How OPC UA addresses attack scenarios

Information Revolution 2014 August 5th – 6th

Microsoft Conference Center Redmond, Washington

Nathan Pocock
Technical Director
OPC Foundation

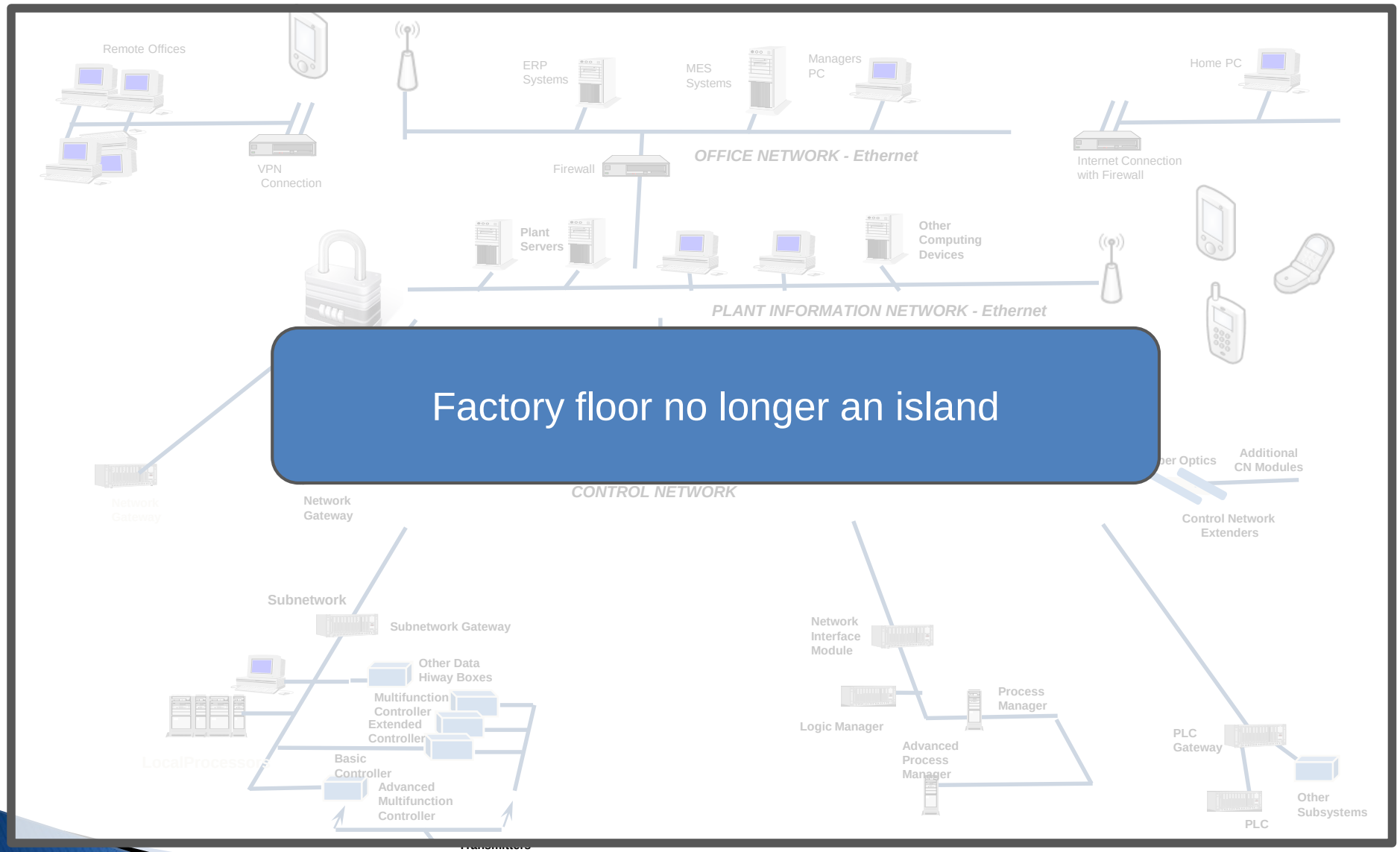
Darek Kominek
Strategic Marketing Manager
MatrikonOPC

Paul Hunkar
Technical Director
DS Interoperability LLC

Agenda

- Security: yesterday vs. today
- Security recap
- Attack modes for ICS
- UA handling of Attack modes
- Case studies

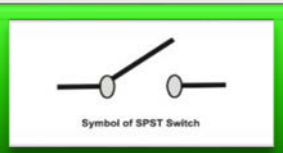
Security Yesterday and Today



Implication #1: ICS Faces IT Attacks

Loss of View (LoV)

Manipulation of View (MoV)

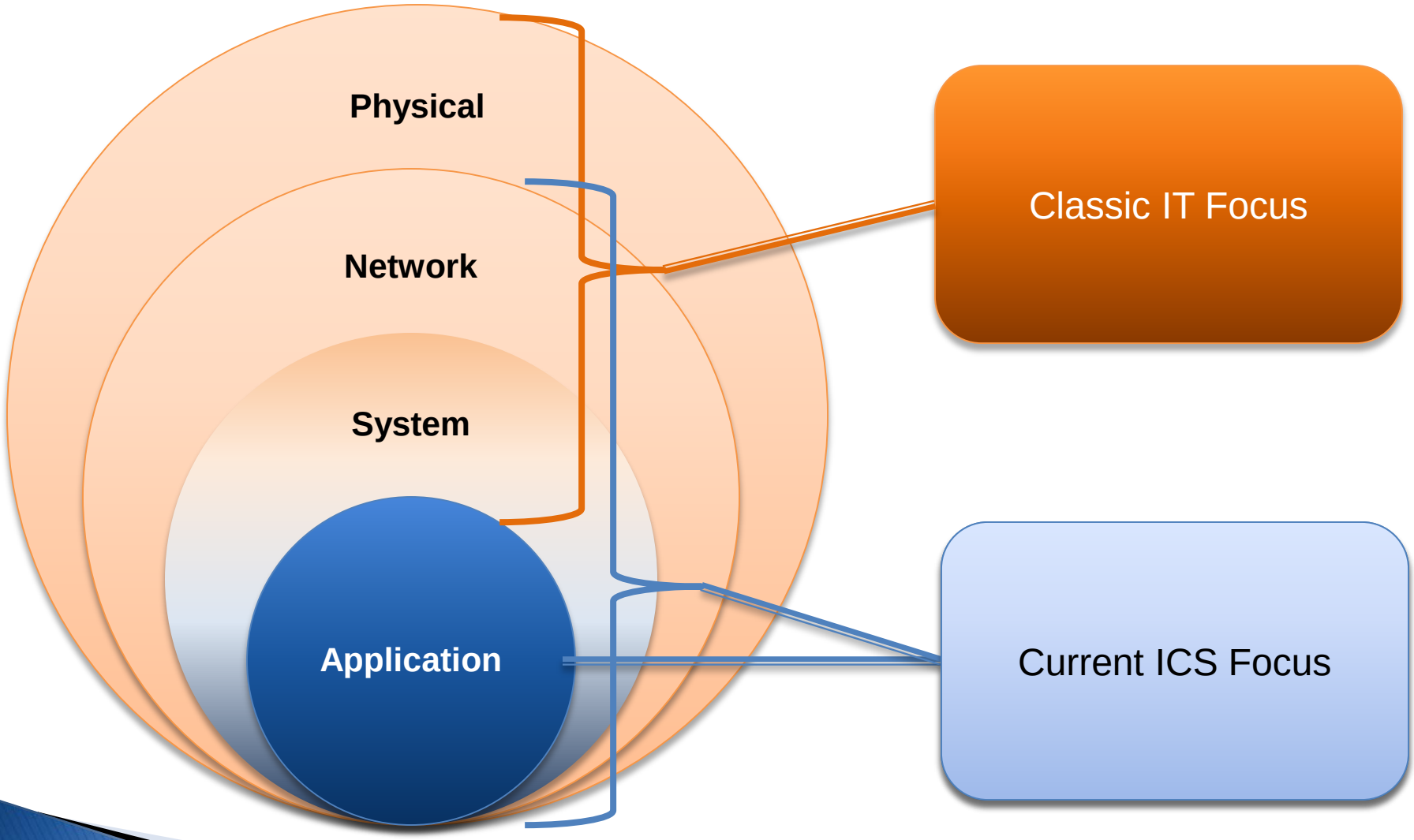


Denial of Control (DoC)

Manipulation of Control (MoC)

Loss of Control (LoC)

Cyber Security – Multiple Aspects

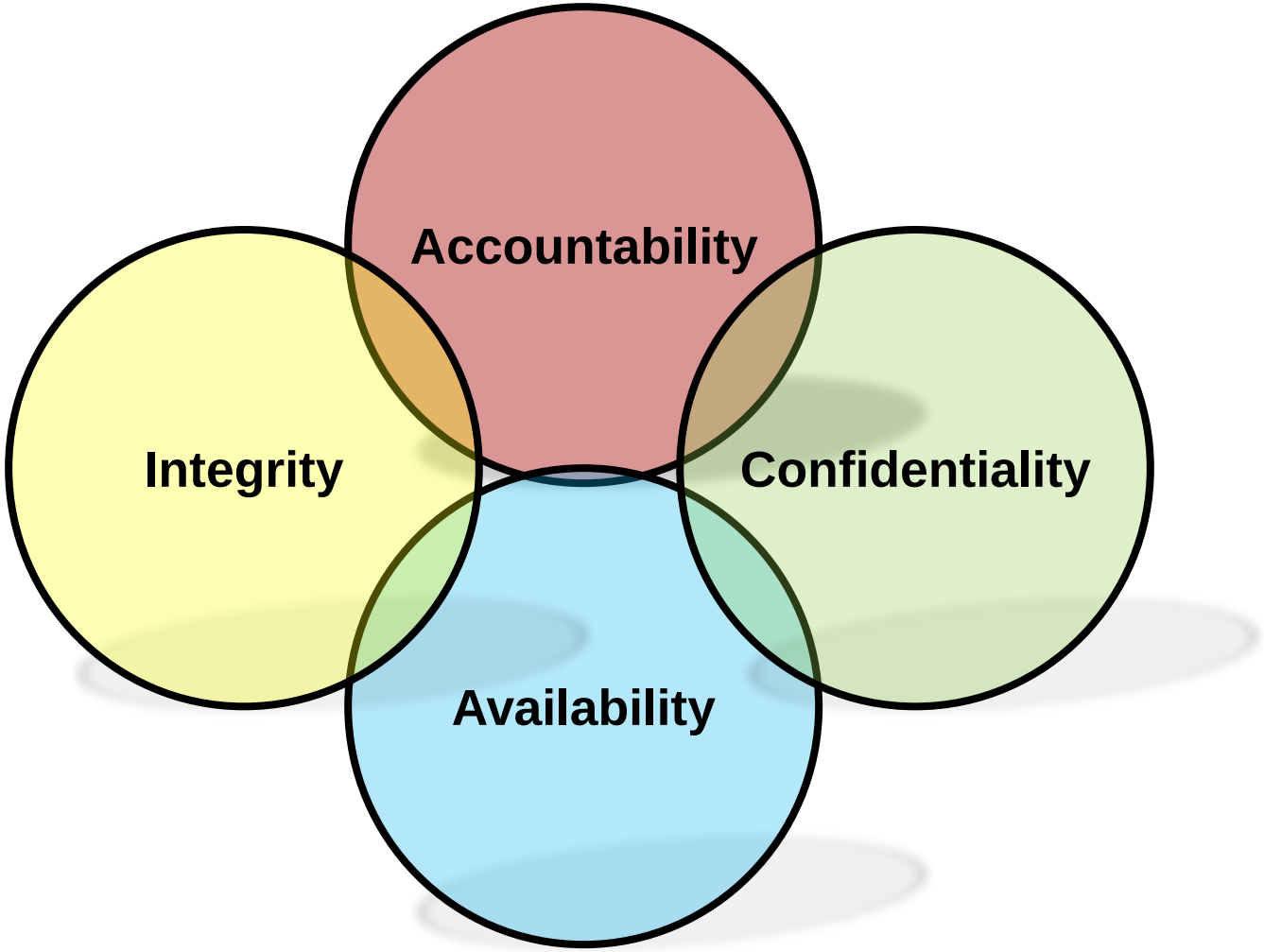


Implications: ICS meets IT

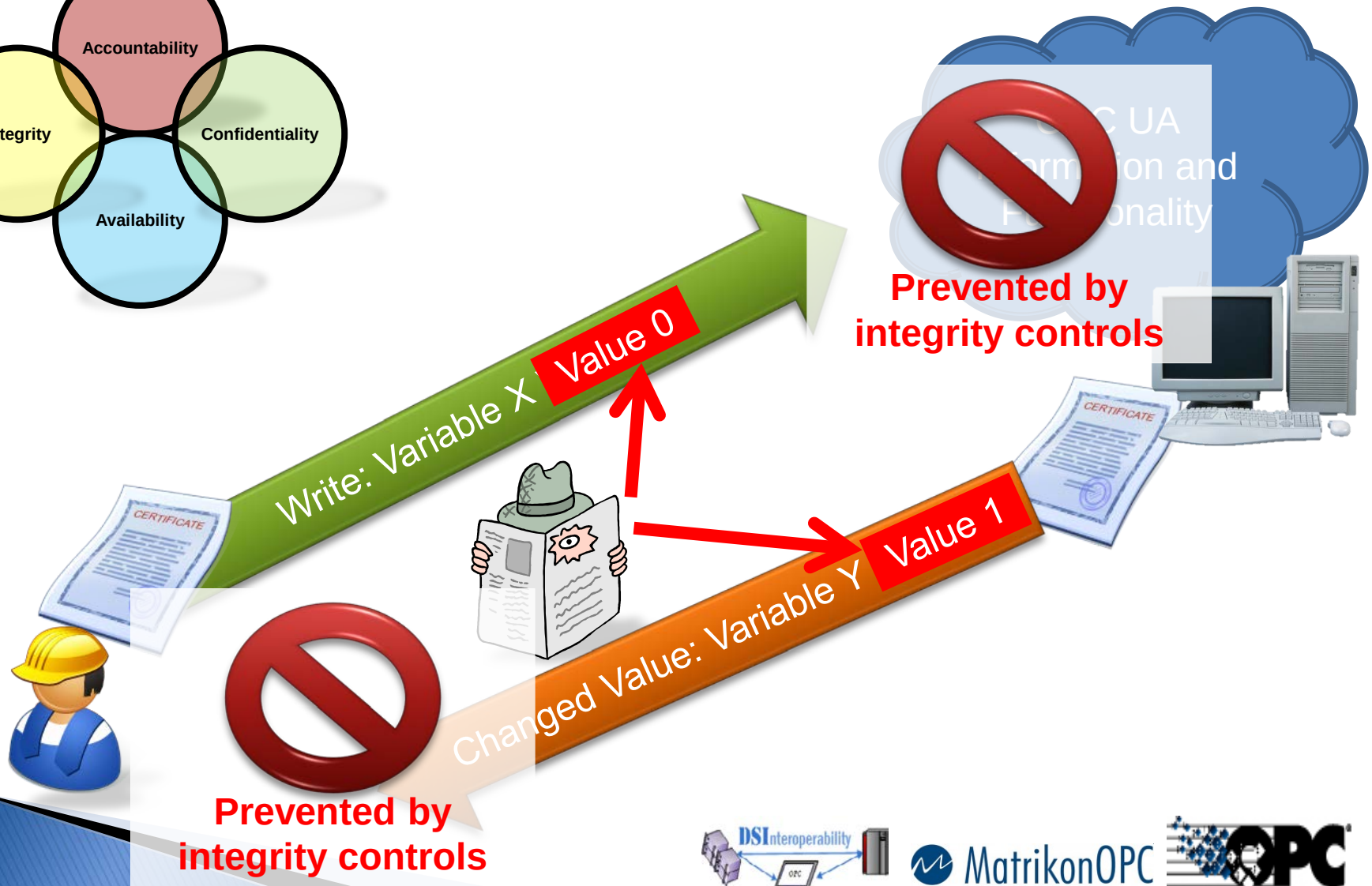
Priority

Traditional IT	Higher-Level ICS	Lower-Level ICS
Confidentiality	Integrity	Availability
Integrity	Availability	Integrity
Availability	Confidentiality	Confidentiality
	Safety	

UA Focus on Security Fundamentals

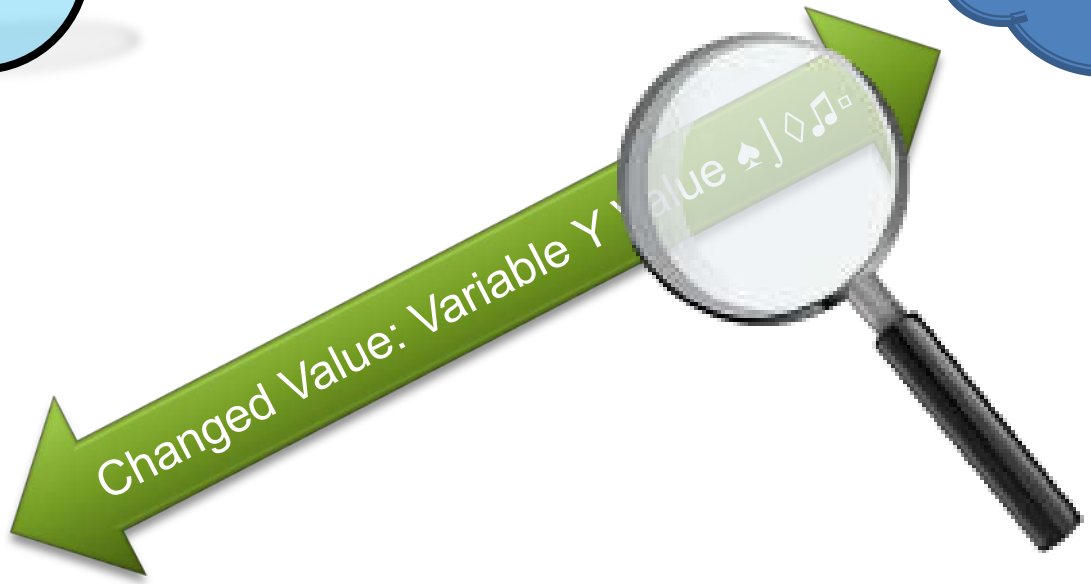


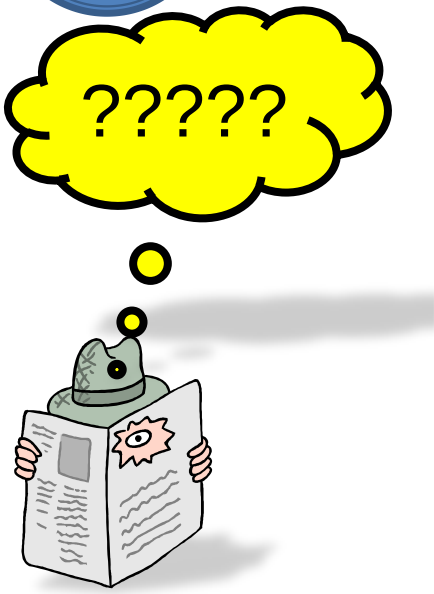
Fundamental: Message Signing



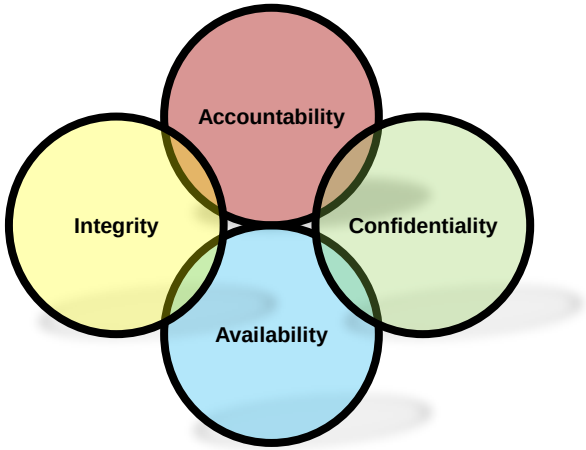
Fundamentals: Encryption

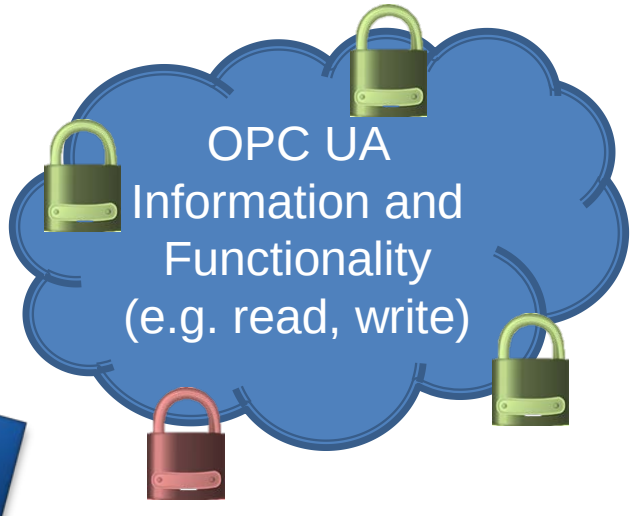
OPC UA
Information and
Functionality





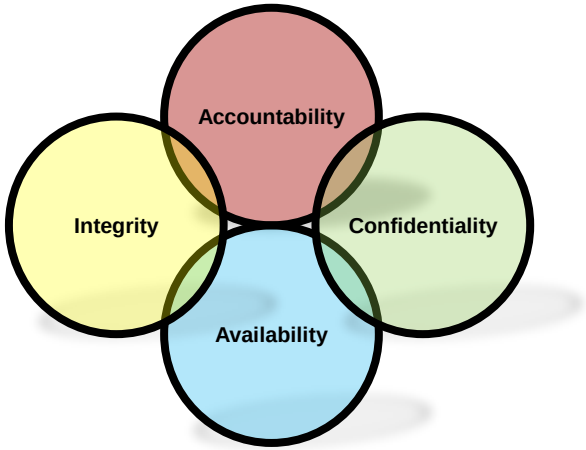
Fundamentals: Authentication - Apps

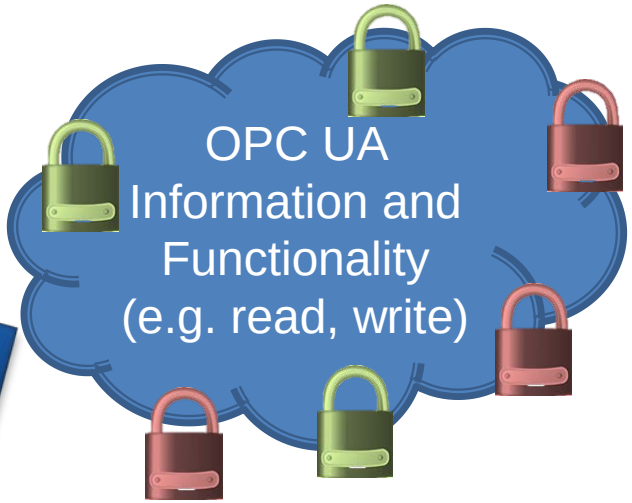


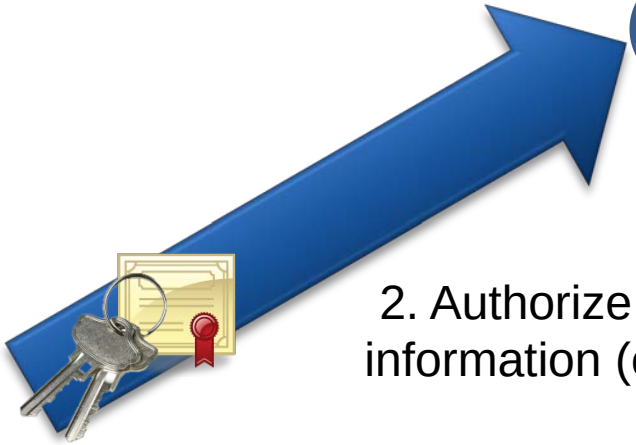


Application Instance
Certificates

Fundamentals: User Authentication







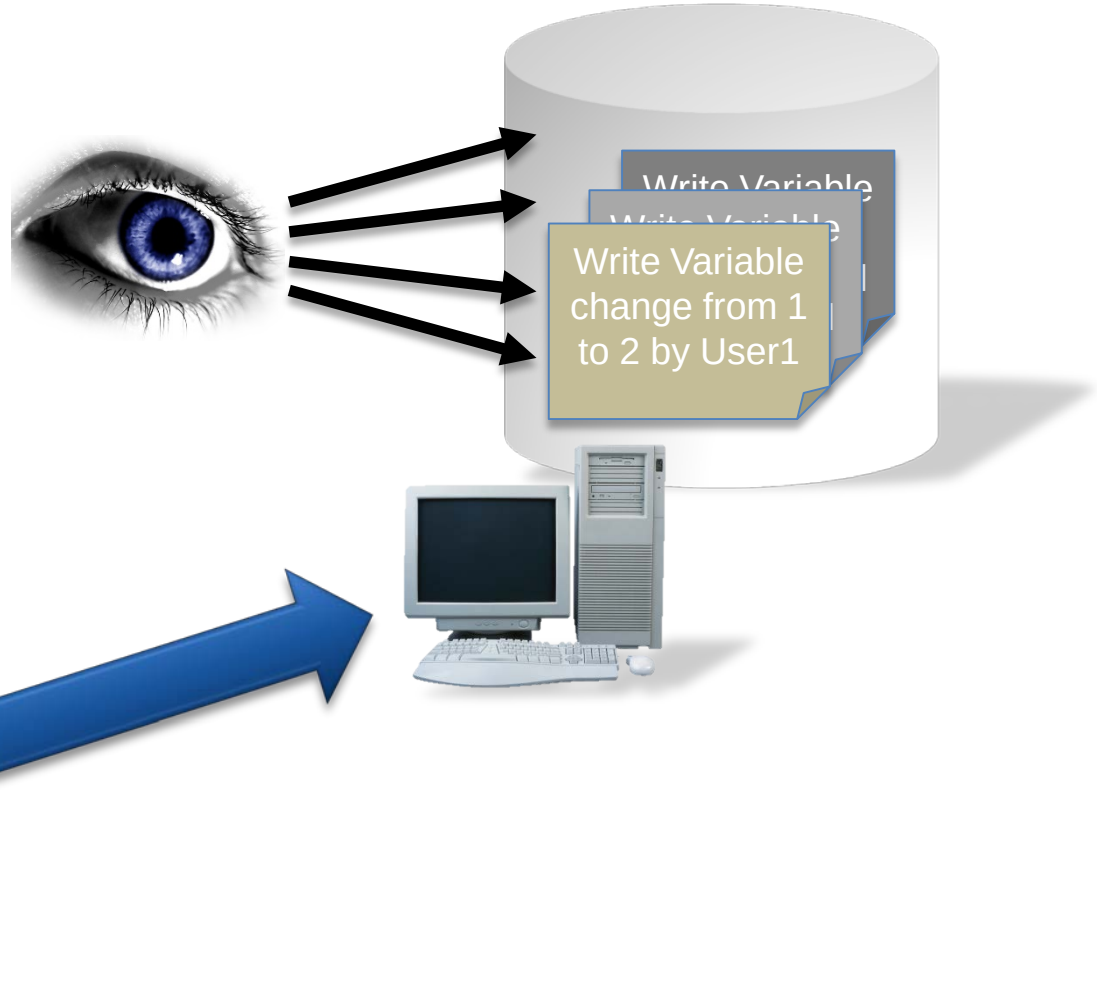
2. Authorize for specific operations and information (e.g. writing a specific value)

1. Authenticate User
(e.g. username and password…..)

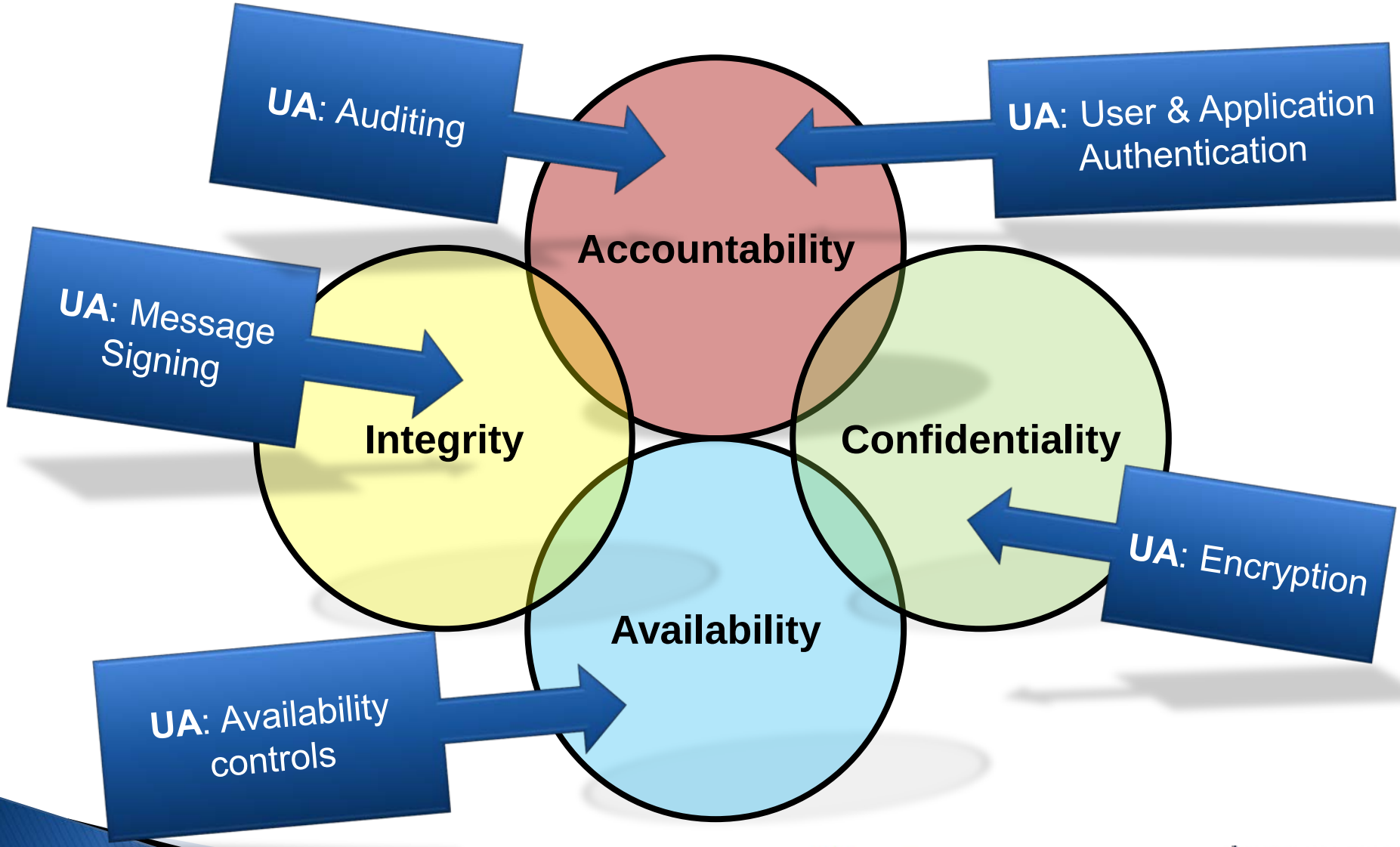
Fundamentals: Availablity

Prevented by Availability Controls

Fundamentals: Auditing

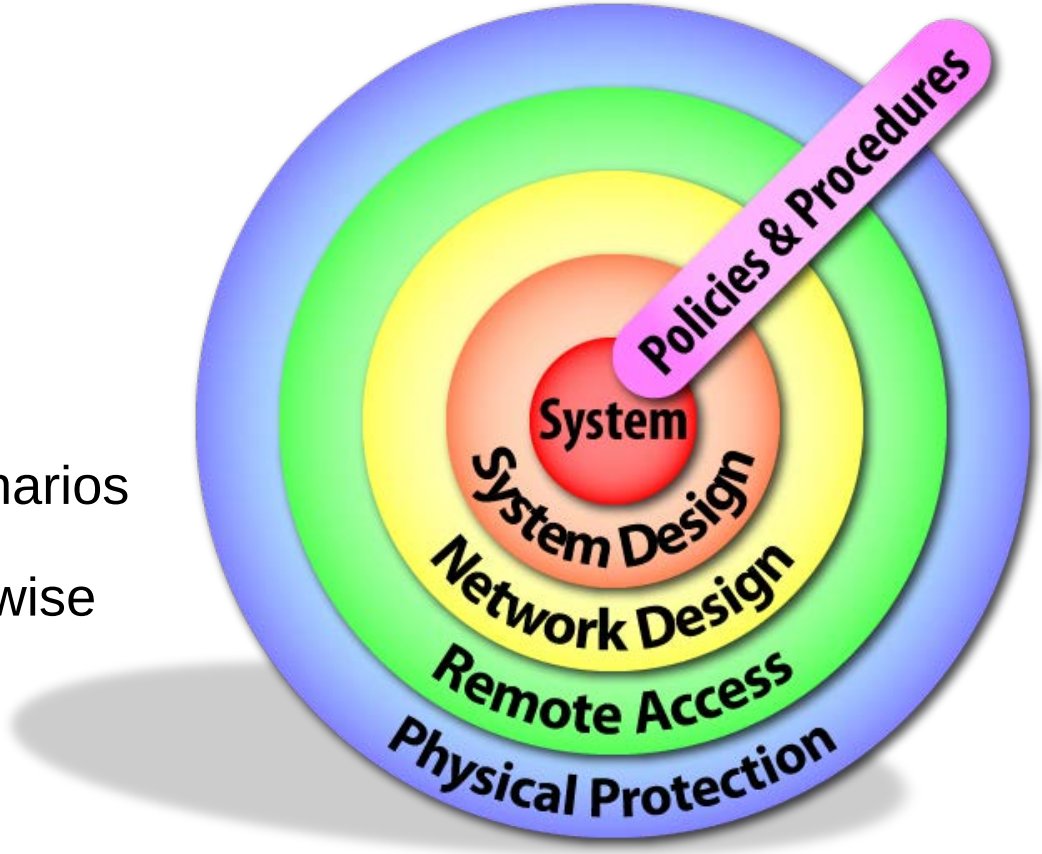


Fundamentals of Security



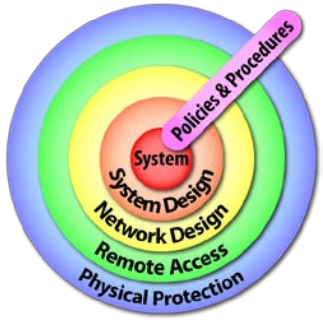
But, where do YOU begin?

- Analyze your system
- Identify each component and analyze it
- Search for all possible vulnerabilities in all attack scenarios
- Mitigate where possible; otherwise consider the alternatives…
- Document everything



OPC UA Security: Assessments

Security Assessment for UA environments: Objectives & Threats



DoS

Eavesdropping

Message Alteration

Malformed Messages

Message Flooding

Message Spoofing

Rogue Server

Rogue Client

Session Hijacking

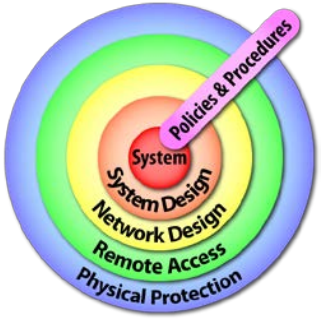
Server Profiling

DDoS

Availability	Non-Repudiation	Accountability/Traceability

Authorization	Authentication	Confidentiality	Integrity

OPC UA Security: Assessments



- Security Assessment for UA environments: Mitigations
  - Goals ⇔ Threats ⇔ Mitigations
  - Various threats and mitigations are described in Part 2

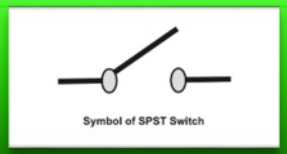
Example:

Goal	Threats	Mitigations
Availability	Denial-of-Service (DoS) ► **Bandwidth approach** ► **Resource approach** ► **System crash approach**	► **Minimize processing data** ► **User authentication** ► **Application authentication** ► **Message authentication** ► **Response delays** ► **Auditing** ► **Intrusion Detection System** ► **Intrusion Prevention System**

Attack Modes for ICS

Loss of View (LoV)

Manipulation of View (MoV)

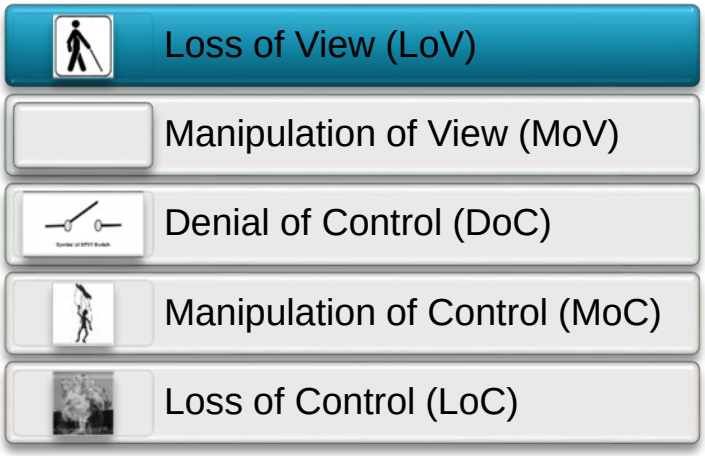


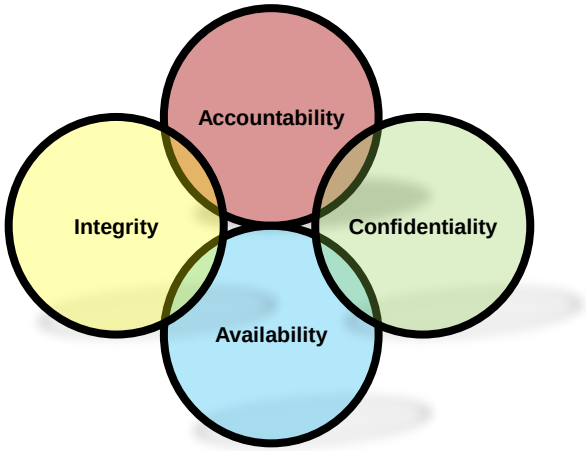
Denial of Control (DoC)

Manipulation of Control (MoC)

Loss of Control (LoC)

Attack Modes for ICS vs UA

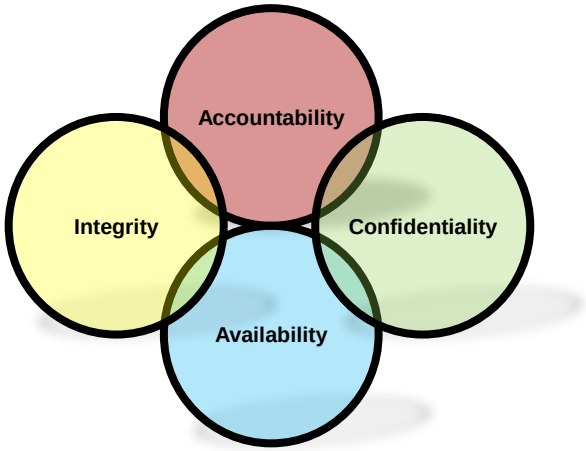




- Loss of View
  - Crashing Server
  - Blocking Access to Server
- OPC UA
  - Security Assessment
    - Of stacks
    - Of specs
    - Of implementations
    - Of toolkits / SDKs
  - Robust Communications

Attack Modes for ICS vs UA

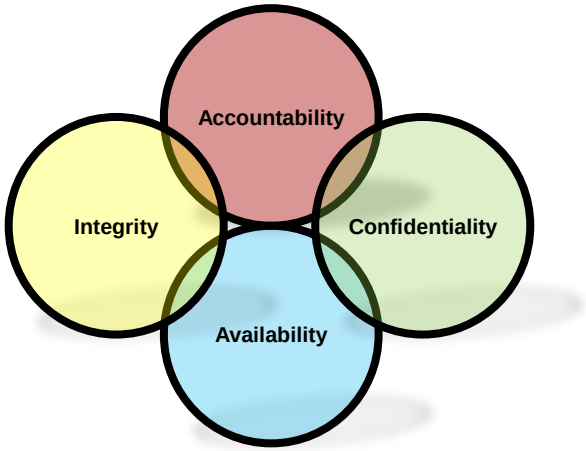
- Loss of View (LoV)
- Manipulation of View (MoV)
- Denial of Control (DoC)
- Manipulation of Control (MoC)
- Loss of Control (LoC)



- Manipulation of view
  - Blocking Messages
  - Reading Data
  - Changing Values
  - Man in the middle
- OPC UA
  - Dedicated secured connection between trusted applications
  - Encrypted data
  - Signed data

Attack Modes for ICS vs UA

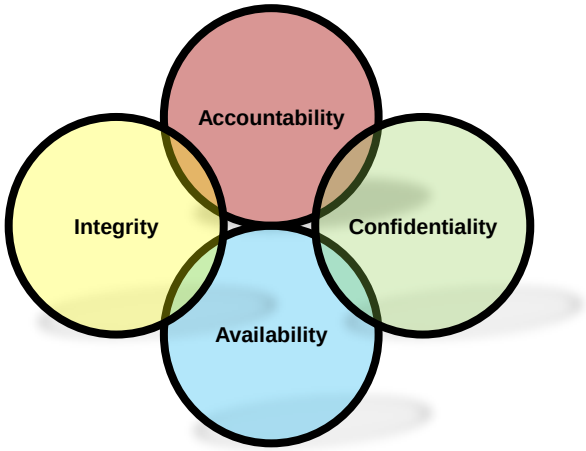
- Loss of View (LoV)
- Manipulation of View (MoV)
- Denial of Control (DoC)
- Manipulation of Control (MoC)
- Loss of Control (LoC)



- Denial of Control
  - Crashing Server
  - Blocking Access to Server
  - Man in the middle
- OPC UA
  - Availability controls

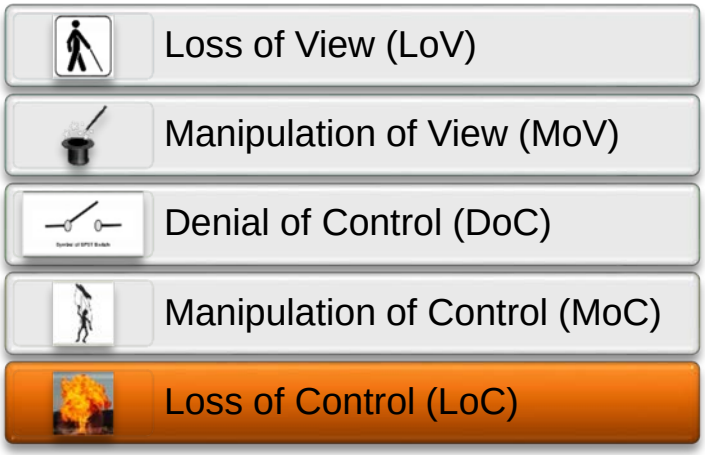
Attack Modes for ICS vs UA

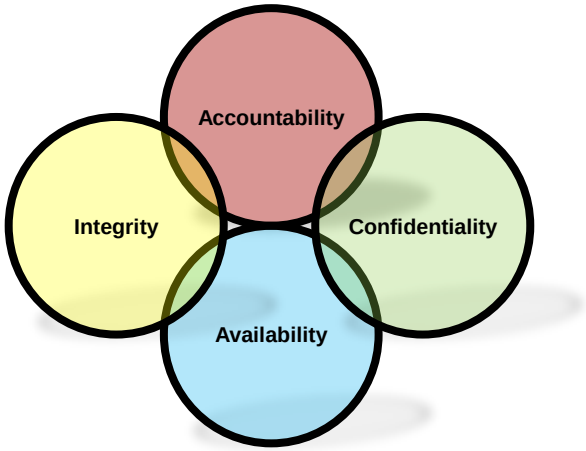
- Loss of View (LoV)
- Manipulation of View (MoV)
- Denial of Control (DoC)
- **Manipulation of Control (MoC)**
- Loss of Control (LoC)



- Manipulation of control
  - Modifying data
  - Filtering data
- OPC UA
  - Only Trusted application
  - Connection Status information
  - Restricted User access

Attack Modes for ICS vs UA





- Loss of Control
  - Client disconnected
  - Foreign client driving
- OPC UA
  - Only Trusted application
  - Connection Status information
  - Restricted User access
  - Signing and Encryption

Havex

What it does:

- Collects: List of Servers, their functionality, and items in address space
- Uses OPC Classic as intended as a client
- Can be remotely controlled
- Additional payloads are possible

Additional information:

- Requires that it is installed on a machine and running under a user account.
- Utilize standard DCOM technology.
- DCOM Security can govern what is available

Havex

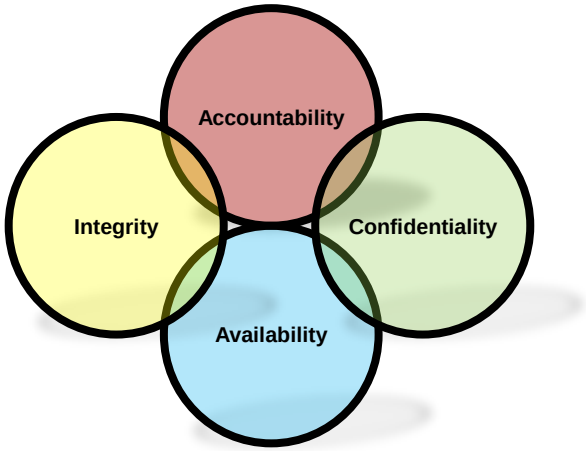
Lessons Learned:

- Uses technology in the intended manner, but to do harm
- Shows a system being used against itself
- People inadvertently/unknowingly installing rogue software
- People not necessarily following company policies
- Exploitation of widely known relaxed DCOM security often deployed to get OPC Classic “working”

Havex

What about OPC UA:

- Discovery still available, but is not required; can be secured!
- Security at the Application and User levels
- Requires higher level access – User accounts for access are different than the administrative account used for managing certificates.



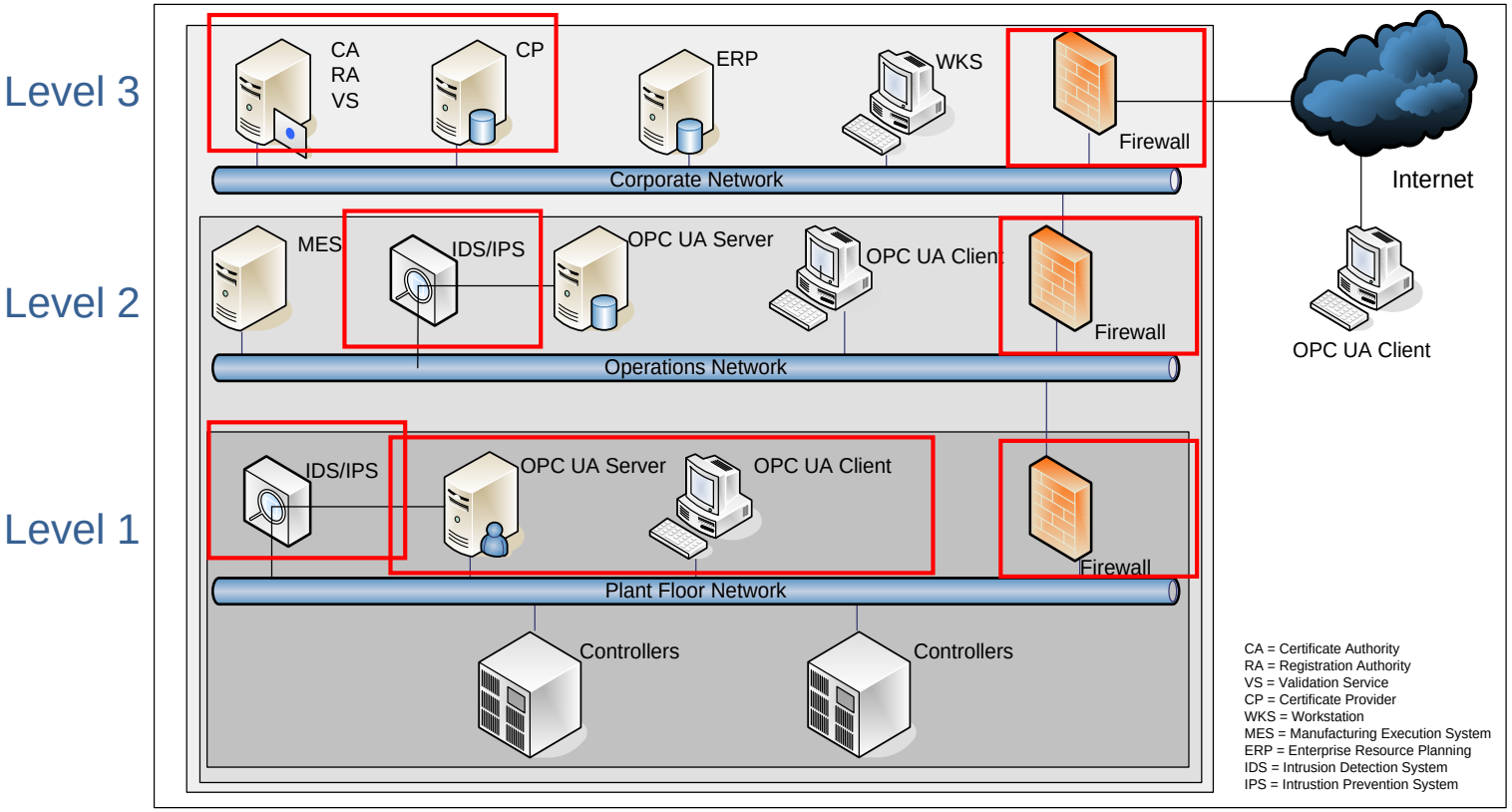
Havex: Defense In Depth

- Secure Infrastructure (Defense-In-Depth)

Public Key Infrastructure (PKI) with X.509 Certificates

Intrusion Detection & Prevention

Secure UA Applications



Hypothetical Cyber-Attack Scenarios

Turbine Overspeed – Power Generation

Ammonia Plant Explosion

Boiler Explosion

Cyber-Attack Scenarios vs UA

Ammonia Plant Explosion

- Manipulate heating during process, disable alarms and safety system, increase CO in methanator
- Disgruntled employee

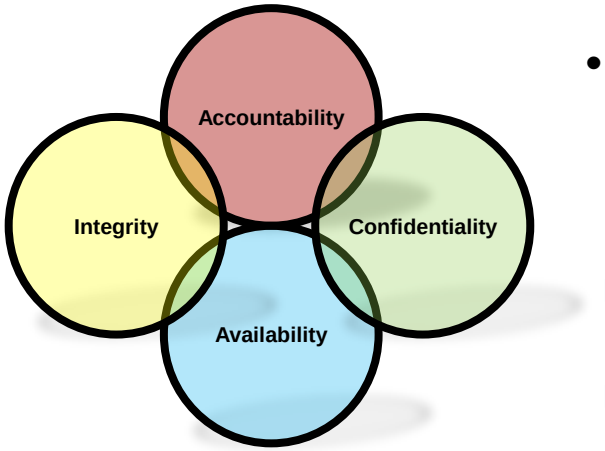
OPC UA

- PKI Infrastructure
- Encryption
- Signing
- Auditing

Cyber-Attack Scenarios vs UA

Boiler Explosion

- Stop feedwater, overheat drum, reintroduce feedwater
- Weaponized proof-of-concept exploit
- USB Infection



OPC UA

- Authentication of applications
- Signing of messages
- Auditing

OPC UA Security: Standards Based

- ICS Security Is Nothing New!
- Developed with industry security experts from multiple companies
- NIST and other experts reviewed the OPC standard
- Working with security Certification Groups to ensure it is current

Security: As a Reminder…

- OPC UA alone will not secure your systems
- People must enact and follow all policies/rules
- Systems require many different “parts” in order to be secure :
  - Anti-malware
  - Firewalls
  - Intrusion detection/prevention
  - Hardware controls (USB, DVD, Bluetooth etc.)
  - Network controls (routers, switches, cables etc.)
  - Operating System controls (file system, workstation etc.)
  - Versioning of software, hardware, and even firmware

Questions?

Nathan Pocock
Technical Director
OPC Foundation

Darek Kominek
Strategic Marketing Manager
MatrikonOPC

Paul Hunkar
Technical Director
DS Interoperability LLC