

Real-World Consequences of SCADA Cybersecurity

Andrew Green
Technical Sales



My daughter's dream car



Her biggest threat



Lululemon

But seriously...a quick object lesson



What I came up with

- Park it someplace dangerous
- Leave it unlocked
- Easily accessible key

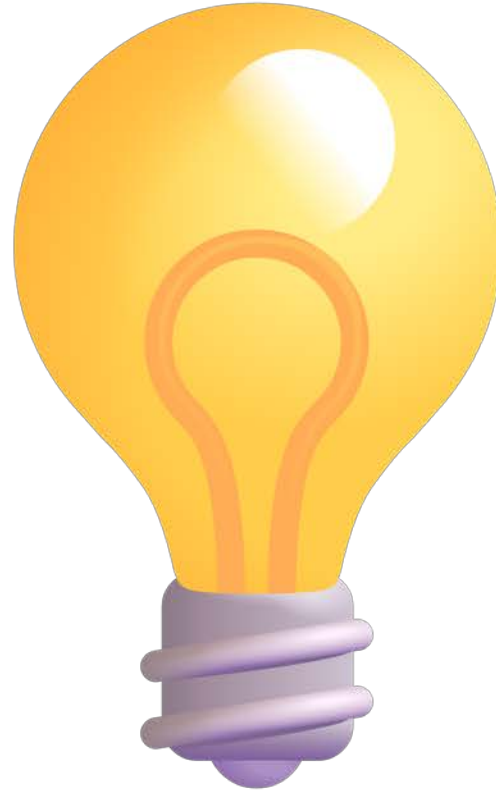
What I came up with

- Park it someplace dangerous
- Leave it unlocked
- Easily accessible key

What I came up with

- Park it someplace dangerous
- Leave it unlocked
- Easily accessible key

A good idea (invert)



The opposite

- Park it someplace safe
- Lock it up
- Limit key access

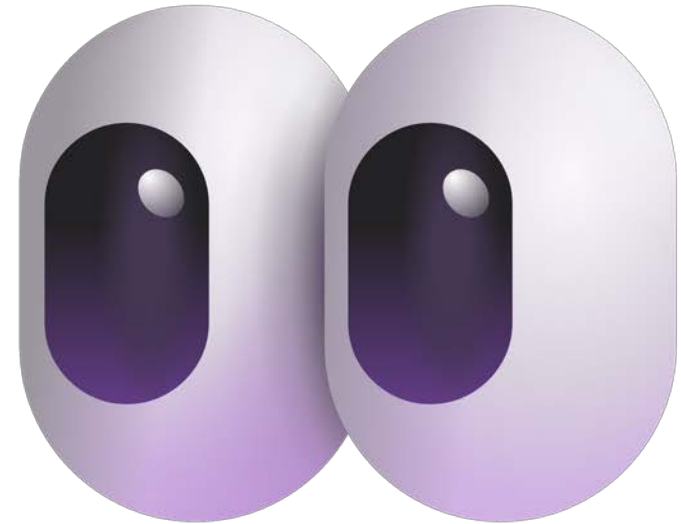
The opposite

- Park it someplace safe
- Lock it up
- Limit key access

The opposite

- Park it someplace safe
- Lock it up
- Limit key access

Sanity check



Quick PSA

“Stranger danger”

Free Resource: VTScada Security Guidelines

<https://www.vtscada.com/downloads/vtscada-latest-general/docs/vtscada-security-guidelines-manual/Guidelines>



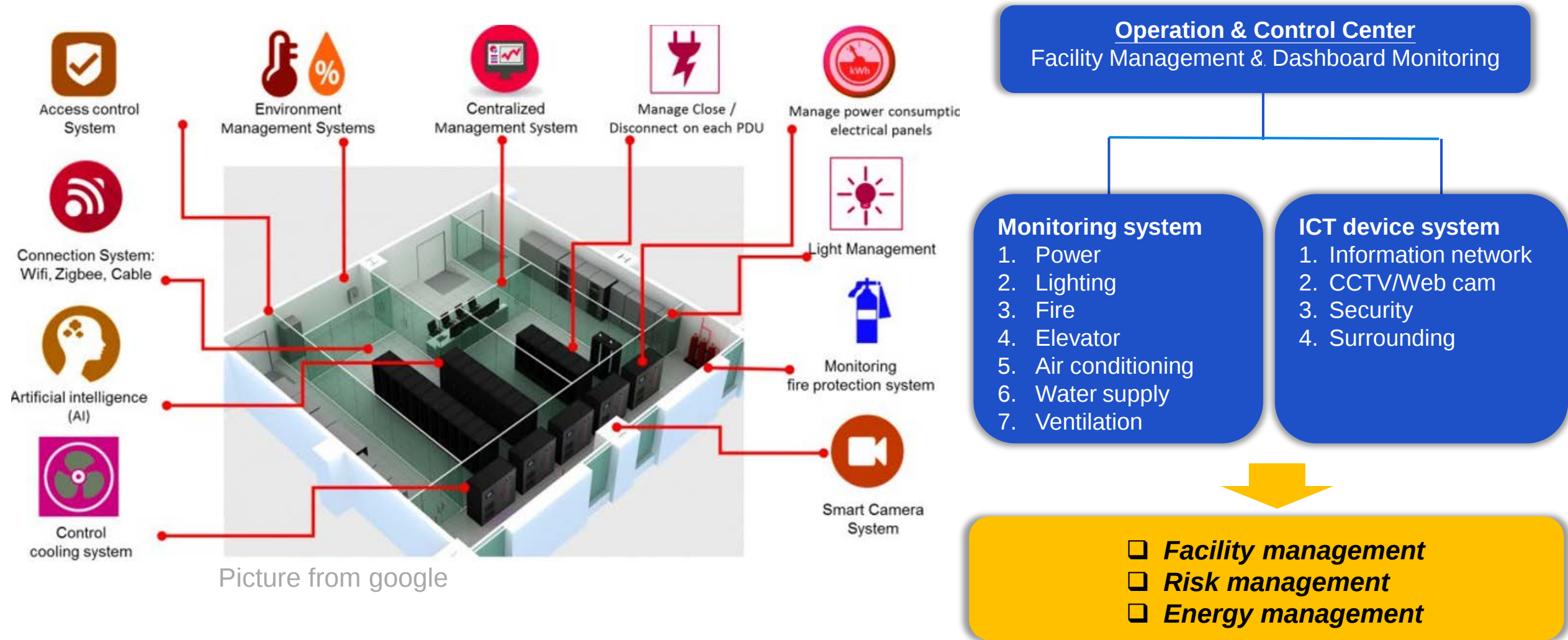
Park it someplace safe

Architecture solutions

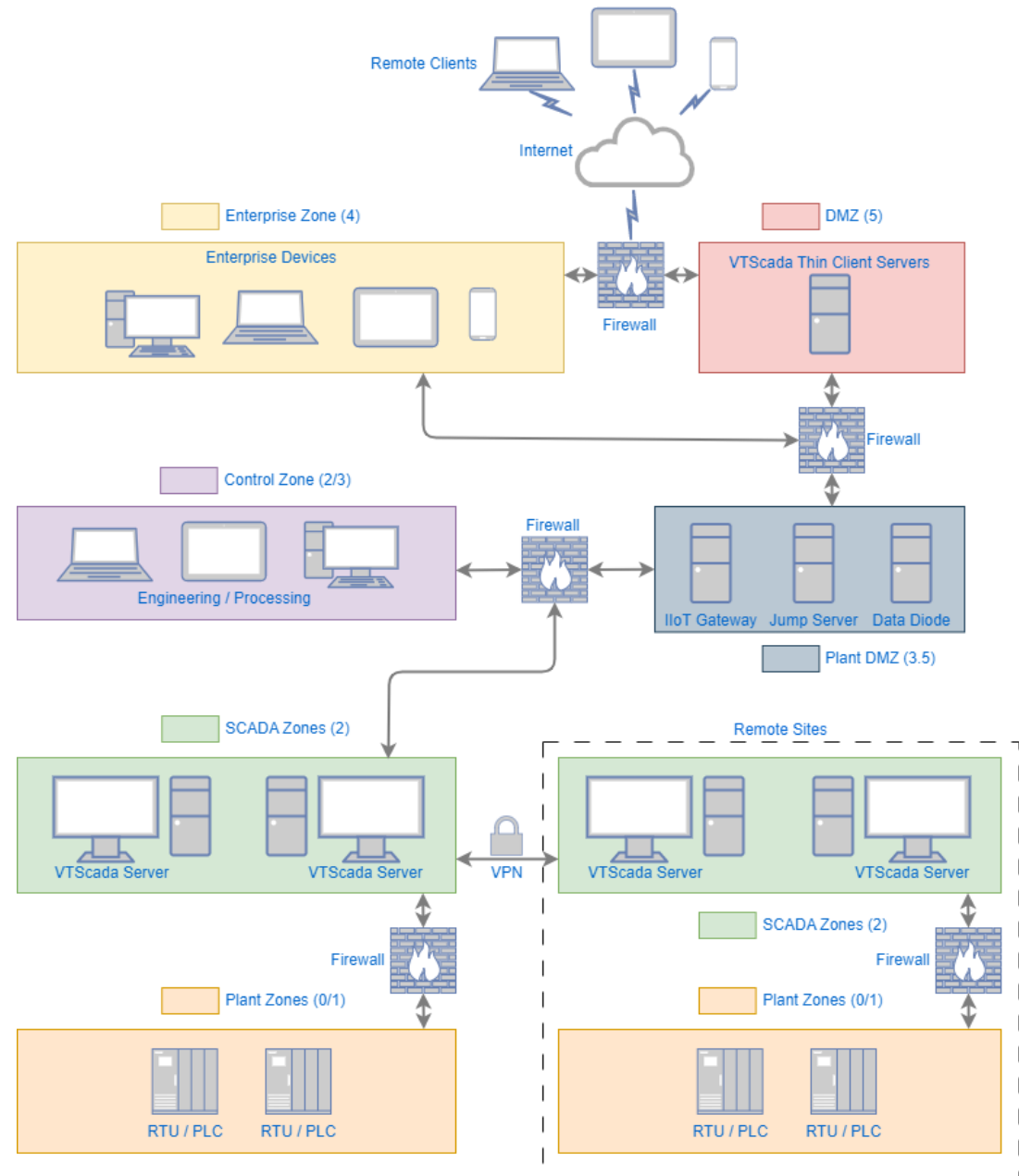
Which one doesn't belong?



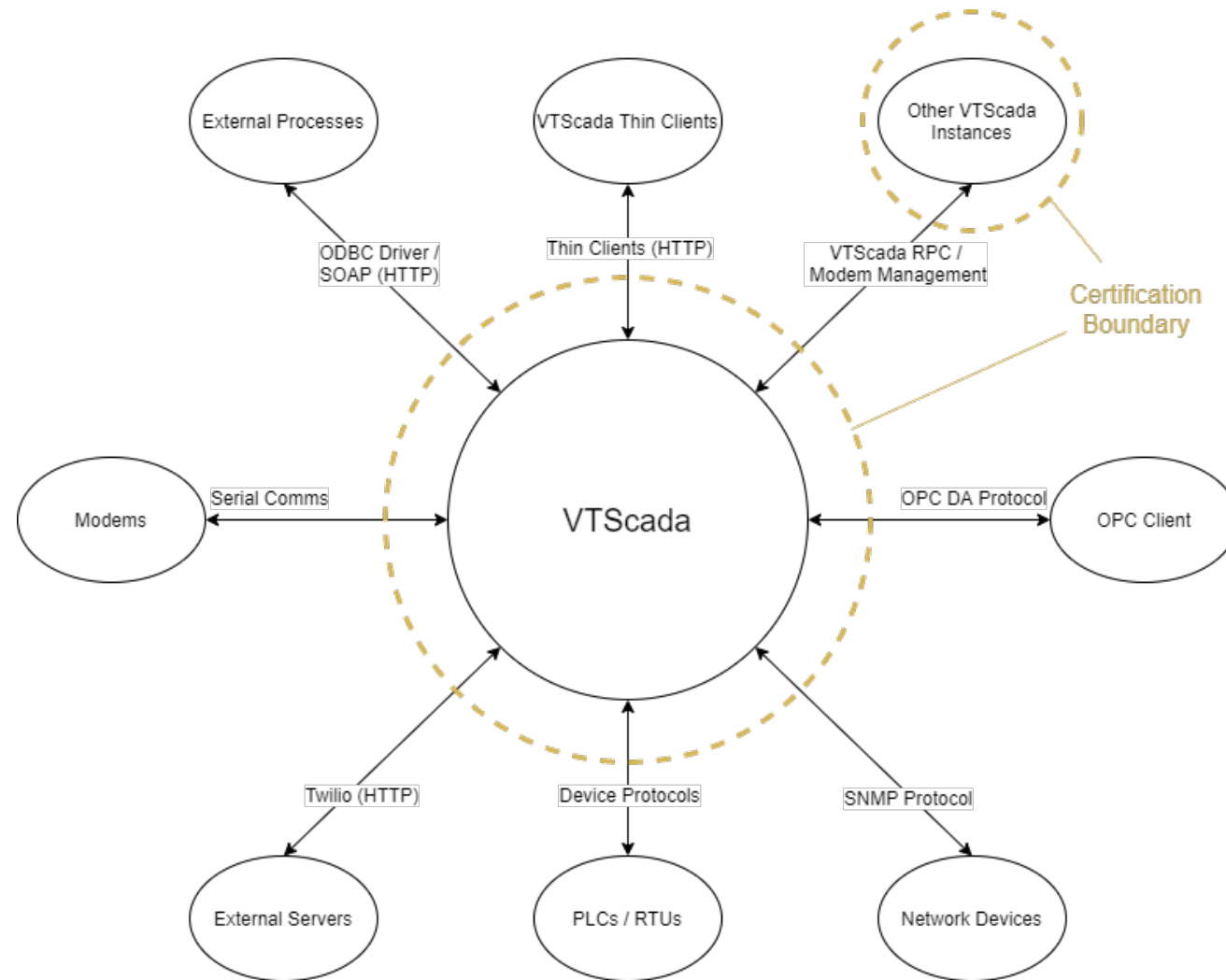
Goal: Monitor a lot of stuff



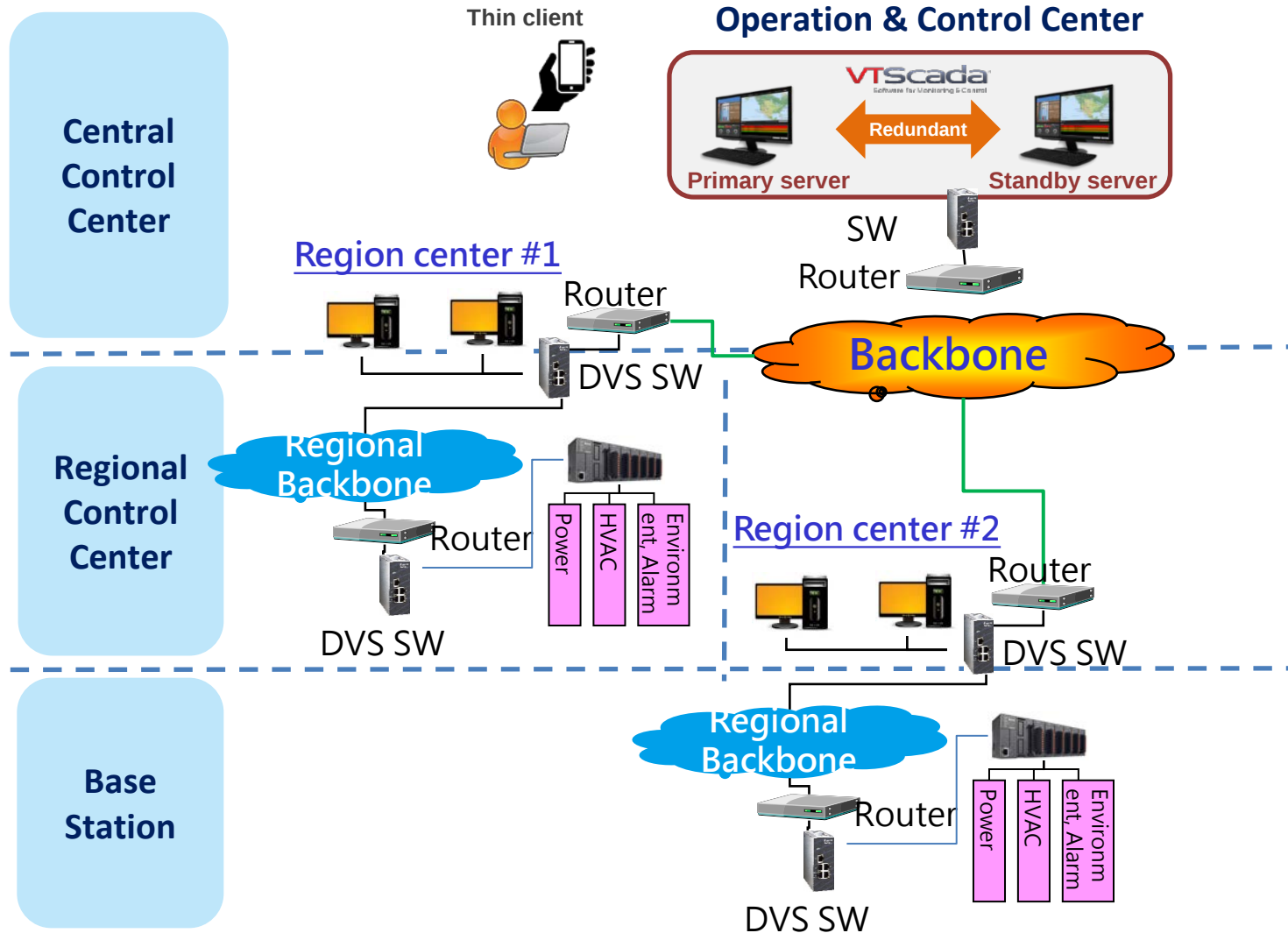
Example of IEC 62443 (-4-1)



Security scope



Sample real-world architecture



Data center Management Platform

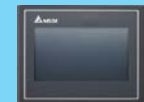
- Hardware x Software
- Real-time Control
- All in One total solution

Operation & Control Center



Redundant & Remote solution

Regional Control Center



Sub system Monitoring & Analytics solution

Free Resource: VTScada Security Guidelines

<https://www.vtscada.com/downloads/vtscada-latest-general/docs/vtscada-security-guidelines-manual/Guidelines>



Lock it up

Remote solutions

Remote benefits



Follow ISA 18.2 Alarms Management Standard. Detail alarm information provided:

Separate encrypted databases for all Alarms and Events.

Use color, symbols, and sound to meet the visual needs of your operators.

Shelved Alarms won't distract operators but are recorded in the events database..

	Time		Event	Area	Name
🔴	2016-12-22 11:19:07	✓	Acknowledge	Water Treatment Plant	WaterTreatmentPlantDemo\TCPIP Port\WaterTreatPlantSim\TestAl
🔴	2016-12-22 11:18:29	🔔	Normal	Water Treatment Plant	WaterTreatmentPlantDemo\TCPIP Port\WaterTreatPlantSim\TestAl
🔴	2016-12-22 11:18:24	🔴	Active	Water Treatment Plant	WaterTreatmentPlantDemo\TCPIP Port\WaterTreatPlantSim\
🟡	2016-12-22 10:22:49	🔴	Shelve	Water Treatment Plant	WaterTreatmentPlantDemo\WaterTreatPlantSim\Pumps\Pump0\
🟡	2016-12-22 10:22:43	🔴	Shelve	Water Treatment Plant	WaterTreatmentPlantDemo\WaterTreatPlantSim\Tanks\Tank3\Tar
🟡	2016-12-22 10:14:21	🔴	Unshelve	Water Treatment Plant	WaterTreatmentPlantDemo\WaterTreatPlantSim\Tanks\Tank1\Tar
🟡	2016-12-22 10:14:19	🔴	Unshelve	Water Treatment Plant	WaterTreatmentPlantDemo\TCPIP Port\WaterTreatPlantSim\Tanks\
🟡	2016-12-22 10:14:08	🔴	Shelve	Water Treatment Plant	WaterTreatmentPlantDemo\TCPIP Port\WaterTreatPlantSim\Tanks\
🟡	2016-12-22 10:14:00	🔴	Shelve	Water Treatment Plant	WaterTreatmentPlantDemo\WaterTreatPlantSim\Tanks\Tank1\Tar
	2016-12-22 10:04:16	🔴	Unshelve	IT	ITResources\Workstation_Barry\PercentCPUUsed
		🔴	Shelve	IT	ITResources\Workstation_Barry\PercentCPUUsed
🔴	2016-12-14 16:26:41	✓	Acknowledge	Water Treatment Plant	WaterTreatmentPlantDemo\TCPIP Port\WaterTreatPlantSim\TestAl
🔴	2016-12-14 16:26:37	🔔	Normal	Water Treatment Plant	WaterTreatmentPlantDemo\TCPIP Port\WaterTreatPlantSim\TestAl
🔴	2016-12-14 16:26:32	🔴	Active	Water Treatment Plant	WaterTreatmentPlantDemo\TCPIP Port\WaterTreatPlantSim\TestAl
🔴	2016-12-14 15:54:13	🔴	Unshelve	IT	ITResources\Workstation_Dave\BatteryLevel
🔴	2016-12-14 15:53:49	🔴	Shelve	IT	ITResources\Workstation_Dave\BatteryLevel
🔴	2016-12-06 12:00:06	✓	Acknowledge	Water Treatment Plant	WaterTreatmentPlantDemo\TCPIP Port\WaterTreatPlantSim\TestAl
🔴	2016-12-06 12:00:00	🔔	Normal	Water Treatment Plant	WaterTreatmentPlantDemo\TCPIP Port\WaterTreatPlantSim\TestAl
🔴	2016-12-06 11:59:55	🔴	Active	Water Treatment Plant	WaterTreatmentPlantDemo\TCPIP Port\WaterTreatPlantSim\TestAl

Easily filter down to only the Alarms you need.

Find Alarms and Events

with this description:

☐ Case sensitive

with this name:

☒ Include children

in this area:

with this priority:

☐ Or higher priority

by this user:

as this event:

in this month:

in this date range: to

OK Cancel Apply

Shelve the selected alarm

☒ for 5 minutes

☐ until 2016-05-04 12:00

☐ indefinitely

OK Cancel

Configuration options

- **Disallowed - SCADA network "Air Gapping"**

- ✓ No outside or remote access
- ✓ Limited Alarm Notification options
- ✓ Data diode

- **Manual connected – temporary access**

- ✓ Typically, remote support use only

- **Allowed – permanent on-demand access**

- ✓ Access to IT, OT, and Business System users
- ✓ Remote support access only temporarily allowed
- ✓ Full Alarm Notification options
- ✓ Requires security
- ✓ DMZs, Firewalls, VPNs, etc.

**SCADA
Network**

**Non-SCADA
Network**



Secure remote access

- **HTML 5 provides a secure remote connection**
- **Ensure the server is HTTPS**
- **Connect via VPN and X509 SSL certificate**
- **Things to consider**
 - Read only access server
 - Separate networks
 - 3rd Party security standards
 - Frequency of updates
 - System as a service



Secure remote access

- HTML 5 provides a secure remote connection
- **Ensure the server is HTTPS**
- Connect via VPN and X509 SSL certificate
- Things to consider
 - Read only access server
 - Separate networks
 - 3rd Party security standards
 - Frequency of updates
 - System as a service



Secure remote access

- HTML 5 provides a secure remote connection
- Ensure the server is HTTPS
- **Connect via VPN and X509 SSL certificate**
- Things to consider
 - Read only access server
 - Separate networks
 - 3rd Party security standards
 - Frequency of updates
 - System as a service



Secure remote access

- HTML 5 provides a secure remote connection
- Ensure the server is HTTPS
- Connect via VPN and X509 SSL certificate
- **Things to consider**
 - Read only access server
 - Separate networks
 - 3rd Party security standards
 - Frequency of updates
 - System as a service



Secure remote access

- HTML 5 provides a secure remote connection
- Ensure the server is HTTPS
- Connect via VPN and X509 SSL certificate
- Things to consider
 - Read only access server
 - Separate networks
 - 3rd Party security standards
 - Frequency of updates
 - System as a service



Secure remote access

- HTML 5 provides a secure remote connection
- Ensure the server is HTTPS
- Connect via VPN and X509 SSL certificate
- Things to consider
 - Read only access server
 - Separate networks
 - 3rd Party security standards
 - Frequency of updates
 - System as a service



Secure remote access

- HTML 5 provides a secure remote connection
- Ensure the server is HTTPS
- Connect via VPN and X509 SSL certificate
- Things to consider
 - Read only access server
 - Separate networks
 - 3rd Party security standards
 - Frequency of updates
 - System as a service



Secure remote access

- HTML 5 provides a secure remote connection
- Ensure the server is HTTPS
- Connect via VPN and X509 SSL certificate
- Things to consider
 - Read only access server
 - Separate networks
 - 3rd Party security standards
 - Frequency of updates
 - System as a service



Secure remote access

- HTML 5 provides a secure remote connection
- Ensure the server is HTTPS
- Connect via VPN and X509 SSL certificate
- Things to consider
 - Read only access server
 - Separate networks
 - 3rd Party security standards
 - Frequency of updates
 - System as a service



Limit key access

Application solutions

Application-level security

1. Privileges

- Tasks such as..
 - Acknowledge alarms
 - Close an application
 - Write a value, control a device

2. Roles

- Set of privileges

3. Accounts

- User
- Assigned roles and privileges

4. Windows Security Integration

5. Two Factor Authentication

The screenshot shows the 'VT Accounts' configuration window. It has three main sections: 'Users', 'Roles', and 'Privileges'. The 'Users' section on the left lists 'Don Draper', 'Peggy Olson', and 'Pete Campbell'. The 'Roles' section on the left lists 'Admin', 'Configurer', 'Logged Off', 'Operator', and 'SuperUser'. The 'Privileges' section on the right is expanded, showing a list of roles with their descriptions. Red boxes with numbers 1, 2, and 3 highlight specific elements: box 1 is on the 'Privileges' section header, box 2 is on the 'Roles' list, and box 3 is on the 'Username' field in the 'General' tab.

VT Accounts

Users

- Don Draper
- Peggy Olson
- Pete Campbell

General

Username: Don Draper

Password

Password: Confirm Password:

Force reset of password at next sign in: ☐

Advanced

Disable Account: ☐

Use Default Sign Out Time Period: ☒

No Automatic Sign Out: ☐

Minutes of Inactivity (0 - 720): 15

Alternate Identification: Unavailable

Privileges

Roles

Role	Description
☐ Admin	Limited role
☐ Configurer	Permits configuration of a VTScada Application
☐ Operator	Permits operation of a VTScada Application
☒ SuperUser	Permits complete control of all aspects of VTScada

Additional Privileges

☒ Manager	...
☒ Administrator	...
☒ Application Stop	...
☒ Configure	...

Buttons: Add, Manage, Apply, Close

Free Resource: VTScada Security Guidelines

<https://www.vtscada.com/downloads/vtscada-latest-general/docs/vtscada-security-guidelines-manual/Guidelines>



Questions?