

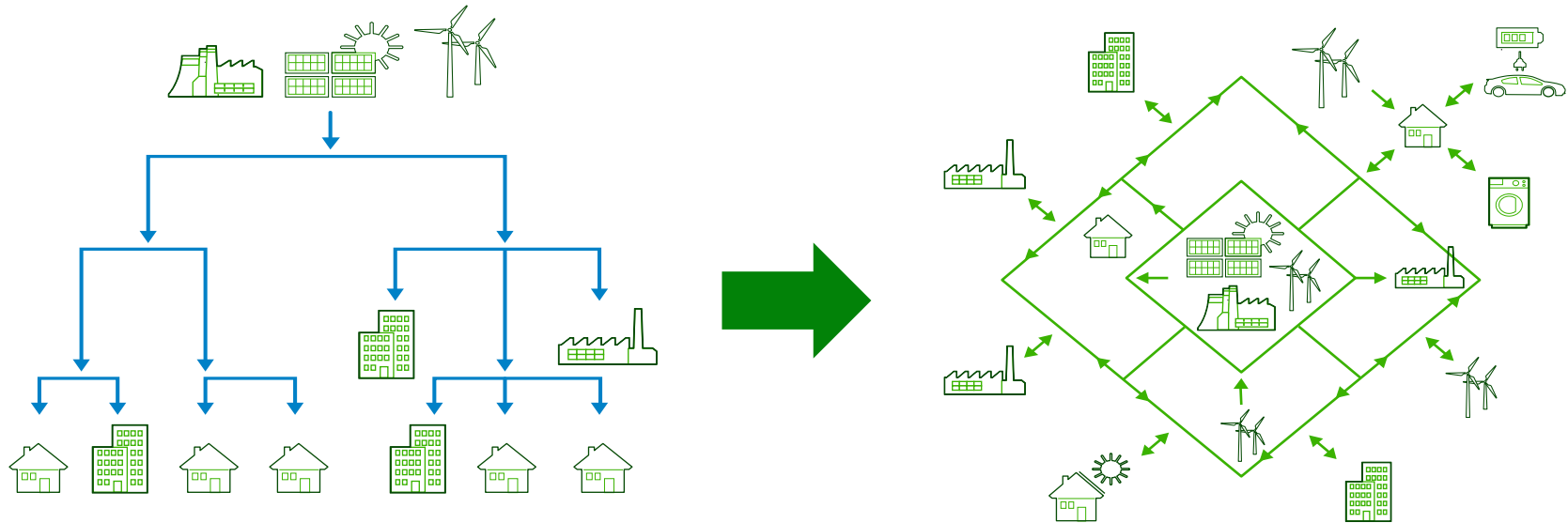
Actual trends in development of Power System Relay Protection and Automation
1–5 June 2015, Sochi (Russia)



Cyber Security measures in Protection and Control IED's

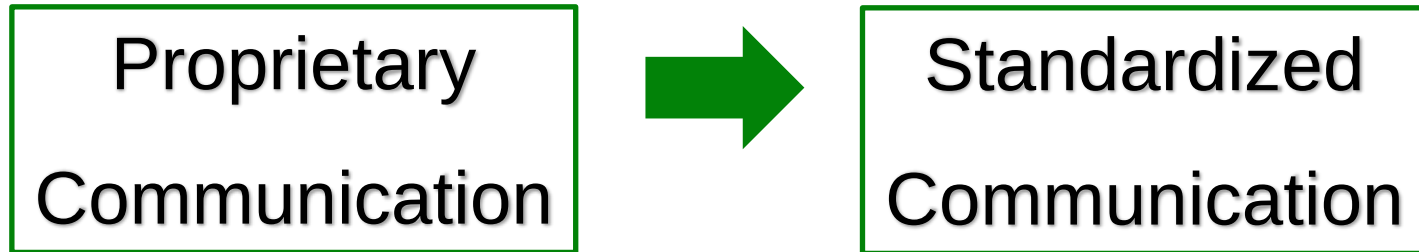
Krister Hagman (KH)
ABB Power Systems
Sweden
krister.hagman@se.abb.com

Trend in the Power Grid



Transforming from conventional Power Grid to Smart Grid

Trend in the Power Grid

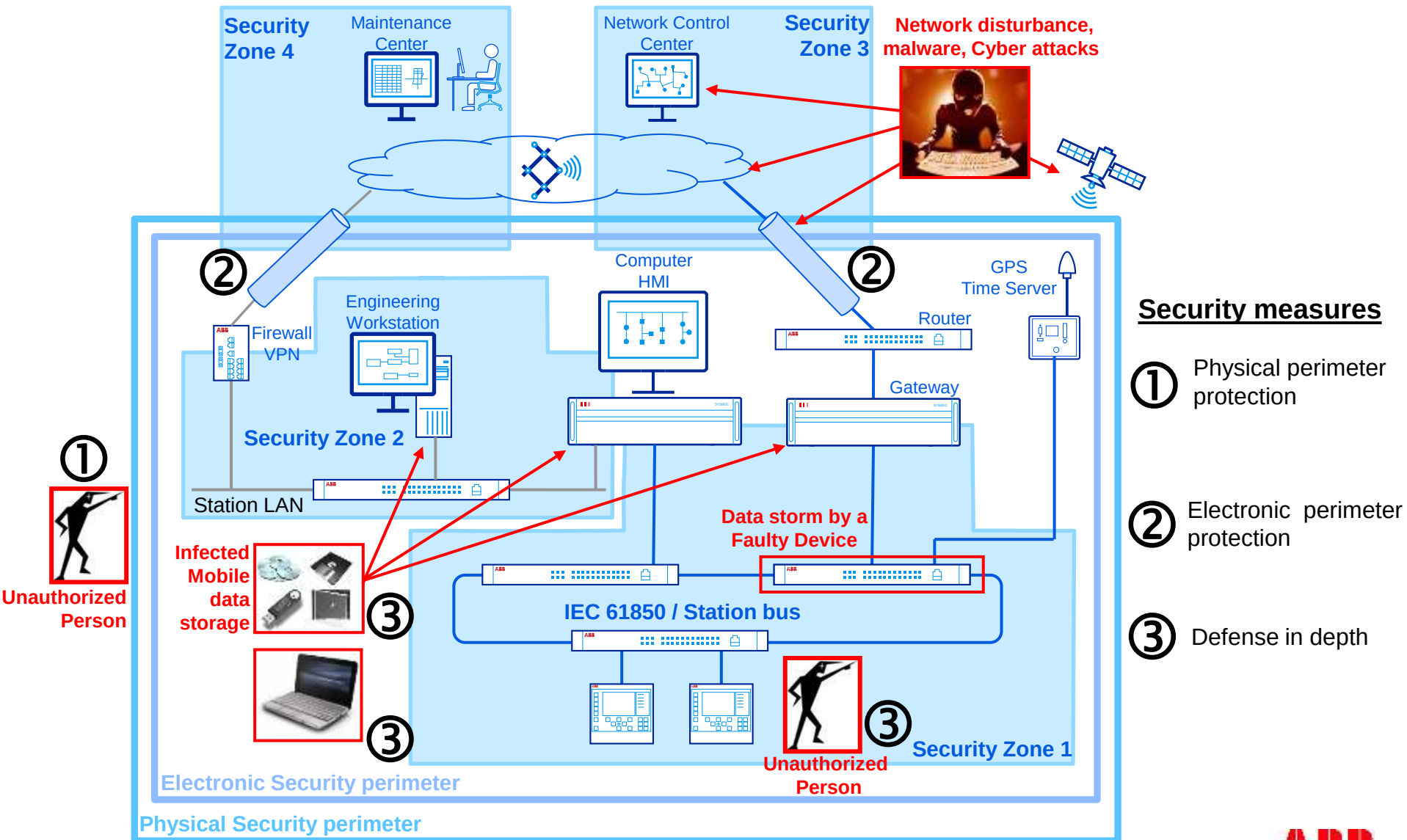


Gave a false feeling of
"Security by Obscurity"

More accessible to ALL!

What measures can we take?

Robustness threats



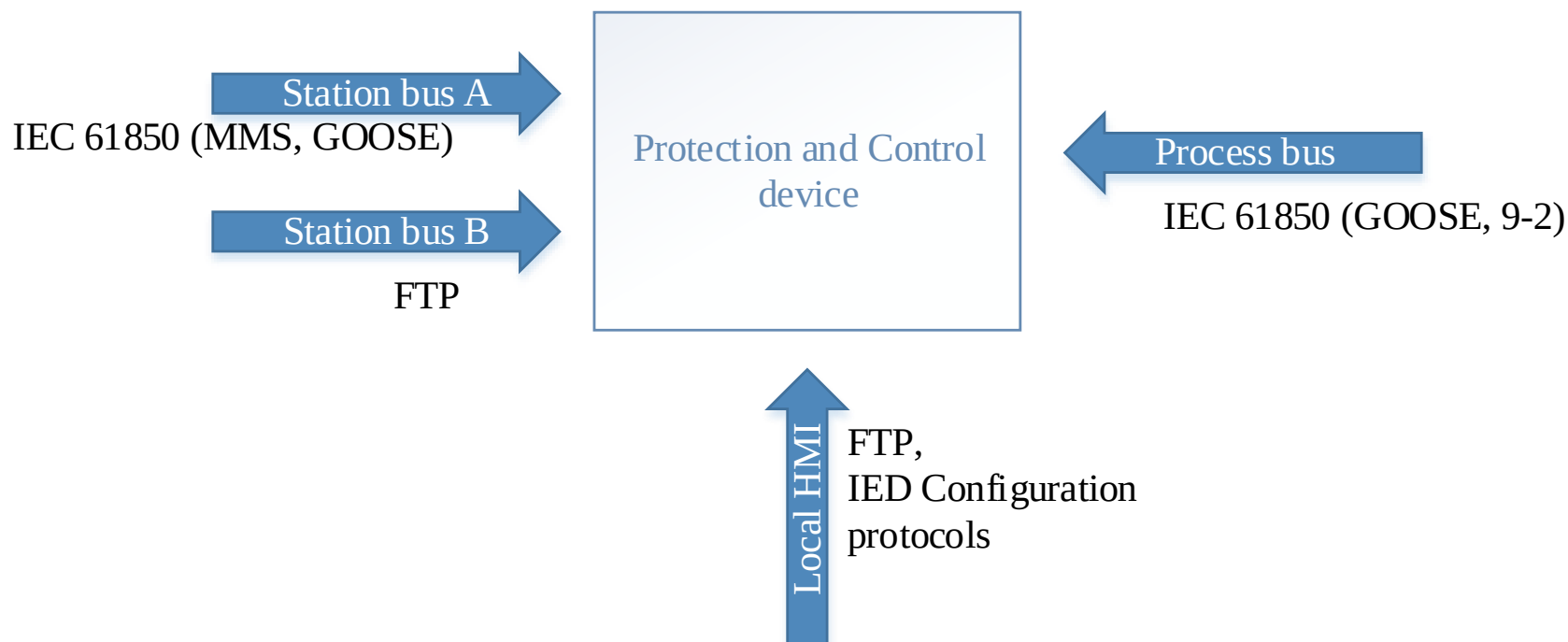
Hardening

Authorization

Authentication

Auditability

#1 Hardening – Attack Surface



#1 Hardening – Attack Surface

<i>Protocol / Interface</i>	<i>Station bus A</i>	<i>Station bus B</i>	<i>Process bus</i>	<i>Local HMI</i>
<i>IEC 61850 – MMS</i>	X			
<i>IEC 61850 - GOOSE</i>	X		X	
<i>IEC 61850 – 9-2</i>			X	
<i>FTP</i>		X		X
<i>IED Configuration protocol</i>				X

#1 Hardening - Fuzzing

fuzzing
black
defects
injection
vulnerabilities
segmentation
fail bugs testing
buffer
box overflows
data
random
fault

#2 Authorization

- First level of defense – Use Authorization
 - User name and Password
 - Not only on perimeter devices but in the entire system
 - Make use of Centralized Account Management technologies
- Role based Access
 - IEC 62351-8



	Right A	Right B	Right C	Right D	Right E	Right F	Right G	Right H
Role A	X			X				
Role B	X	X		X				
Role C	X	X	X	X		X	X	
Role D	X	X		X	X			
Role E	X	X					X	

#2 Authorization

	Right A	Right B	Right C	Right D	Right E	Right F	Right G	Right H
Role A	X			X				
Role B	X	X		X				
Role C	X	X	X	X		X	X	
Role D	X	X		X	X			
Role E	X	X					X	



User 1: Role A + C

User 2: Role B

User 3: Role A + D + E

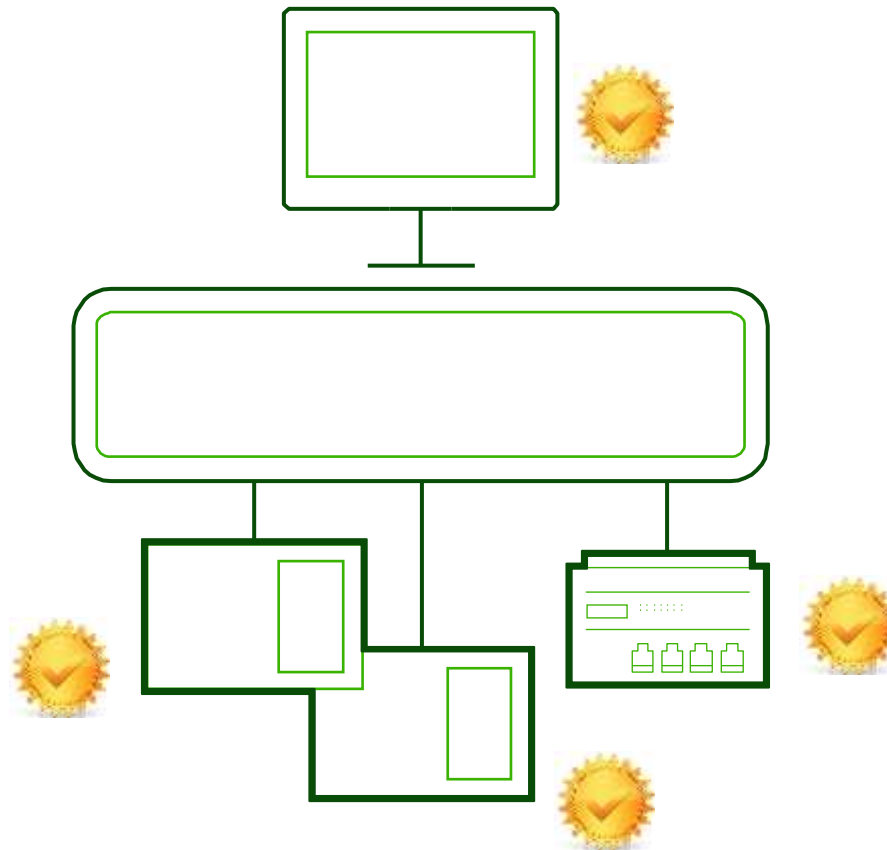
User 4: Role E

#3 Authentication

- The user must be certain they operate the proper device
- The device must be certain it is an authenticated user/system

Certificates

#3 Authentication – Trusted peers



#4 Auditability

- Observability is key
- In case of event – analyze logs
- In case of isolation – offline logs
- Centralized logs
 - Huge amount of data
 - Use pattern recognition to find abnormalities



Conclusion

Use technologies from IT world

Don't rely on physical perimeter protection

Don't rely on security by obscurity

Keep the system up-to-date

Observe and measure to build up knowledge

Continue the work on pattern recognition

Thanks for listening