OPC and MES 2014 Finland

OPC UA Security

Uwe Steinkrauss (ascolab GmbH)

Getting real about the risk

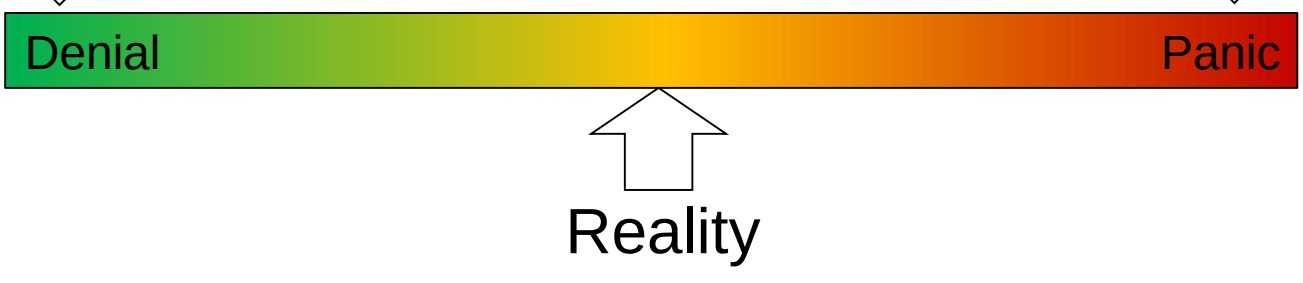
Stephen Cummings, director of the British government's Centre for the Protection of National Infrastructure,

"Cyberterrorism is a myth"

CNN INTERNATIONAL .com/US

September 27, 2007 -- Updated 1317 GMT (2117 HKT)

Mouse click could plunge city into darkness, experts say



- Cyber incidents are real and cyber security for industrial control systems must be taken seriously
- **but** it is a challenge that **can** be met

OPC FOUNDATION

Why, what and how to use?

- Thread

Why?
- Which security concerns are addressed by OPC UA?
- Which are not addressed by OPC UA security?

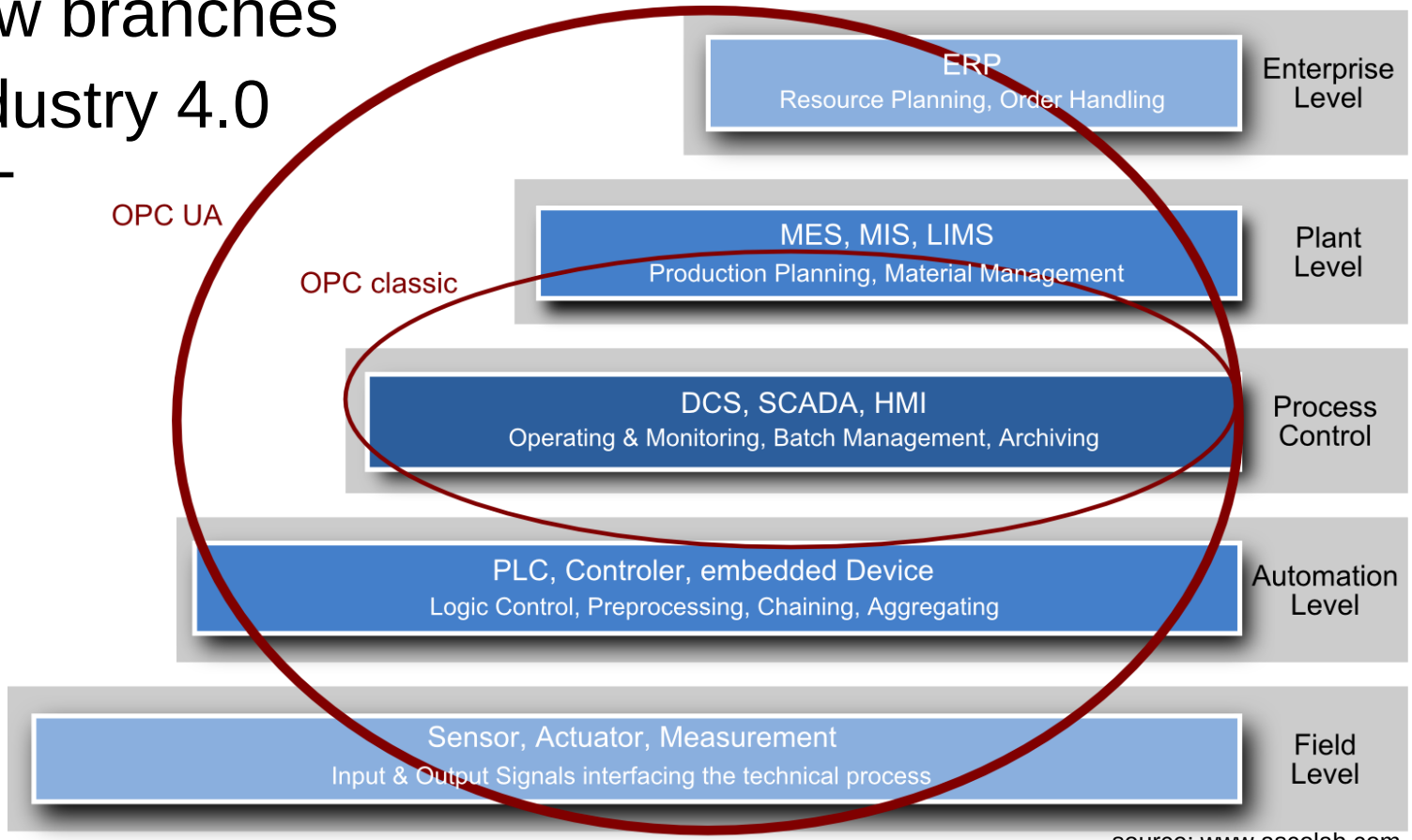
What?
- What are the concepts of OPC UA security?

How to Use?
- How to choose the target security level?
- How to manage OPC UA certificates?

- Secure

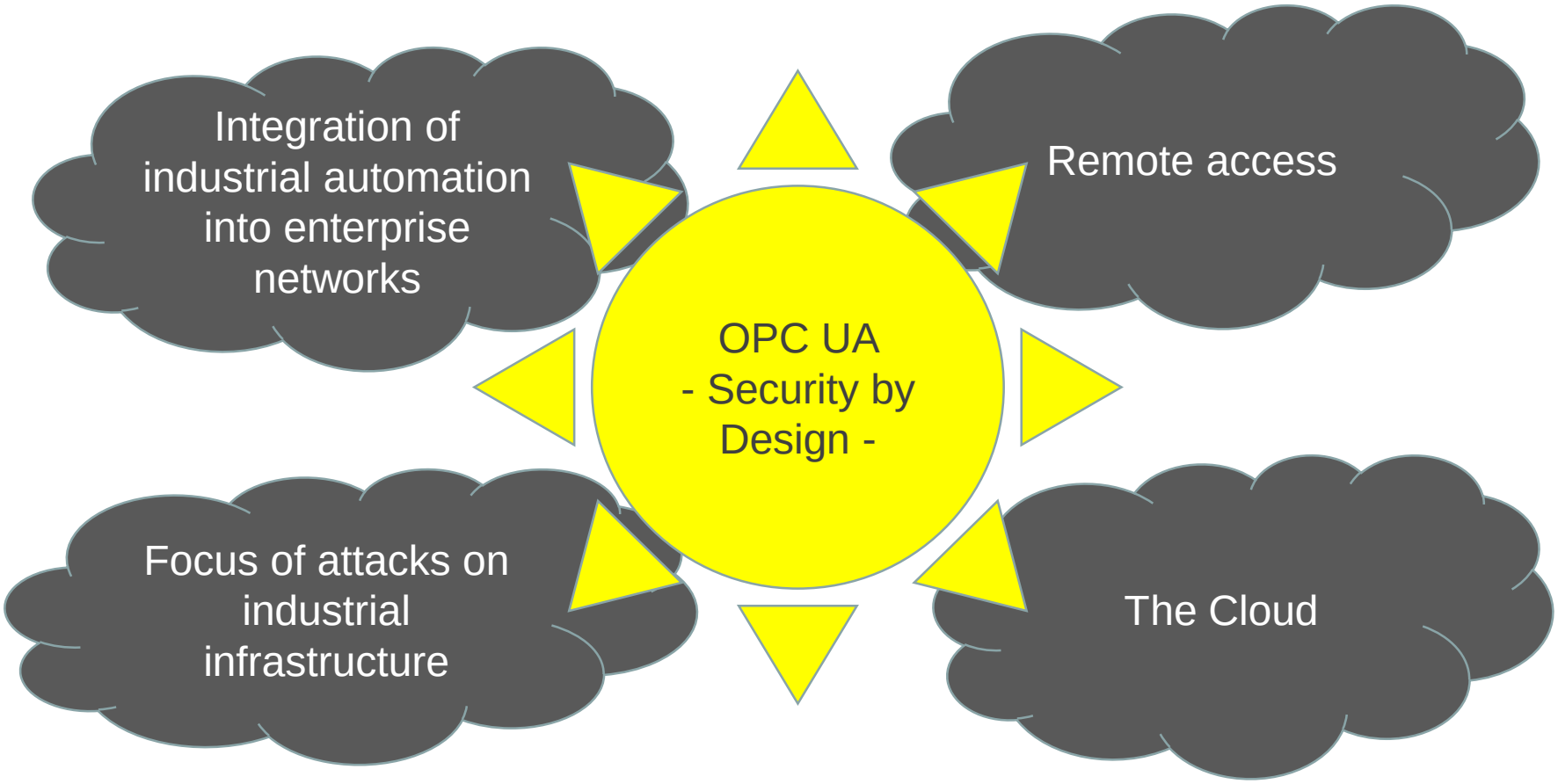
OPC UA - Communication

- OPC UA covers more applications
- new branches
- Industry 4.0
- IoT



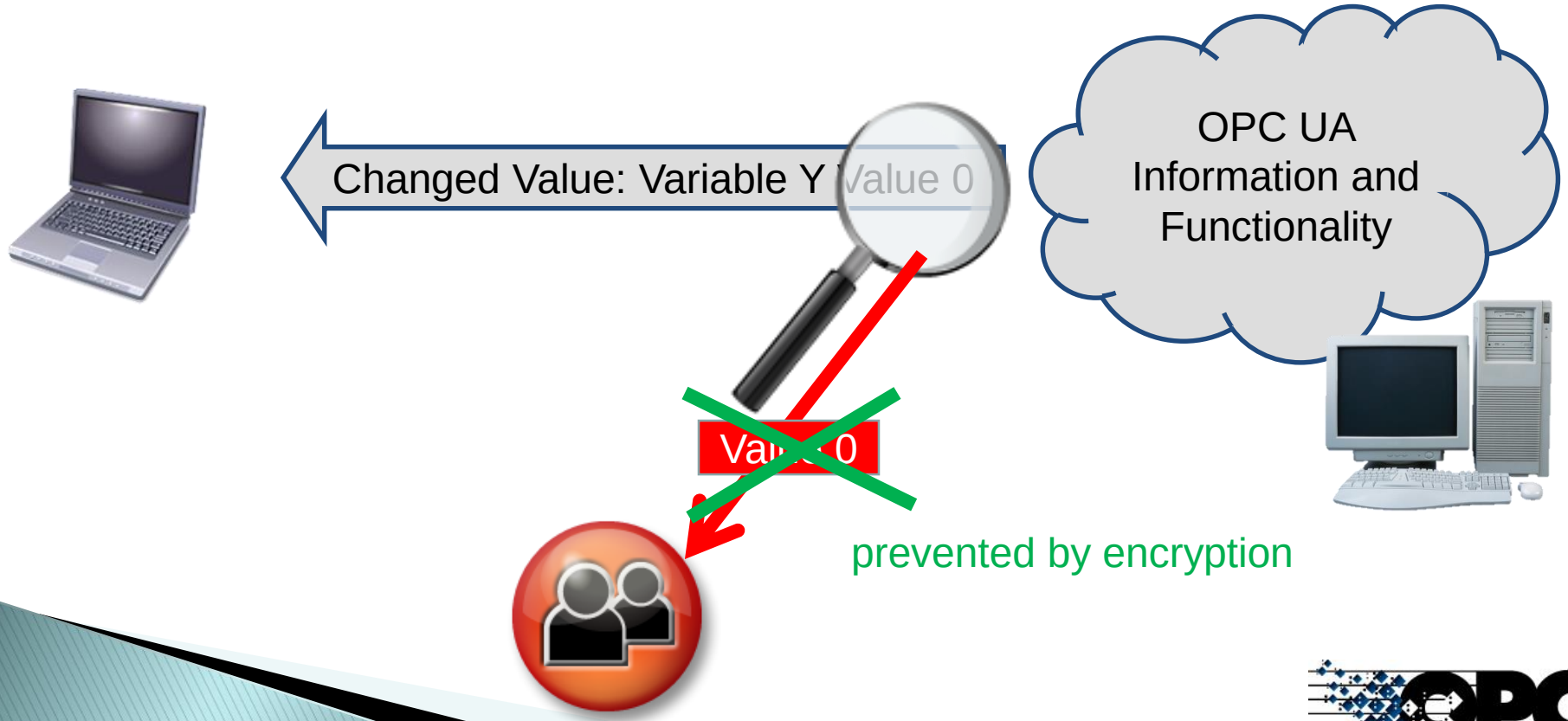
source: www.ascolab.com

Why – OPC UA Security?



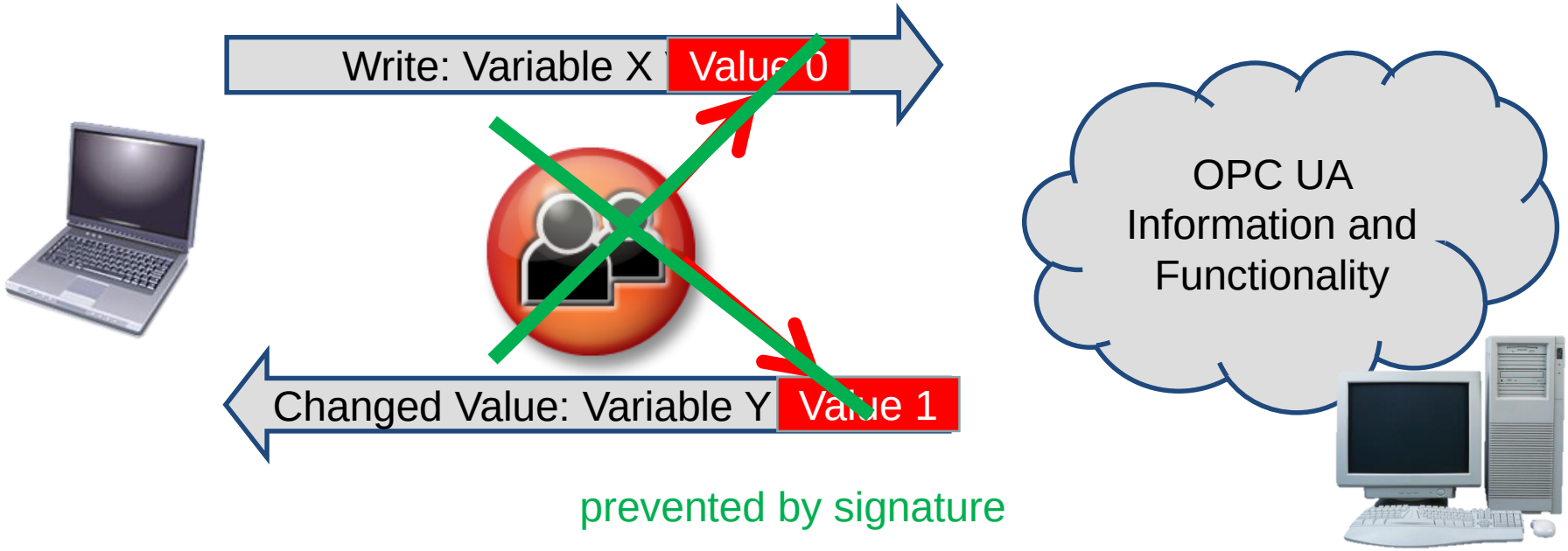
Security Aspect - 1

- Confidentiality
  → Not reading the content of a message



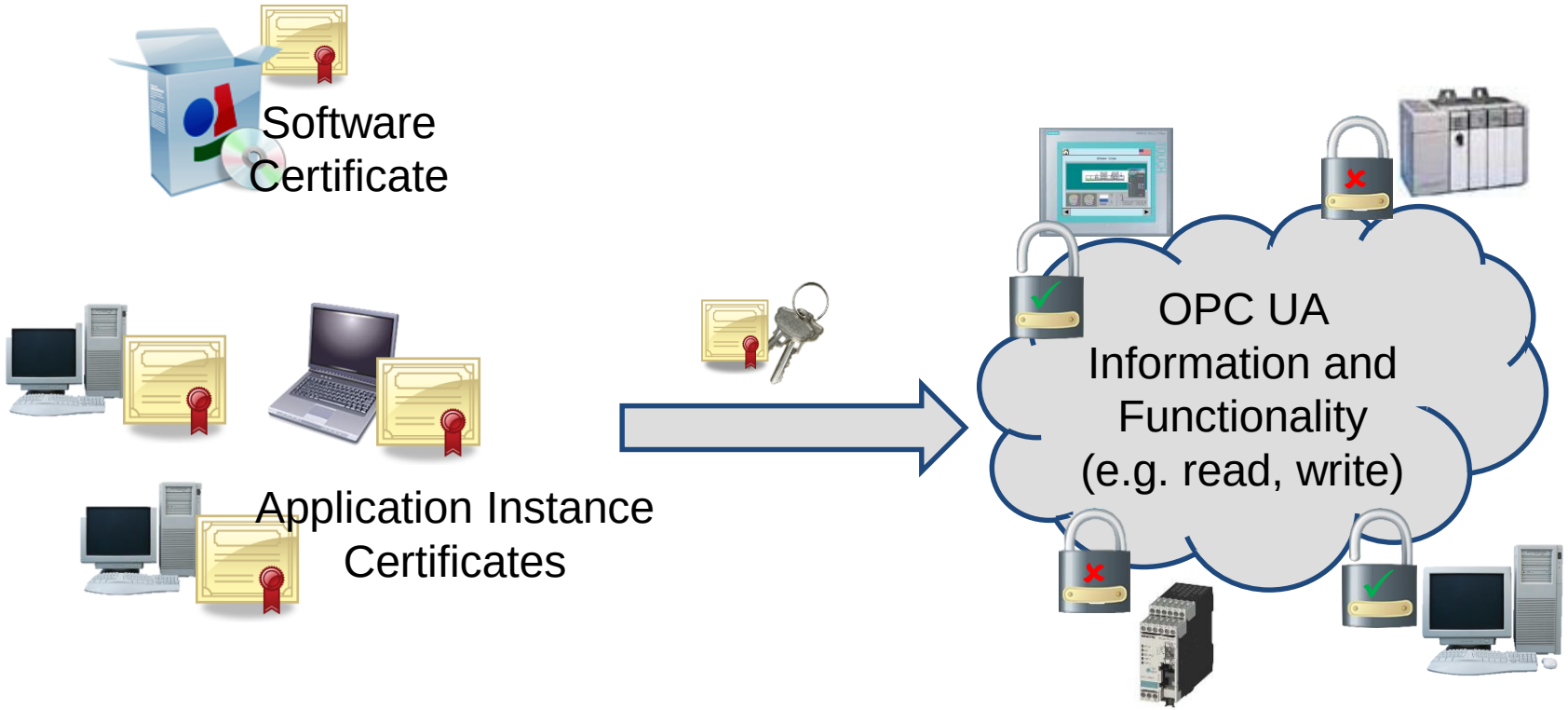
Security Aspect - 2

- Integrity
  → Not manipulating the content of a message



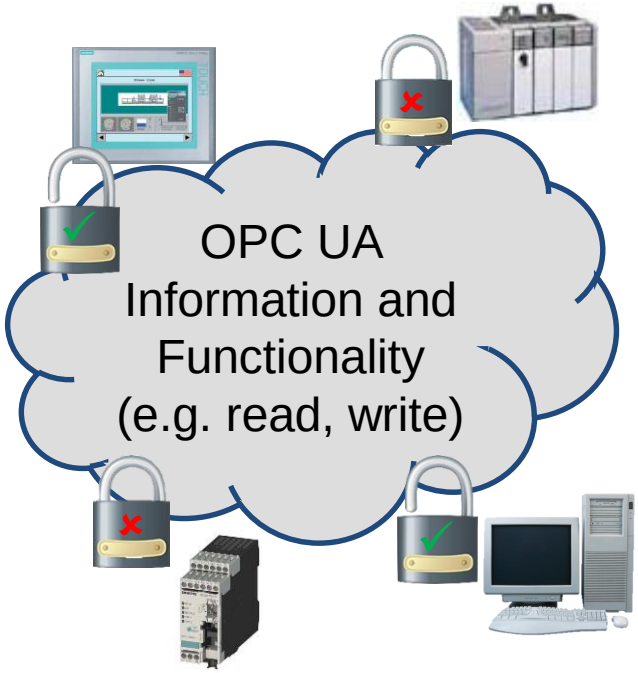
Security Aspect - 3

- Application Authentication
  → Identification and access control for applications



Security Aspect – 4 + 5

- User Authentication and Authorization
  → Identification and access control for users
  → Access/execution rights on item level

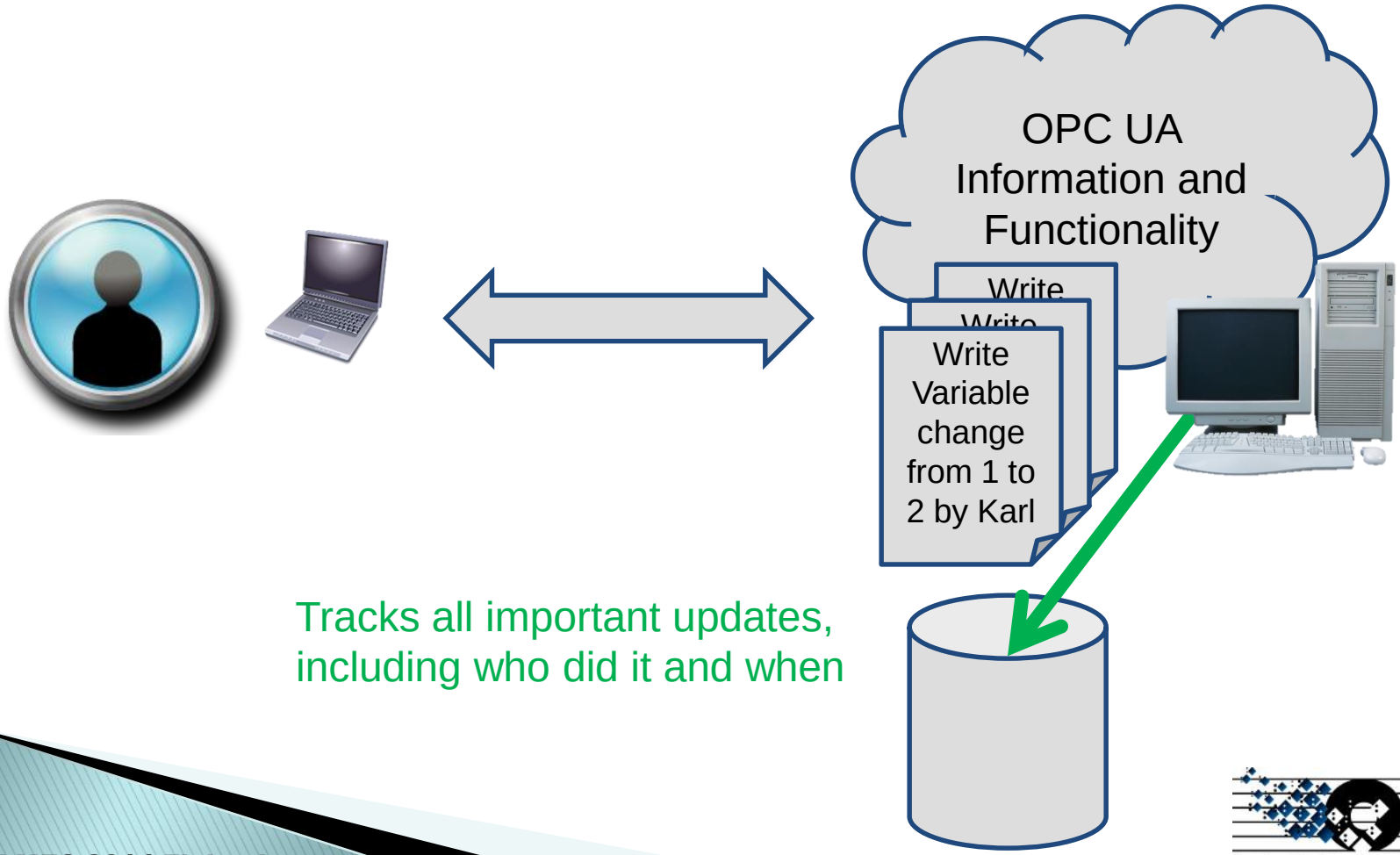


1. Authenticate User
(e.g. username and password)

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

Security Aspect - 6

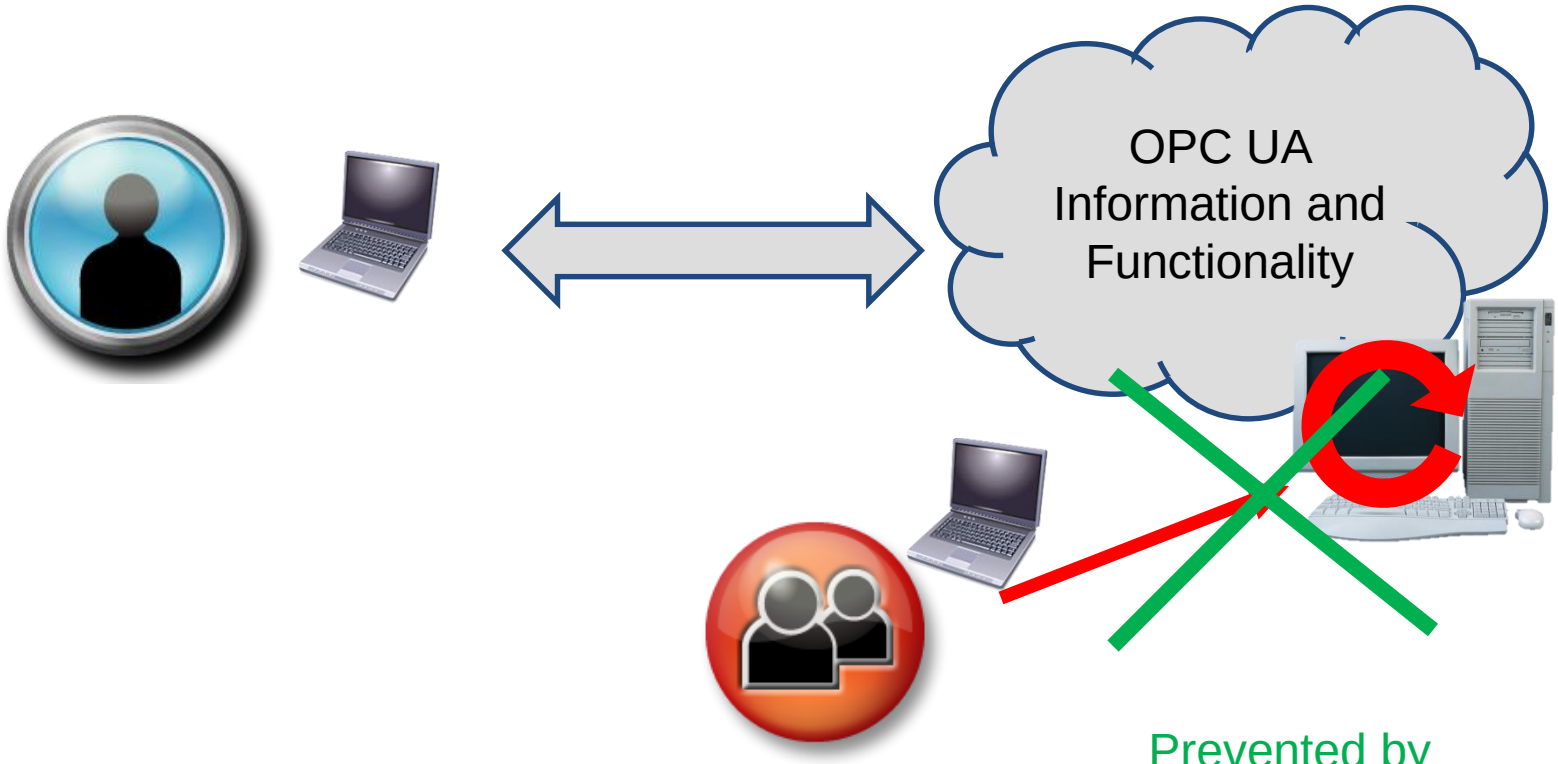
- Auditability
  →Tracking all important interactions



Tracks all important updates, including who did it and when

Security Aspect - 7

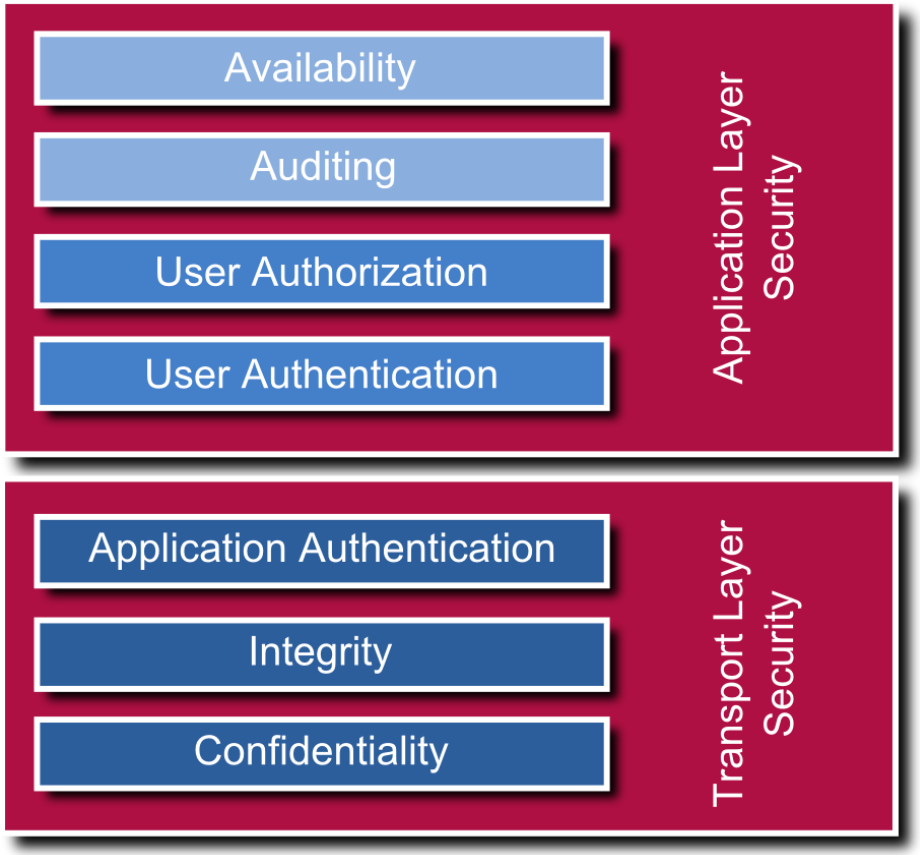
- Availability
  → Always be functional



Prevented by
availability controls

OPC UA Security-Concept

OPC UA covers 7 security aspects, which are in the core of the technology:



source: www.ascolab.com

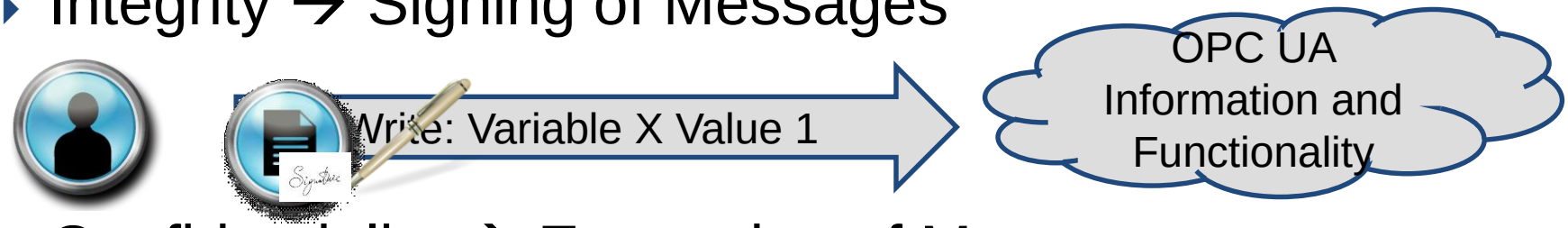
Application Layer Security

- Authentication of users
  - Username / password, WS-Security Token or X.509
  - Fits into existing infrastructures like Active Directory
- Authentication of individual installations
  - Application instance certificates
  - Certificate Authority (CA)

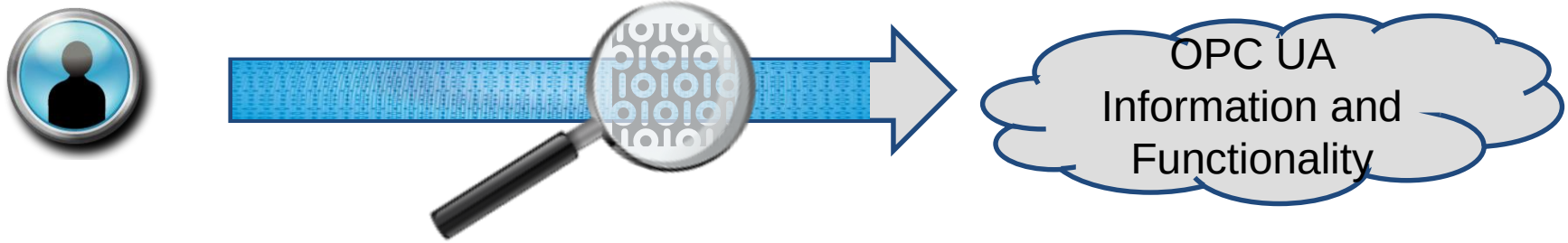
- Authorization
  - Enforcement of authorization is server-specific
  - Fine-granular information in address space
    - *AccessLevel* and *UserAccessLevel* – Reading and writing of values and their history
    - *WriteMask* and *UserWriteMask* – Writing of meta data
    - *Executable* and *UserExecutable* – Calling methods
    - Information not accessible is not visible to client (references, events, …)
- Auditability
  - Generating audit events for security related operations

Transport Layer Security

- Availability
  - Depends primarily on the site for protection
  - Minimum processing before authentication
    - Restricting message size
    - No security related error codes returned
    - …
- Integrity → Signing of Messages



- Confidentiality → Encrypting of Messages



NOT addressed by OPC UA

- **User Management**
  - No standard way how to manage users like adding, deleting, assignment to roles
  - No standard user roles
  - > This is server-specific or defined in companion specifications
- **User Authorization Management**
  - No standard way to define access rights
  - > This is server-specific or defined in companion specifications
- **User Authentication Management**
  - Not addressing mechanisms like biometric authentication, etc. directly, but can be used by the OPC UA infrastructure
  - No rules for passwords
    - Syntax rules (min. length, requires upper case, number, special characters, …)
    - How often they need to change
    - Where (not to) store passwords (e.g. note on screen)
- **Organizational issues**
  - No definition how to handle physical access to site
  - No definition of zones, security lifecycle or security policies
  - Not addressing training of personal
- Those **things are addressed by other specifications** like
  - IEC 62443 (ISA 99)
  - NERC CIP
  - Regulations and Corporate Standards

Practical Approach

- **Identify and Verify your Security Risks**

Drivers of cyber security

Compliance vs. risk management

- Many cyber security activities are motivated by regulation or similar compliance regulation
  - "Checking the boxes" exercises with least effort possible
  - Defining out of scope as much as possible

- Cyber security is a risk management activity
  - Should be driven by understanding of the risk
  - Should follow an organization's risk management framework

?

Consequence assessment

Answer the "*what if*" ?!

- What if I cannot operate this asset?
- What if someone else can operate this asset?
- What if this information gets disclosed?

What if someone opens this valve?
What if it does not close when it should?

Likelihood assessment

Accident / Error

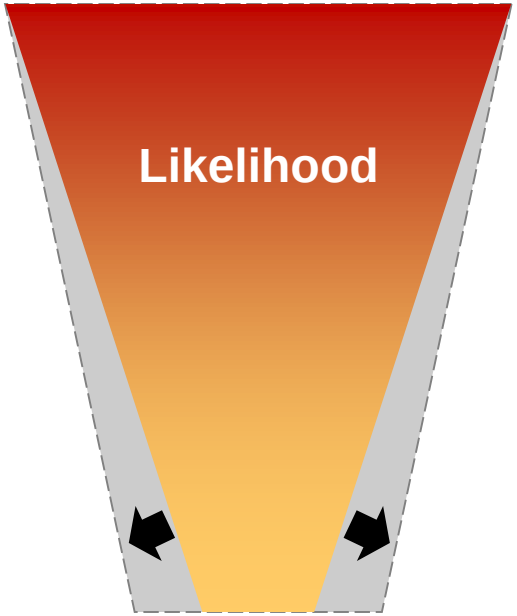
Rogue insider/employee

Malware/Virus/Trojans

Thieves / extortionists

Sabotage / competitors

Enemies / nation states / terrorists



→ Not enough recorded incidents or statistical data

Choosing appropriate security

Risk management based approach

- Identify critical assets
- Identify potential threats
- Assess likelihood of attack types
- Assess potential consequences of different types of security breaches
- Derive security objectives
- Select appropriate security controls

Using OPC UA security

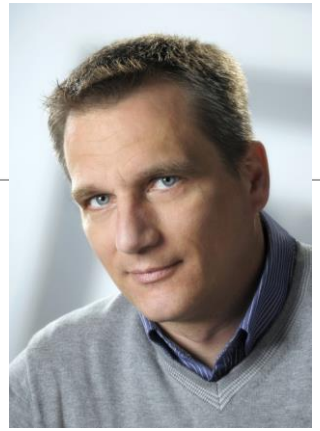
- Select appropriate security controls for each of the critical assets
- Implement and maintain selected security controls

- The OPC UA Security Model support includes
- Different security policies specified in the standard
- Product design and system engineering define when to use which policies
- Endpoints support security policies, exposed in Discovery Services
- SecureChannel Services utilize supported policies

Conclusion

- **Use of OPC UA security must be embedded in a security management system to provide meaningful security**
- **OPC UA is secure-by-design** and addresses security concerns by providing
  - Authentication of
    - Users
    - Application instances
    - (Software)
  - Confidentiality and integrity by signing and encrypting messages
  - Availability by minimum processing before authentication
  - Auditability by defined audit events for OPC UA operations
- OPC UA allows to setup different levels of security
- OPC UA certificate management can be
  - integrated into existing infrastructure of the site or
  - newly set up based on requirements

Thanks for Your Attention !



Uwe Steinkrauss
Executive Director

ascolab GmbH
Am Weichselgarten 7
D-91058 Erlangen
Phone +49-9131-691-120
info@ascolab.com