

TETRA Verboden & Industriële security

AGENTSCHAP
INNOVEREN &
ONDERNEMEN

28/04/16 4^{de} Gebruikersgroep vergadering



KU LEUVEN



howest
De Hogeschool West-Vlaanderen

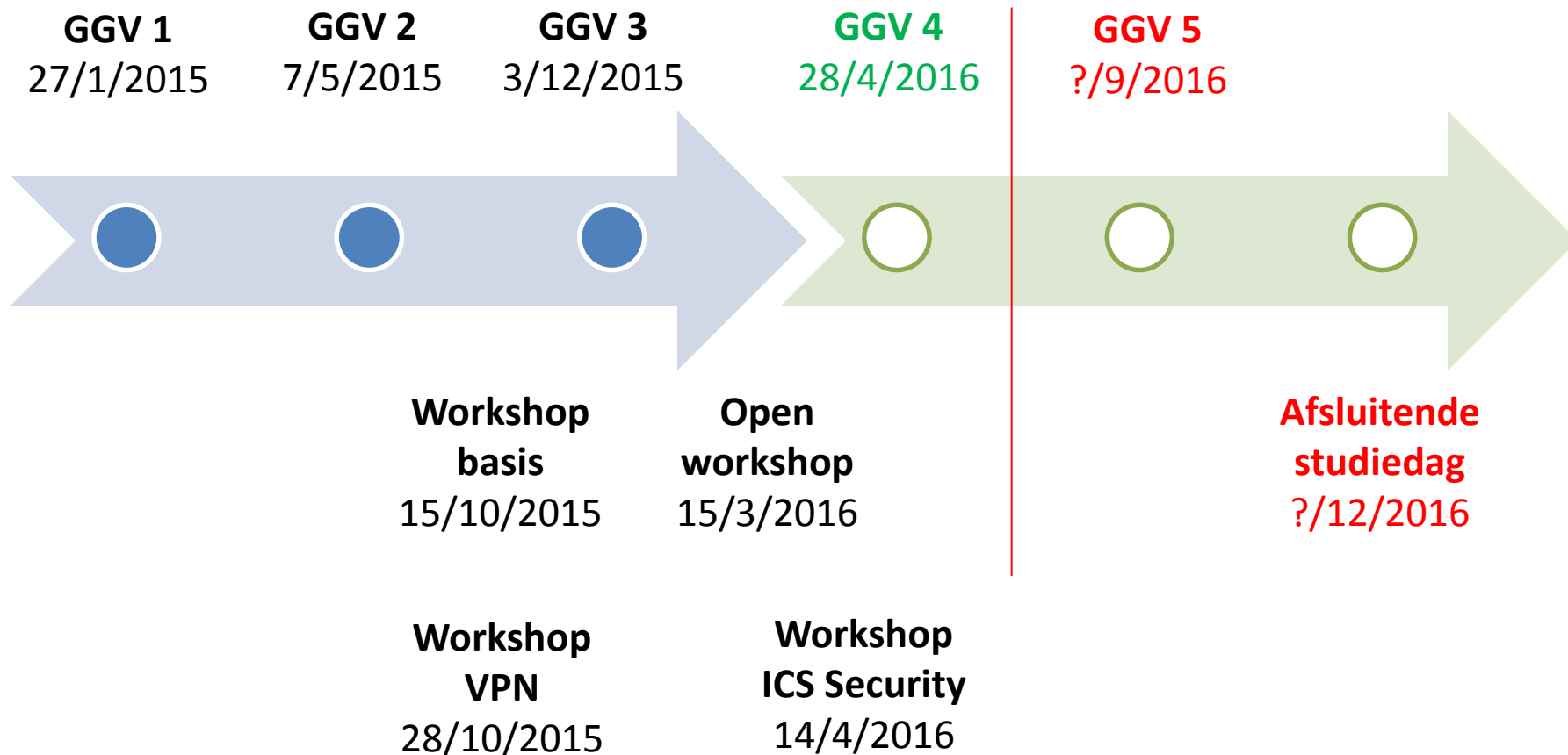
28/04/16 4^{de} Gebruikersgroep vergadering

- 15h45** Ontvangst met koffie
- 16h00** Verwelkoming en introductie (E-bo Enterprises)
- 16h10** Project status (Johannes Cottyn, XiaK-UGent)
- 16h25** Aanvallen op industriële installaties mogelijke technieken, doelwitten en de gevolgen (Hendrik Derre, E&A-KUL)
- 16h50** Integrating mobile devices in Industrial Environments (Jan Vossaert, MSEC-KUL)
- 17h15** Ervaringen vanuit industriële case studies (Tijl Deneut, Howest & Thibaut Demasure, XiaK-UGent)
- 17h45** Conclusie, volgende stappen & discussie (Johannes Cottyn, XiaK-UGent)
- 18h15** Afsluitende receptie

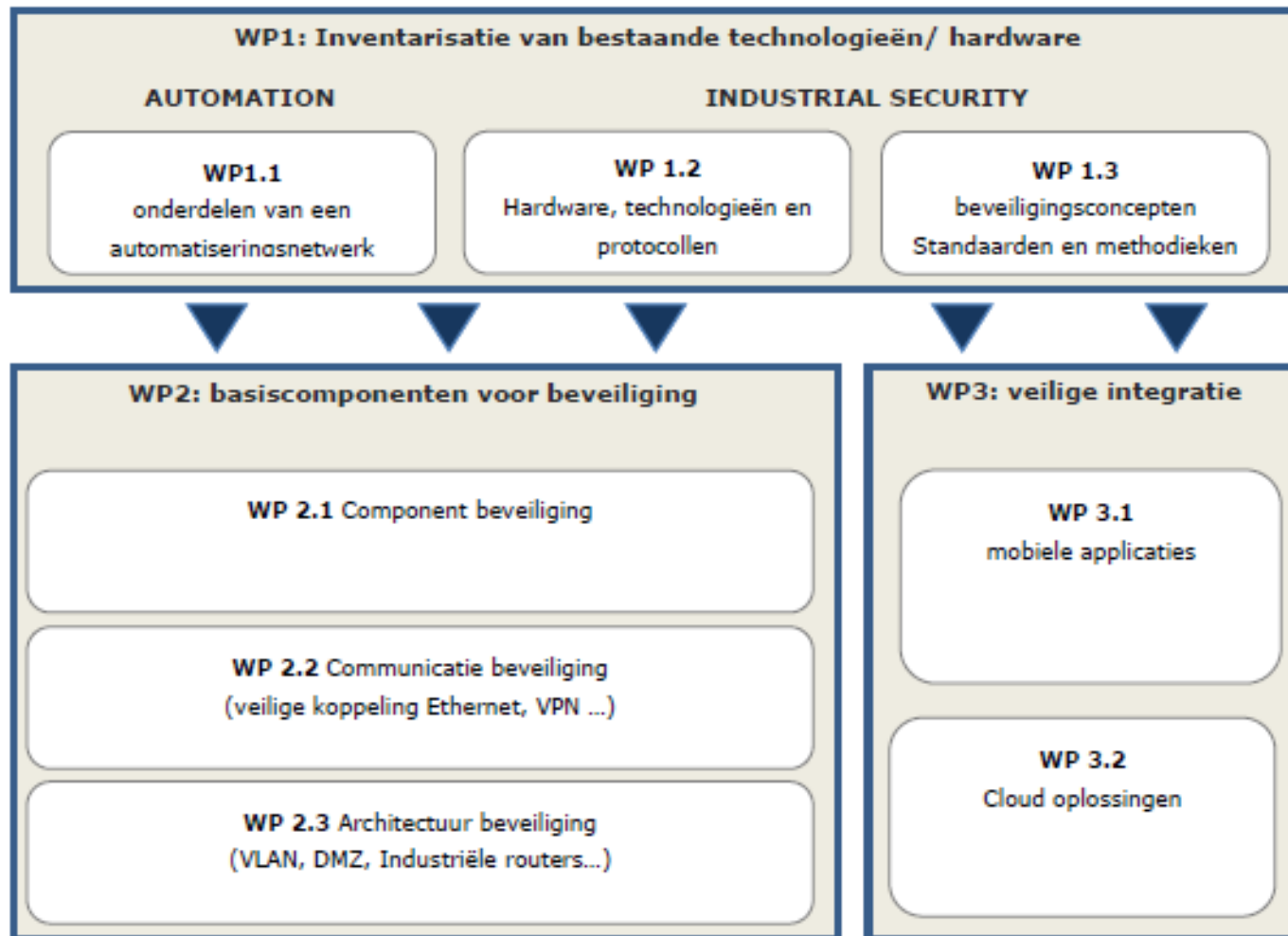
TETRA Verboden & Industriële security

AGENTSCHAP
INNOVEREN &
ONDERNEMEN

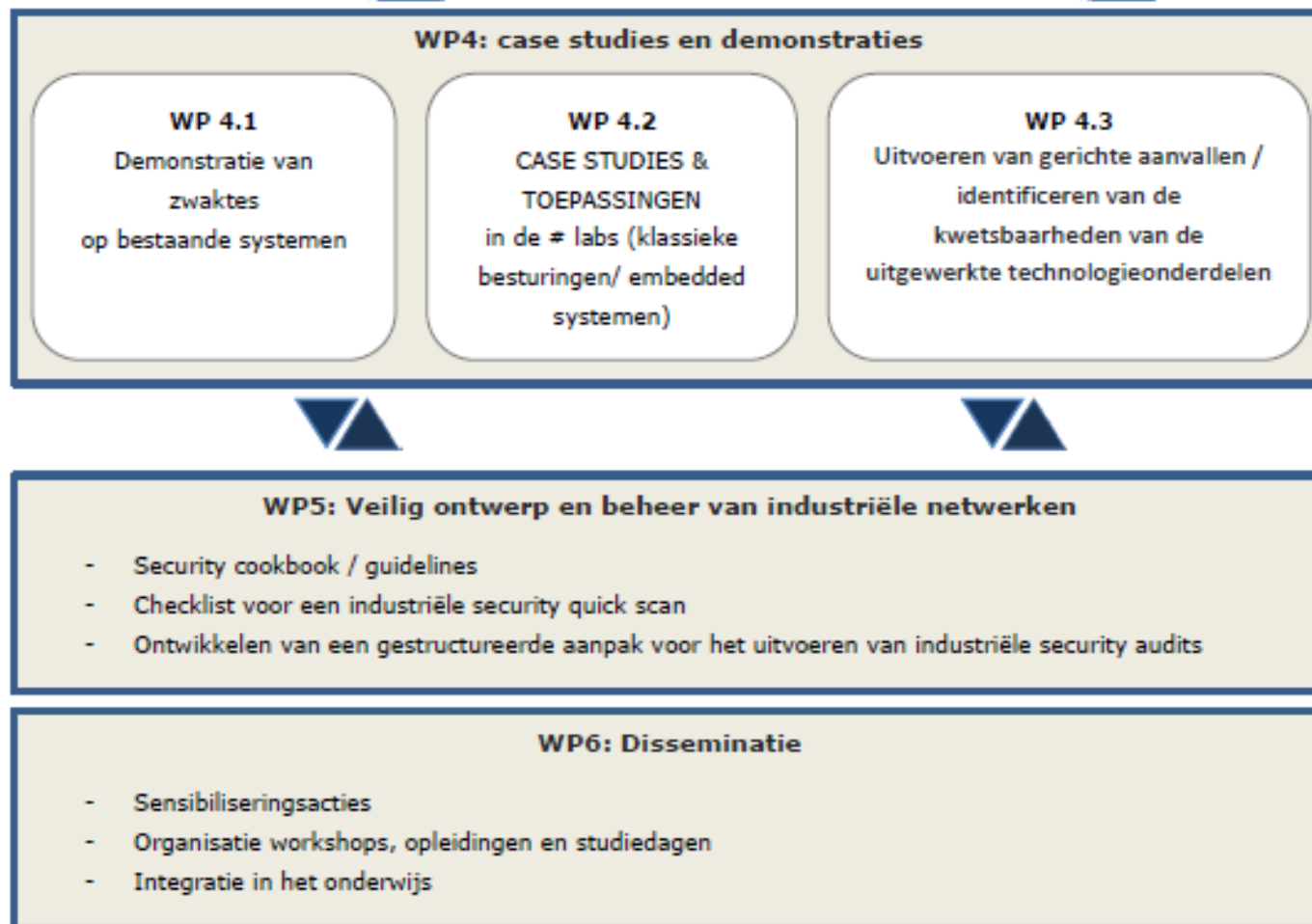
Project status



Project status



Project status



Project status

GebruikersPoll

Vraag 1: In welke mate is het project nog steeds relevant voor uw onderneming

3-12-2015



Vraag 5: In welke mate verwacht u dat de projectresultaten bij uw eigen onderneming (of uw ledenbedrijven) op korte termijn toegepast zullen worden (KT is tijdens het project of < 1 jaar na afloop van het project)

3-12-2015

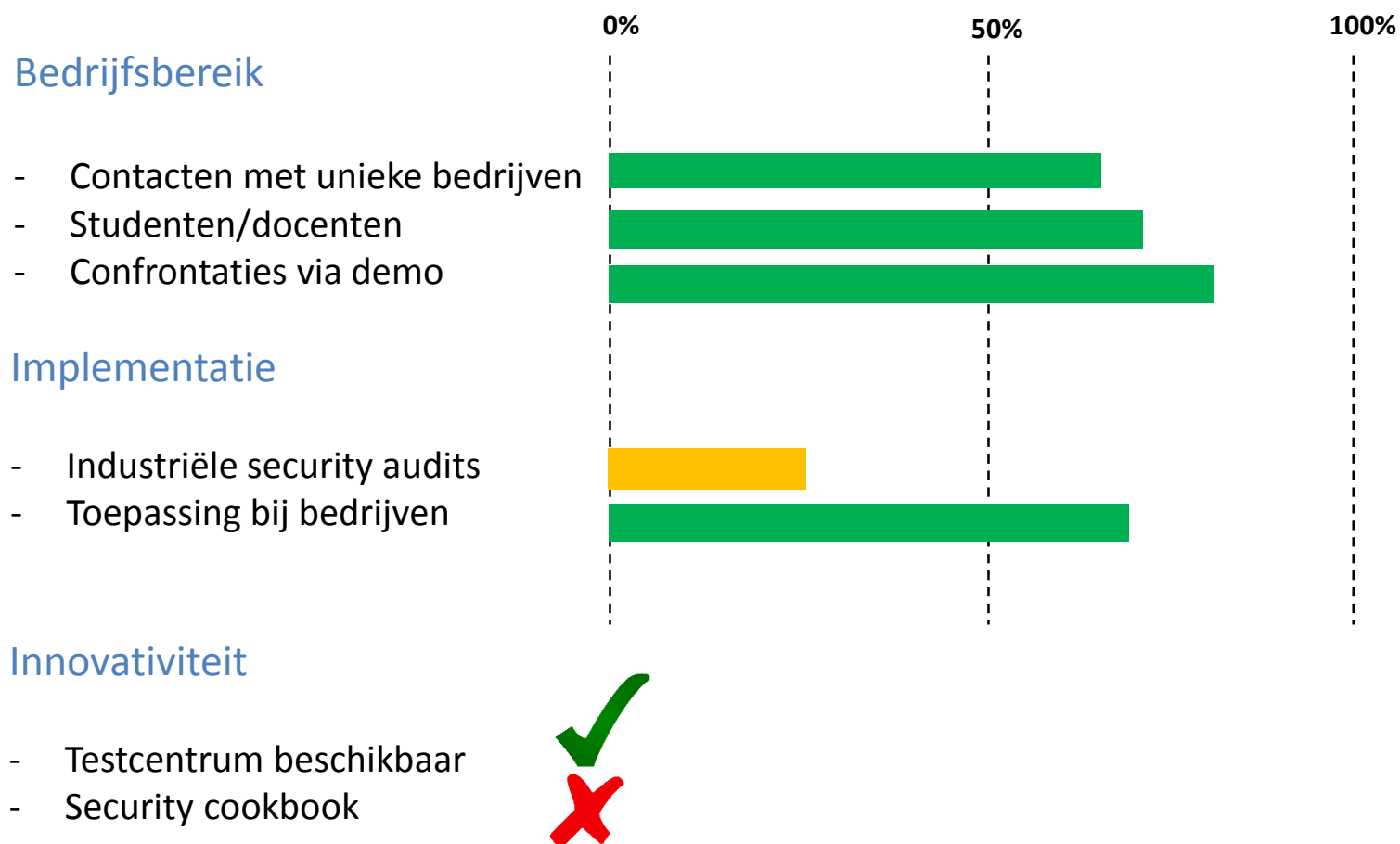


Antwoorden

- Resultaten worden al toegepast
- De resultaten zullen wellicht binnen het jaar na afloop van het project worden toegepast
- Resultaten blijken tot op heden niet bruikbaar voor mijn onderneming (of uw ledenbedrijven) op kt maar mits bedrijfsspecifiek onderzoek zal dit in de toekomst wel het geval zijn
- Resultaten blijken tot op heden niet bruikbaar voor mijn onderneming (of uw ledenbedrijven)
- Weet niet

Project status

Key Performance Indicatoren



28/04/16 4^{de} Gebruikersgroep vergadering

- 15h45** Ontvangst met koffie
- 16h00** Verwelkoming en introductie (**E-bo Enterprises**)
- 16h10** Project status (Johannes Cottyn, **XiaK-UGent**)
- 16h25** Aanvallen op industriële installaties mogelijke technieken, doelwitten en de gevolgen (Hendrik Derre, **E&A-KUL**)
- 16h50** Integrating mobile devices in Industrial Environments (Jan Vossaert, **MSEC-KUL**)
- 17h15** Ervaringen vanuit industriële case studies (Tijl Deneut, **Howest** & Thibaut Demasure, **XiaK-UGent**)
- 17h45** Conclusie, volgende stappen & discussie (Johannes Cottyn, **XiaK-UGent**)
- 18h15** Afsluitende receptie

28/04/16 4^{de} Gebruikersgroep vergadering

- 15h45** Ontvangst met koffie
- 16h00** Verwelkoming en introductie (E-bo Enterprises)
- 16h10** Project status (Johannes Cottyn, **XiaK-UGent**)
- 16h25** Aanvallen op industriële installaties mogelijke technieken, doelwitten en de gevolgen (Hendrik Derre, **E&A-KUL**)
- 16h50** Integrating mobile devices in Industrial Environments (Jan Vossaert, **MSEC-KUL**)
- 17h15** Ervaringen vanuit industriële case studies (Tijl Deneut, **Howest** & Thibaut Demasure, **XiaK-UGent**)
- 17h45** Conclusie, volgende stappen & discussie (Johannes Cottyn, **XiaK-UGent**)
- 18h15** Afsluitende receptie

Volgende stappen

Security cookbook

Focus van het cookbook:

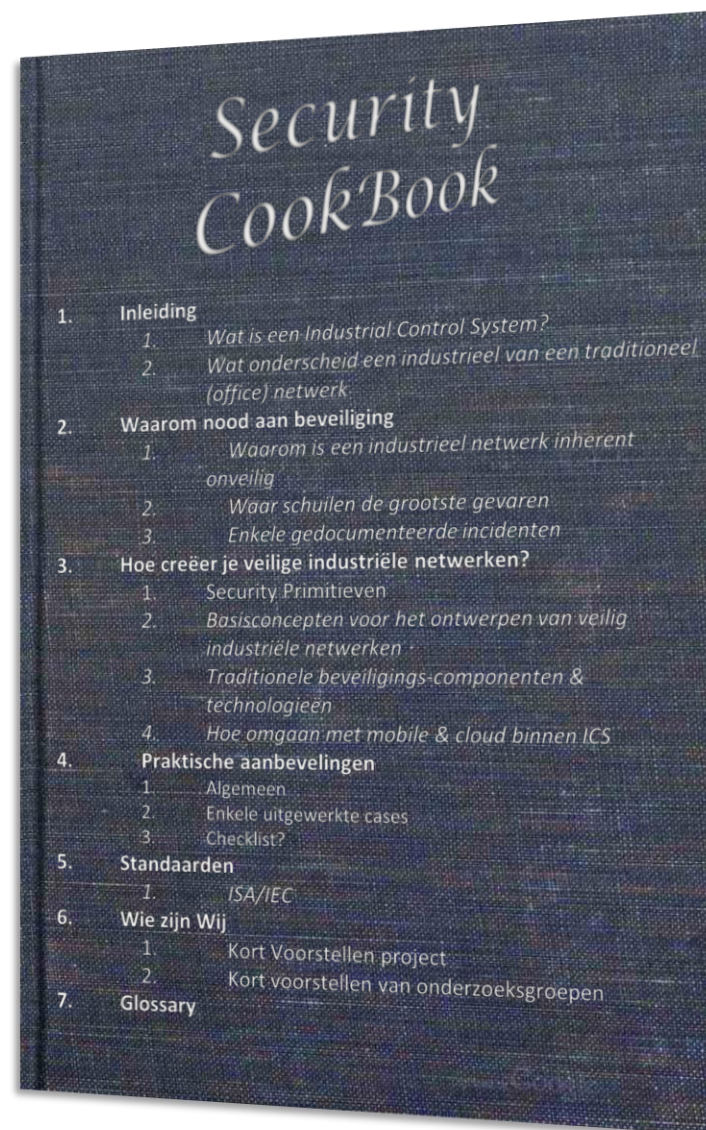
- Toelichten problematiek
- Aanbrengen basisbegrippen en concepten
- Praktische aanbevelingen

Praktisch

- Brochure van 20/30 tal pagina's
- Geschreven in het Nederlands
- Laagdrempelig (weinig voorkennis vereist)
- Digitaal en op papier verkrijgbaar

Doelstelling Timing: GGV september

Had u graag nog iets toegevoegd?



Volgende stappen

Industrial security checklist



- Laagdrempelig
- Gebruiksvriendelijk
- Online

- Vooral sensibiliseren
- Automatiseringscontext

1 Communicatie protocol

- Beschrijving
- Authenticatie
- Encryptie
- Integriteit
- Mechanismes

2 Applicatie/ Service

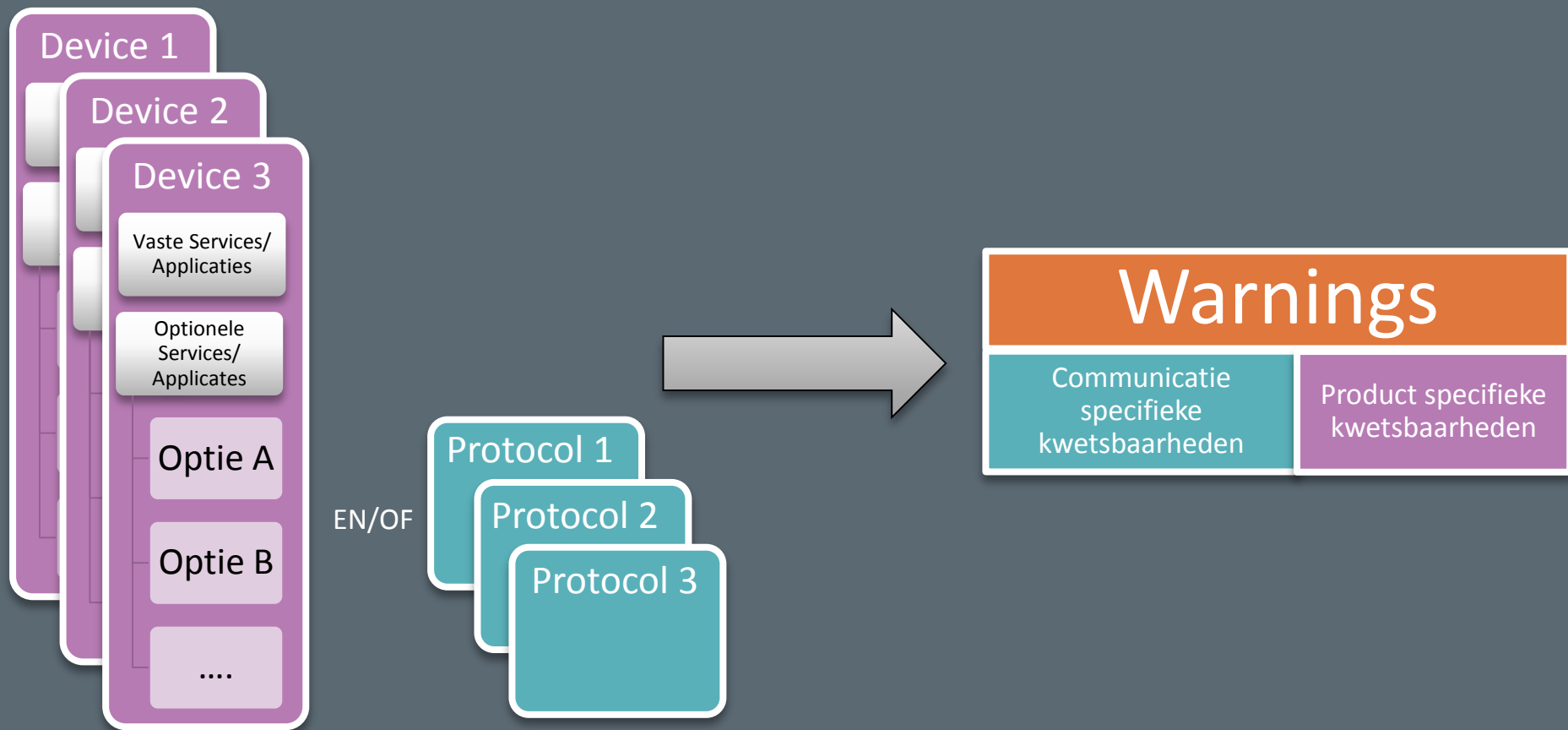
- Beschrijving
- Protocollen
- Implementatie protocollen
- Partner applicaties

3 OS

- Beschrijving
- Problemen inherent aan OS

4 Device

- Beschrijving
- OS
- Applicaties/ Services
- Implementatie applicaties/ services
- Toestel specifieke problemen



Controller



HMI



SCADA



Switches



Drives



IO Device



Routers

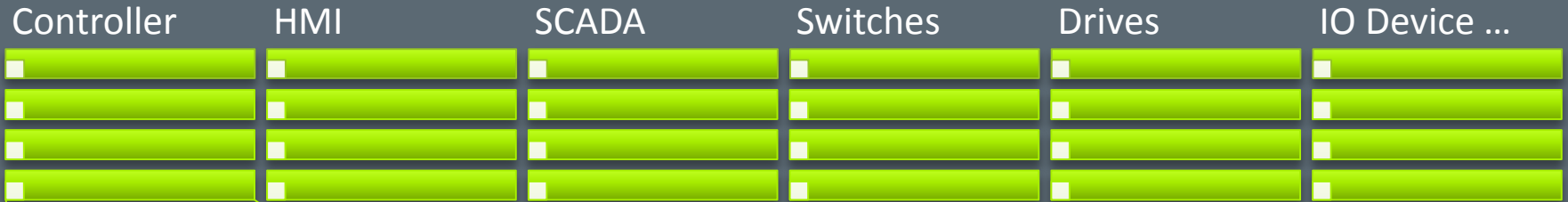


PC/Server



...





Controller D

☐ Vaste Instellingen

☐ Webserver

☐ FTP server

☐ SNMP

☐ Modbus TCP server

☐ ...

☐ OS

☐ Profinet controller

☐ Programming interface

☐ ...

Controller	HMI	SCADA	Switches	Drives	IO Device ...
☐	☐	☐	☐	☐	☐
☐	☐	☐	☐	☐	☐
☐	☐	☐	☐	☐	☐
☒	☐	☐	☐	☐	☐

Controller D

☒ Vaste Instellingen

☒ Webserver

☐ FTP server

☐ SNMP

☒ Modbus TCP server

☐ ...

☒ OS

☒ Profinet controller

☒ Programming interface

☒ ...

Controller	HMI	SCADA	Switches	Drives	IO Device ...
☐	☐	☐	☐	☐	☐
☐	☒	☐	☐	☐	☐
☐		☐	☐	☐	☐
☒		☐	☐	☐	☐

HMI B

☒ Vaste Instellingen

- ☒ OS
- ☒ Webbrowser
- ☒ Programming interface
- ☒ ...

Controller	HMI	SCADA	Switches	Drives	IO Device ...
☐	☐	☐	☐	☐	☐
☐	☒	☐	☒	☐	☐
☐	☐	☐	☒	☐	☒
☒	☐	☐	☐	☐	☐

Product specifieke kwetsbaarheden

Controller D

Webserver

- Geen authenticatie: laat onbevoegde toegang tot de webserver toe

Programming

- Mogelijkheid tot onbevoegd downloaden van configuraties

HMI B

SNMP agent

- Foutieve implementatie van SNMP zorgt dat dit toestel zijn administrator + wachtwoord vrijgeeft bij SNMP request

Communicatie specifieke kwetsbaarheden

Profinet DCP

Controller D

Switch C

IO device C

- De IP instellingen van alle devices die Profinet ondersteunen kunnen aangepast worden via het Profinet DCP protocol

Modbus TCP

Controller D

HMI B

- Modbus TCP bezit geen mogelijkheden voor authenticatie en autorisatie, dus kan ieder deelnemer in het netwerk in feite IO- en registerwaardes aanpassen

Discussie

Wat wilt u nog aan bod zien komen?



TETRA Verboden & Industriële security

AGENTSCHAP
INNOVEREN &
ONDERNEMEN

Volgende data?

