, authorization, and role hierarchy to access critical systems in an industrial control system (ICS).



NATIONAL INSTITUTE of STANDARDS and TECHNOLOGY (NIST)

The National Institute of Standards and Technology (NIST) was founded in 1901 and now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. Congress established the agency to remove a major challenge to U.S. industrial competitiveness at the time—a second-rate measurement infrastructure that lagged behind the capabilities of the United Kingdom, Germany, and other economic rivals.


NIST
National Institute of Standards and Technology
U.S. Department of Commerce
Search NIST
TOPICS
PUBLICATIONS
LABS & MAJOR PROGRAMS
SERVICES & RESOURCES
NEWS & EVENTS
ABOUT NIST
Framework for Improving Critical Infrastructure Cybersecurity
Version 1.0
UPDATE

Wearable 'Watches' to Monitor Your Blood Pressure

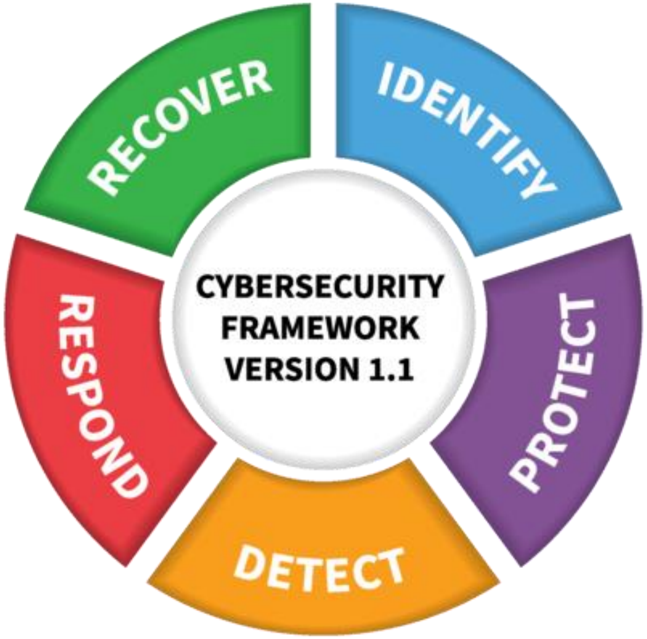
NIST Releases Update to Cybersecurity Framework

NIST Updates 'Sweet' 1950s Separation Method to Clean Nanoparticles from Organisms

NATIONAL INSTITUTE of STANDARDS and TECHNOLOGY (NIST)

The NIST Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover.

- **Identify**
  - Assets
- **Protect**
  - Access Control
  - Data Security
  - Information Protection
  - Protective Technology
- **Detect**
  - Configuration Management
  - Firewall Management
  - Authorized Access



NIST GUIDELINES
Identity Management, Authentication and Access Control

Access to physical and logical assets and facilities limited to authorized users, processes and devices managed according to the assessed risk.

- PR.AC-1: Identities and credentials managed/verified for authorized devices, users and processes
- PR.AC-2: Physical access to assets managed and protected
- PR.AC-3: Remote access managed
- PR.AC-4: Access permissions managed using least privilege and separations of duty

- PR.AC-5: Network integrity is protected (segregation, segmentation)
- PR.AC-6: Identities proofed and bound to credentials
- PR.AC-7: Users, devices, and other assets authenticated (single-factor/multi-factor) commensurate with the risk of the transaction (individual and organizational risks)

WATER/WASTEWATER CYBERSECURITY GUIDELINES

American Water Works Association

- AWWA using NIST as guide
- Updated guideline issued in 2017
- Security framework includes best practices from NIST, AWWA, WaterISAC and others

Practice Categories:

- Governance and Risk Management
- Business Continuity/Disaster Recovery
- Server and Workstation Hardening
- Access Control
- Application Security
- Encryption
- Telecom, Network Security & Architecture
- Physical Security
- Service Level Agreements (SLAs)
- Operations Security (OPSEC)
- Education
- Personnel Security

SECURE COMMUNICATIONS

Unprotected wired and wireless communications can be intercepted or manipulated in transit.

Preventative Controls:

- **Secure Channel**
  - Cryptography
- **Robust Channel**
  - Cryptography
- **Available Channel**
  - Anti-Denial of Service
  - Anomaly Detection
- **Device Hardening**
  - Robust access controls
  - Patch management

SECURE REMOTE ACCESS

Good Practices for Secure Remote Access

- Undertake a formal threat and risk assessment
- Eliminate all direct connections to critical assets
- Secure modem access
- Use Demilitarized Zones (DMZ) to segment business and control architecture
- Establish user-specific authentication servers

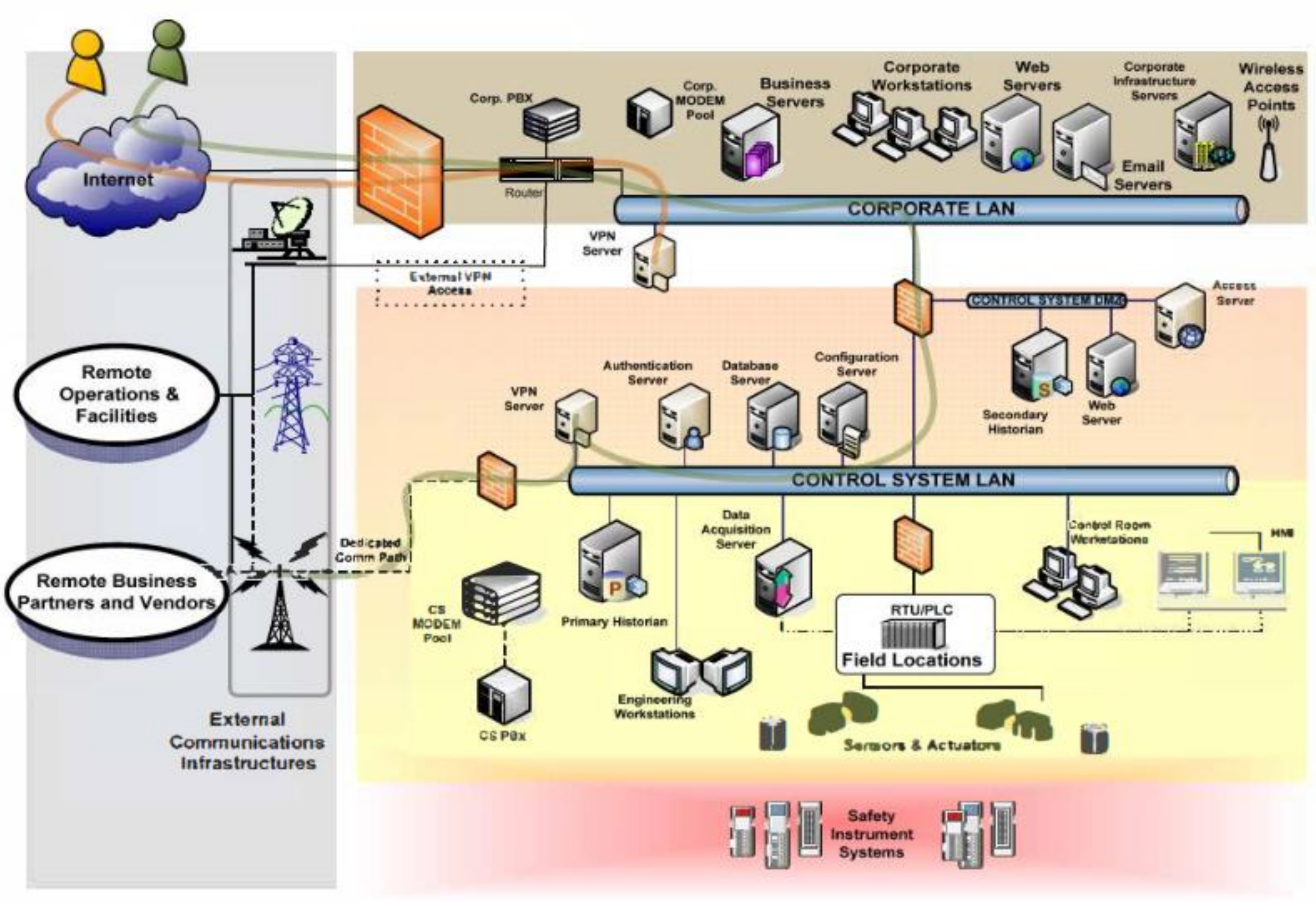
SECURE REMOTE ACCESS

Good Practices for Secure Remote Access

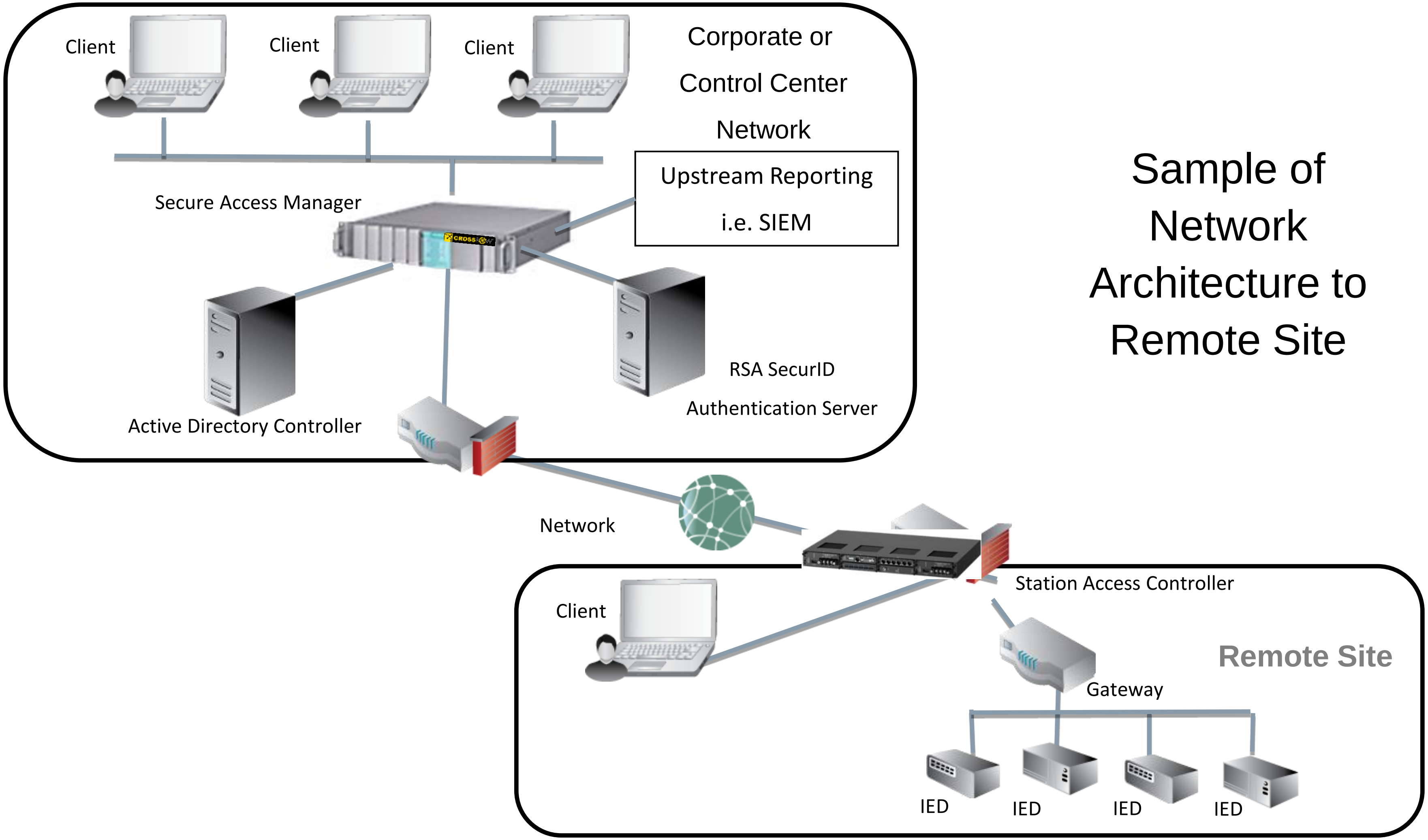
- Create a security assurance policy for all remote access
- Use only full tunneling cryptographic technology
- Use a password policy specific to remote access
- Use multifactor authentication where possible
- Use role-based authorization levels

SECURE REMOTE ACCESS

Virtual Private Networks (VPN) provide access control and authentication for remote access to business networks and process control systems



SECURE REMOTE ACCESS



Client
Client
Client
Corporate or Control Center Network
Upstream Reporting i.e. SIEM
Secure Access Manager
RSA SecurID Authentication Server
Active Directory Controller
Network
Station Access Controller
Client
Remote Site
Gateway
IED
IED
IED
IED

Sample of Network Architecture to Remote Site

CALL TO ACTION

- Understand what assets you have in your Process Control System (asset inventory)
- Determine who should have access to what assets (and who should not)
- Decide what type of access control and authentication meets your business needs and risk levels

CONTACT PAGE

Todd Wedge

Business Development Manager
RUGGEDCOM Solutions

Siemens Industry

Mobile: +1 (206) 427-8892

E-mail: todd.wedge@siemens.com

Answers for industry.