



Heeft u security incidenten nodig om tot een goed ontwerp van uw automatiseringsnetwerk te komen?

Prof. dr. ing. Johannes Cottyn

Coördinator XiaK-UGent - Projectleider TETRA Industriële Security

Ing. Tijn Deneut

Lector Howest – Projectmedewerker TETRA Industriële Security

KU LEUVEN


UNIVERSITEIT
GENT
CAMPUS KORTRUIK

howest
De Hogeschool West-Vlaanderen

Workshop - 15 maart 2016

Beheer van Security Kwetsbaarheden in Industriële Netwerken



FicTile company

Johannes Cottyn
Operations Manager

Tijl Deneut
IT Manager

KU LEUVEN


**UNIVERSITEIT
GENT**
CAMPUS KORTRIJK

howest
De Hogeschool West-Vlaanderen

Workshop - 15 maart 2016



Beheer van Security Kwetsbaarheden in Industriële Netwerken

“Remote monitoring mogelijk maken door de verschillende installaties te koppelen aan het bedrijfsnetwerk”

Johannes Cottyn
Operations Manager

KU LEUVEN

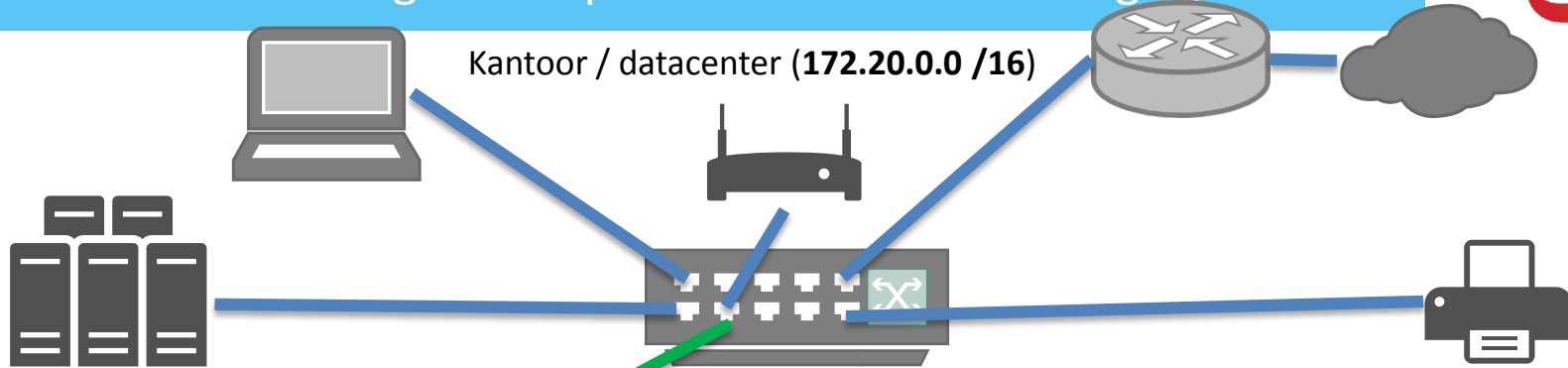

UNIVERSITEIT
GENT
CAMPUS KORTRIJK

howest
De Hogeschool West-Vlaanderen

Workshop - 15 maart 2016



Remote monitoring van de productie installaties mogelijk maken



Persinstallaties
172.20.1.0 /16

Ovenstraat
172.20.2.0 /16

Doseerinstallaties
172.20.3.0 /16
Vulinstallatie 1

Workshop - 15 maart 2016

Beheer van Security Kwetsbaarheden in Industriële Netwerken



“PLC van de doseerinstallatie gaat voortdurend in stop mode”



Tijl Deneut
IT Manager



KU LEUVEN

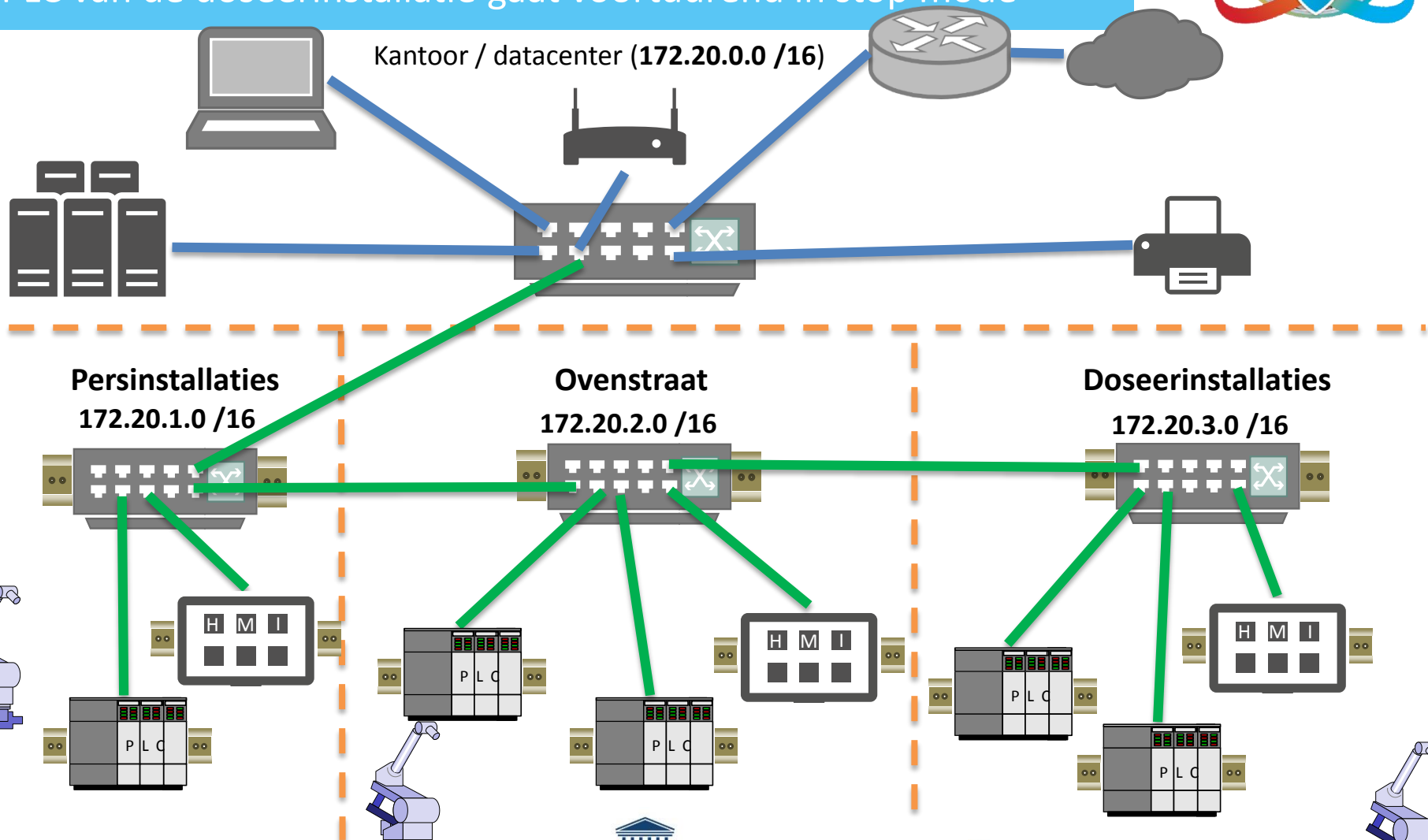

**UNIVERSITEIT
GENT**
CAMPUS KORTRIJK

howest
De Hogeschool West-Vlaanderen

Workshop - 15 maart 2016



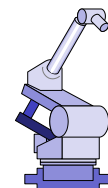
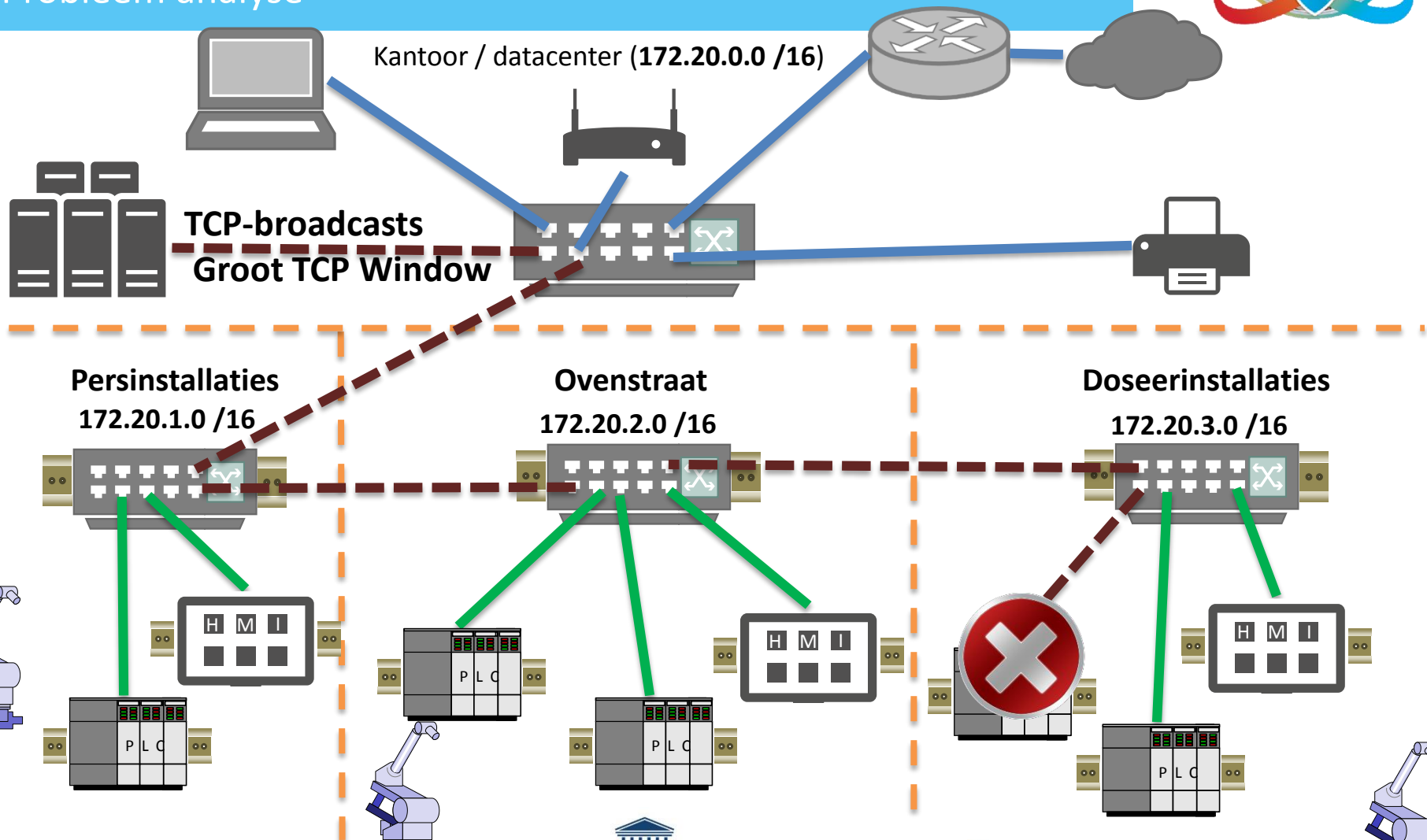
PLC van de doseerinstallatie gaat voortdurend in stop mode



Workshop - 15 maart 2016



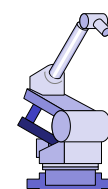
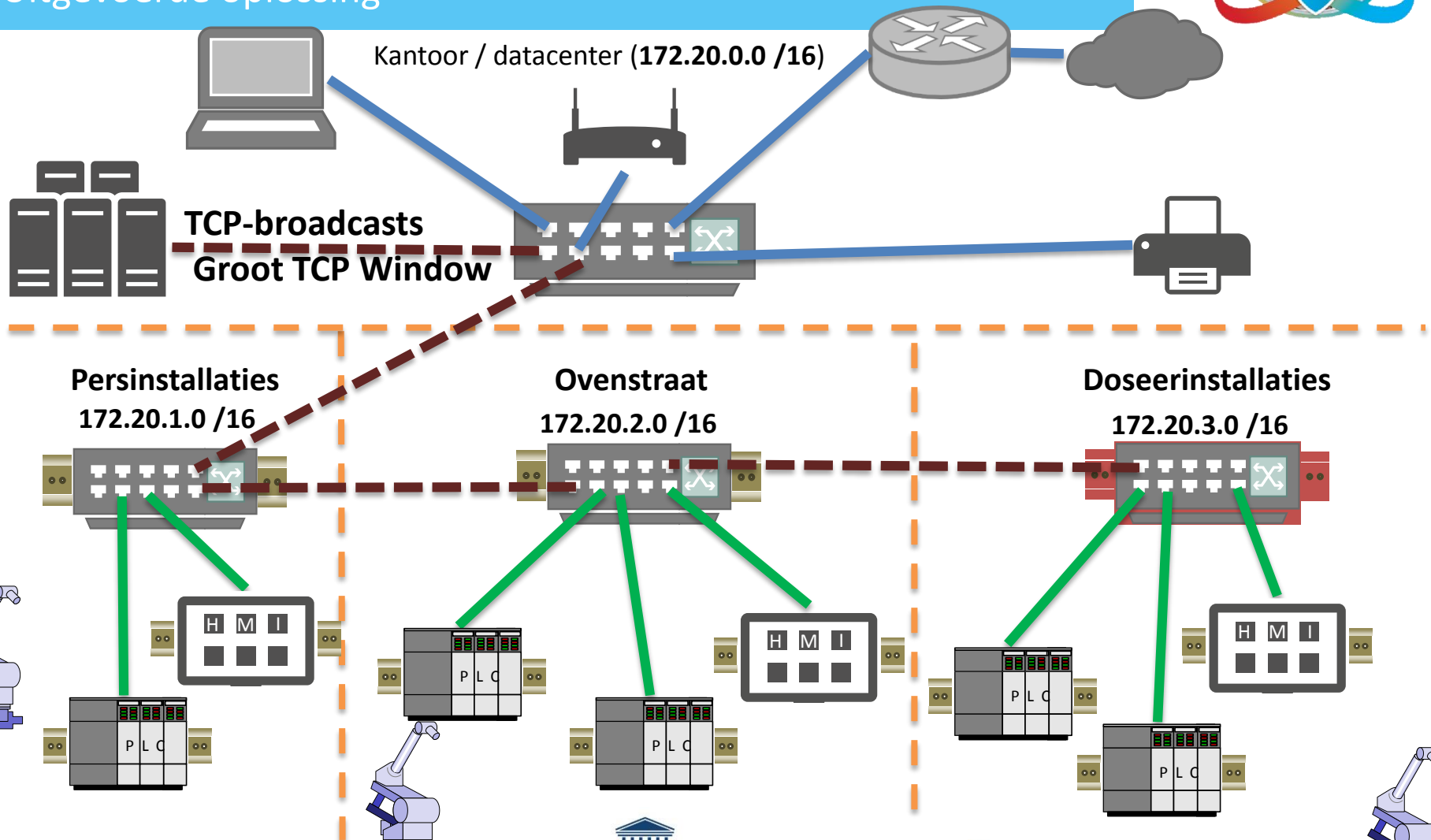
Probleem analyse



Workshop - 15 maart 2016



Uitgevoerde oplossing



Workshop - 15 maart 2016

Beheer van Security Kwetsbaarheden in Industriële Netwerken



“Doseerinstallatie gaat onverklaarbaar in de fout en kan niet meer herstart worden”



Tijl Deneut
IT Manager



KU LEUVEN

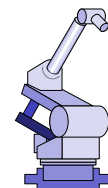
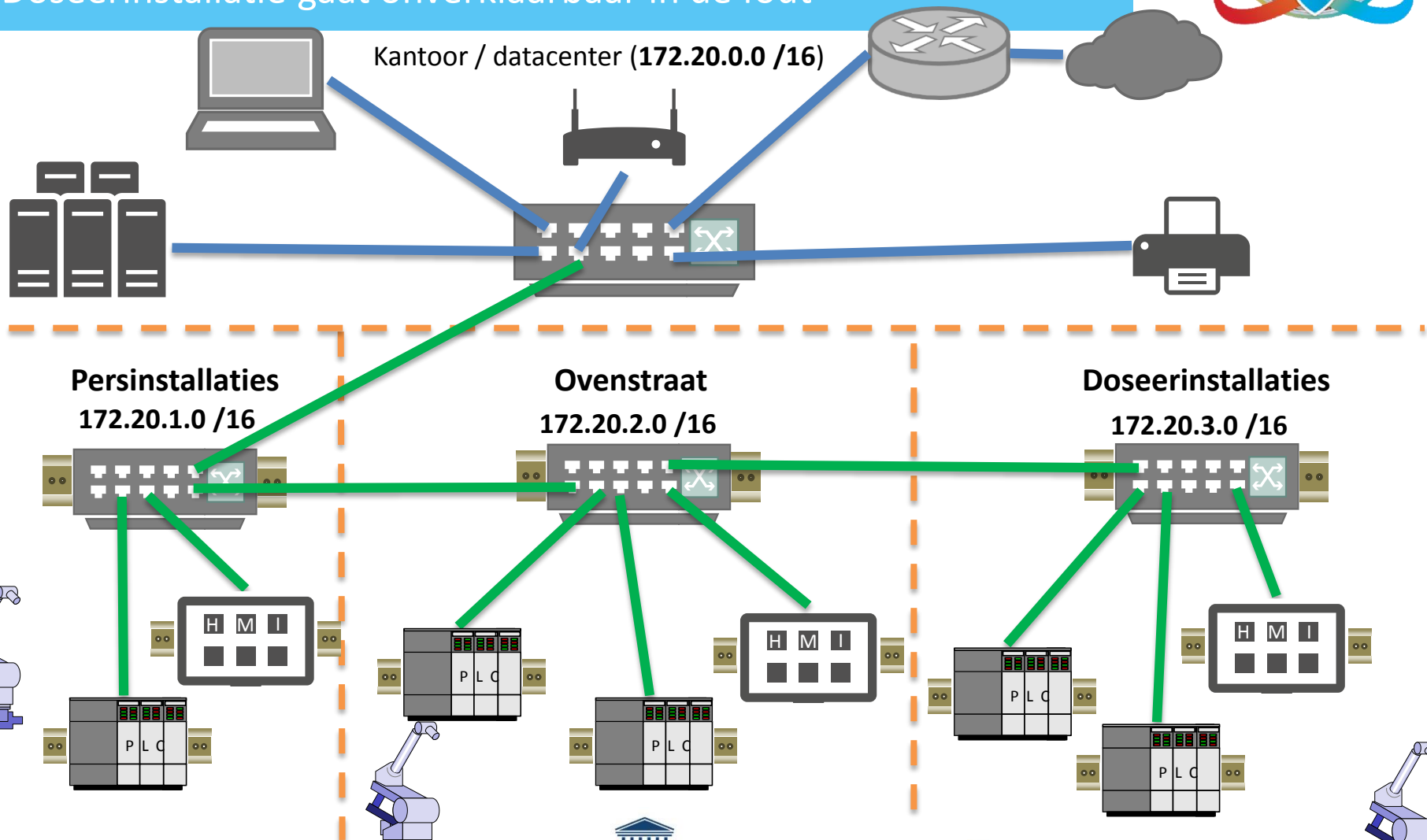

**UNIVERSITEIT
GENT**
CAMPUS KORTRIJK

howest
De Hogeschool West-Vlaanderen

Workshop - 15 maart 2016



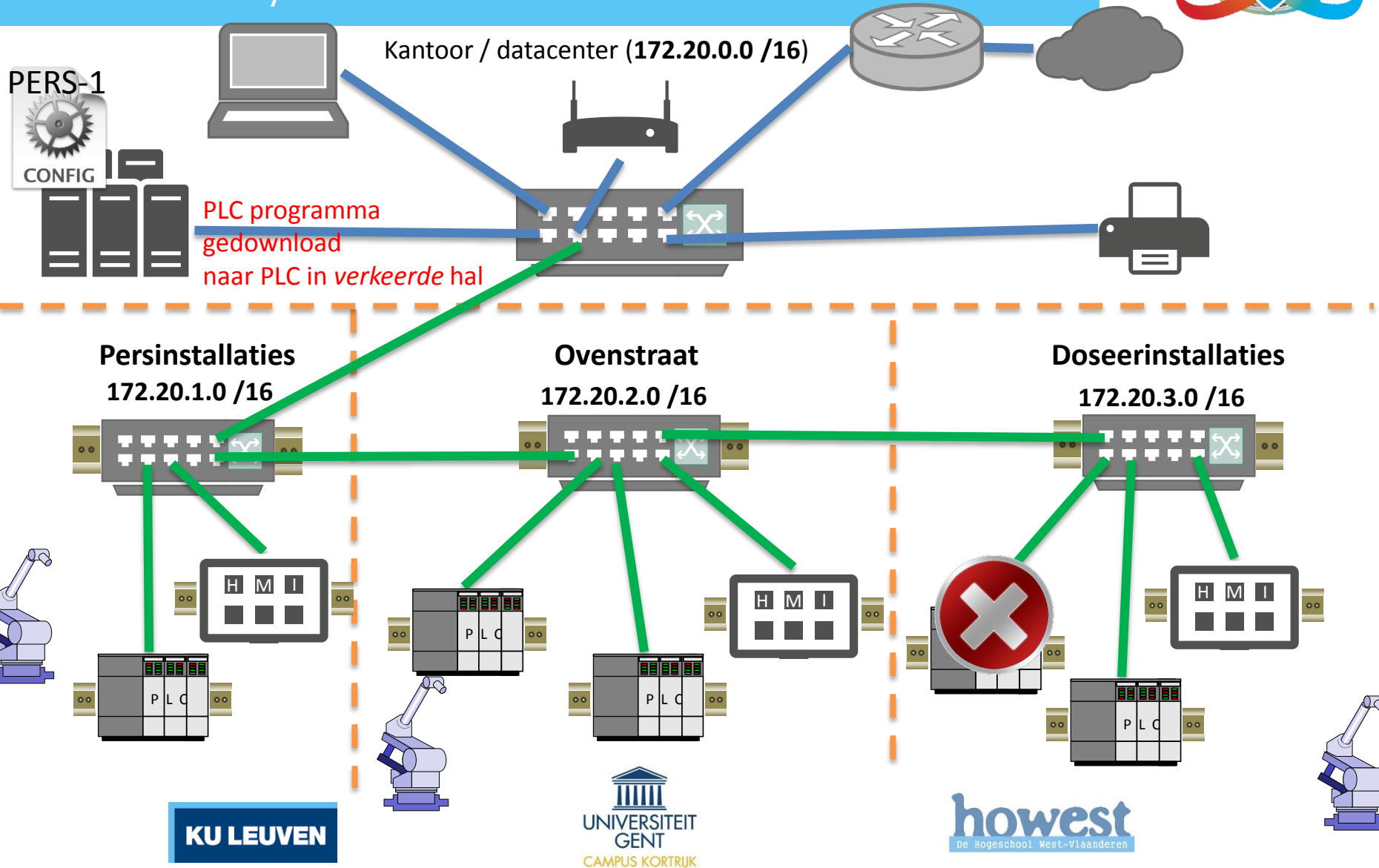
Doseerinstallatie gaat onverklaarbaar in de fout



Workshop - 15 maart 2016



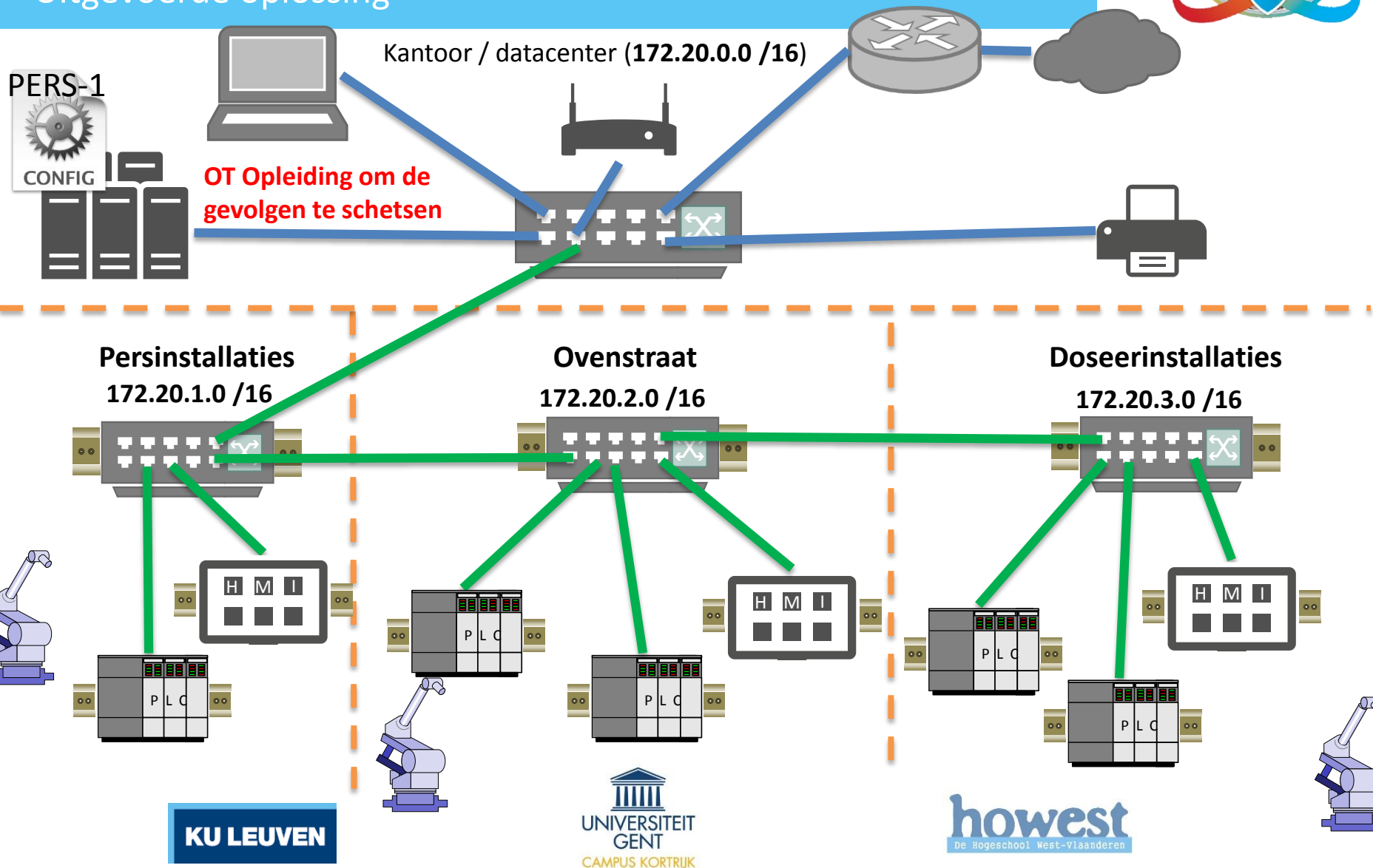
Probleem analyse



Workshop - 15 maart 2016



Uitgevoerde oplossing



Workshop - 15 maart 2016

Beheer van Security Kwetsbaarheden in Industriële Netwerken



“USB stick legt volledige productie stil”



Tijl Deneut
IT Manager

KU LEUVEN

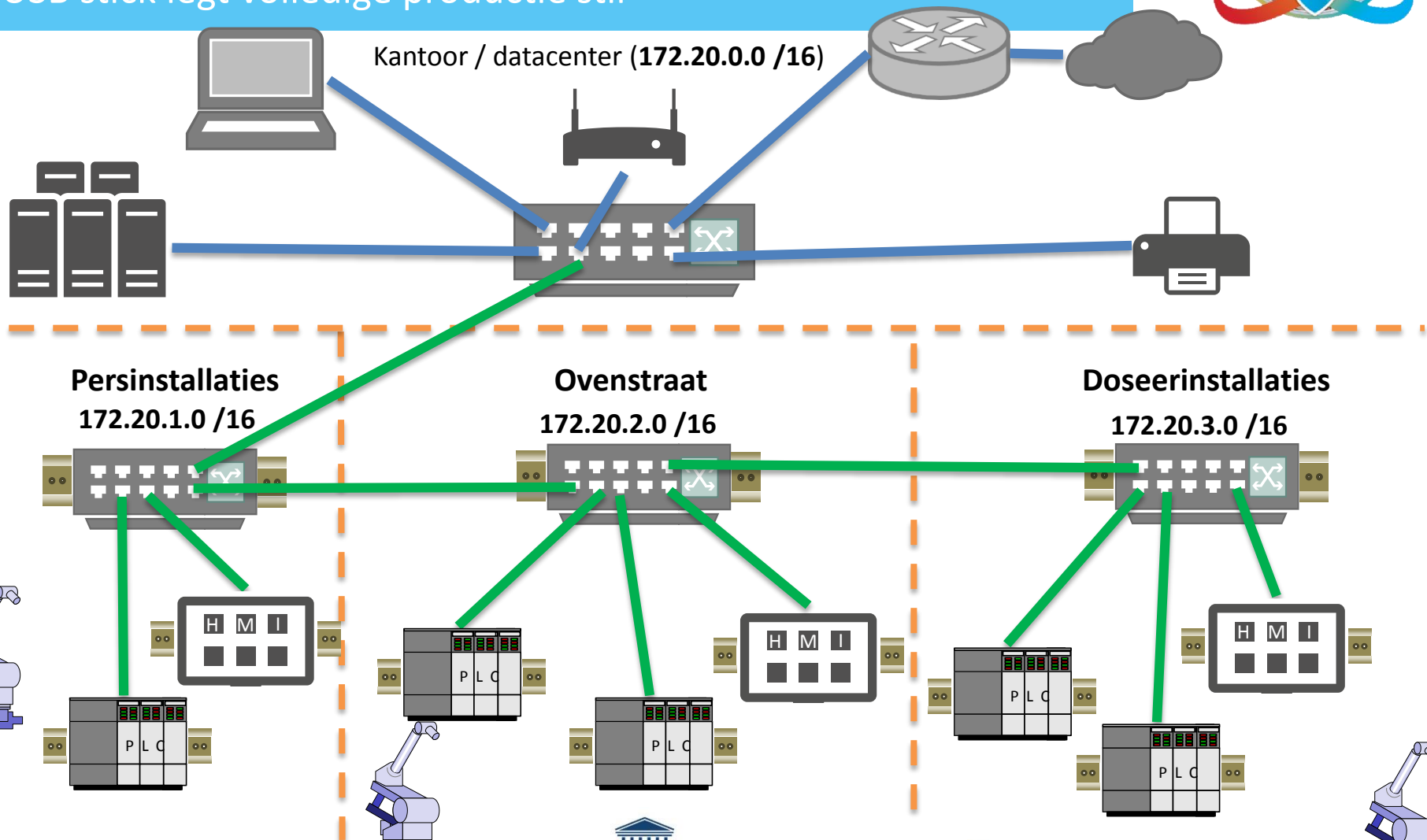

**UNIVERSITEIT
GENT**
CAMPUS KORTRIJK

howest
De Hogeschool West-Vlaanderen

Workshop - 15 maart 2016



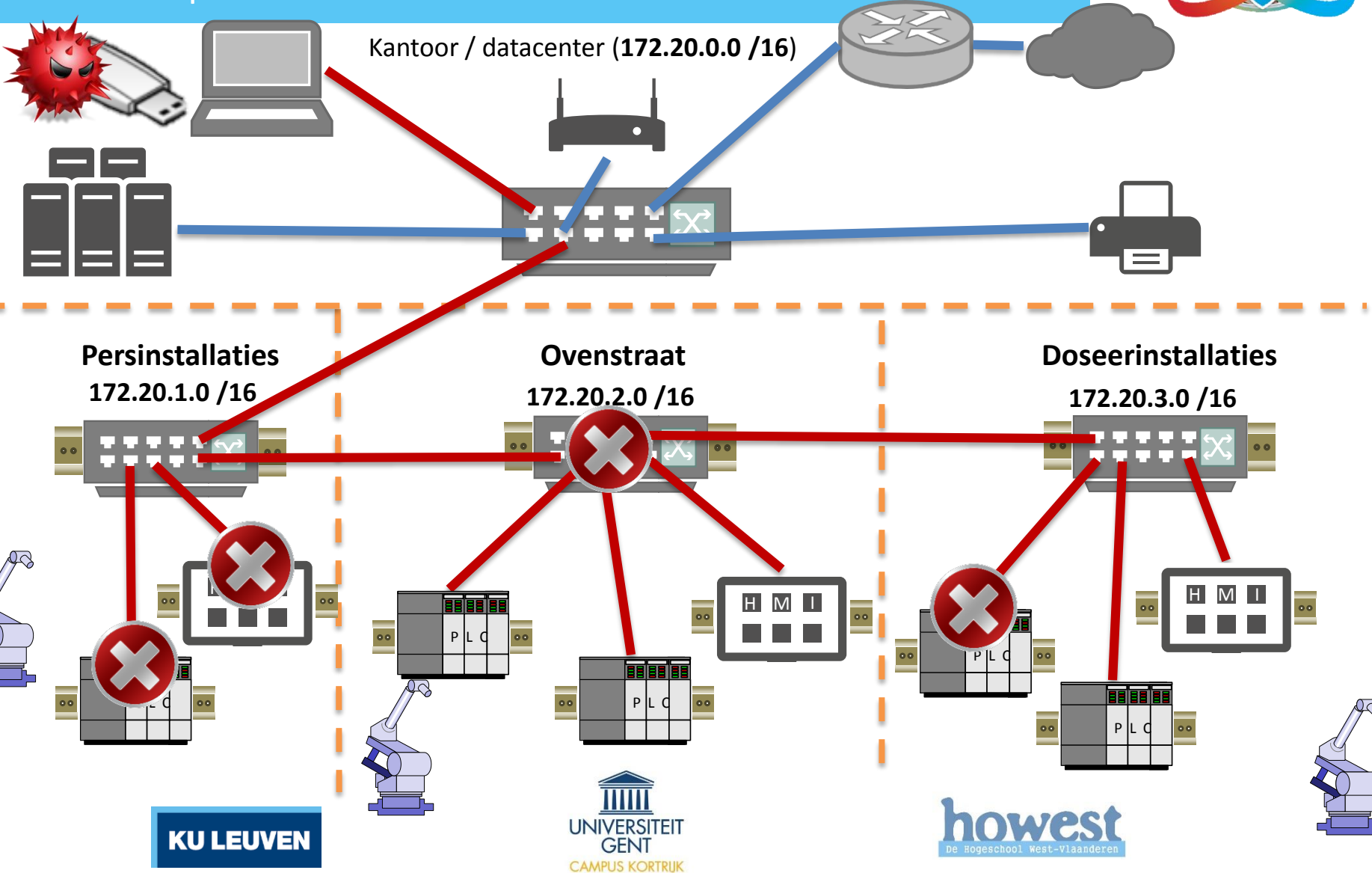
USB stick legt volledige productie stil



Workshop - 15 maart 2016



Malware op de stick veroorzaakt uitval

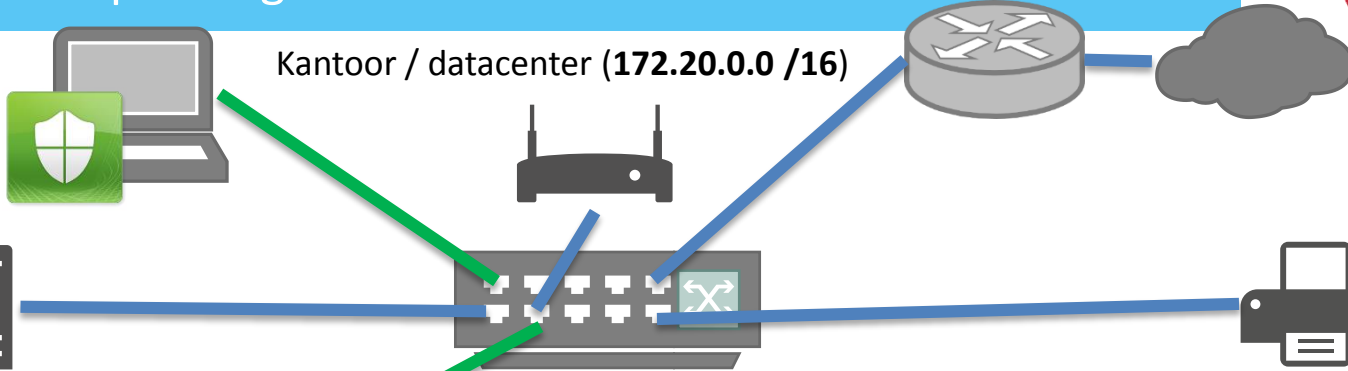


Workshop - 15 maart 2016



Uitgevoerde oplossing

Antivirus
installatie

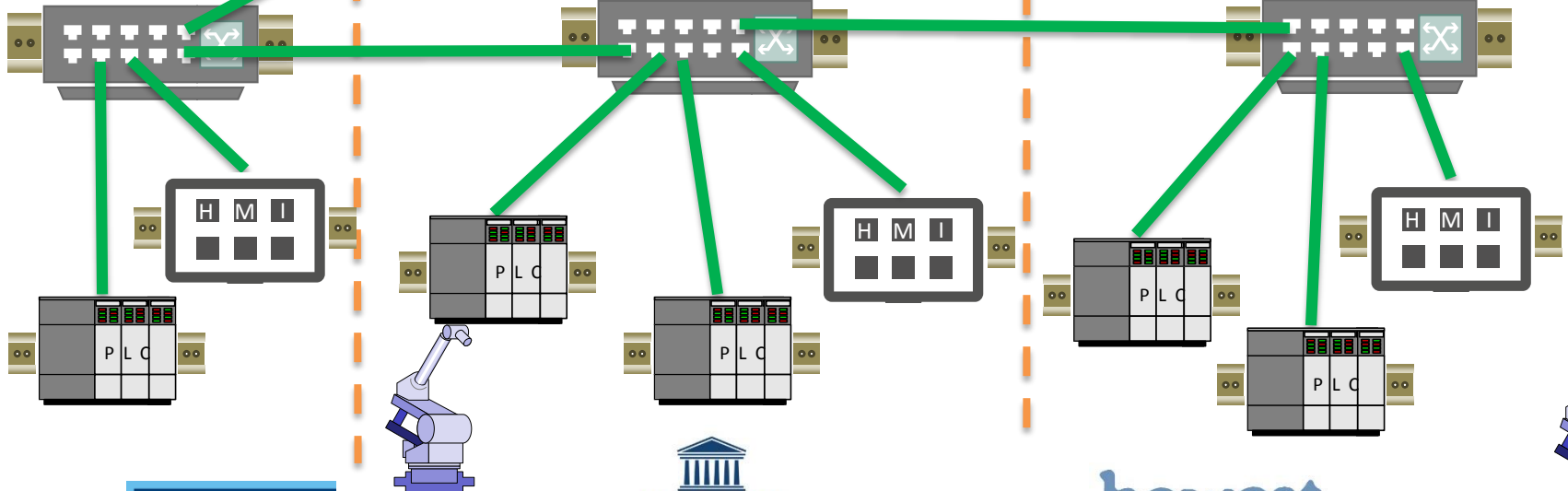


Kantoor / datacenter (172.20.0.0 /16)

Persinstallaties
172.20.1.0 /16

Ovenstraat
172.20.2.0 /16

Doseerinstallaties
172.20.3.0 /16



KU LEUVEN

UNIVERSITEIT
GENT
CAMPUS KORTRIJK

howest
De Hogeschool West-Vlaanderen



Het zogenaamde “platte” netwerk

- D.w.z. één “broadcast” domain
- De verschillen in IP adressen zijn puur op papier
- Elk toestel heeft een rechtstreekse verbinding met elk ander toestel
- Geen mogelijkheid tot afzondering van zones of gebieden
- Geen controle op het verkeer

⇒ een onveilig netwerk!

- Niet **safe**: misconfiguraties of fouten hebben invloed op het volledige netwerk
- Niet **secure**: ongeoorloofde toegang is niet beheersbaar



Remote monitoring van de productie installaties mogelijk maken

Oplossing: netwerksegmentatie

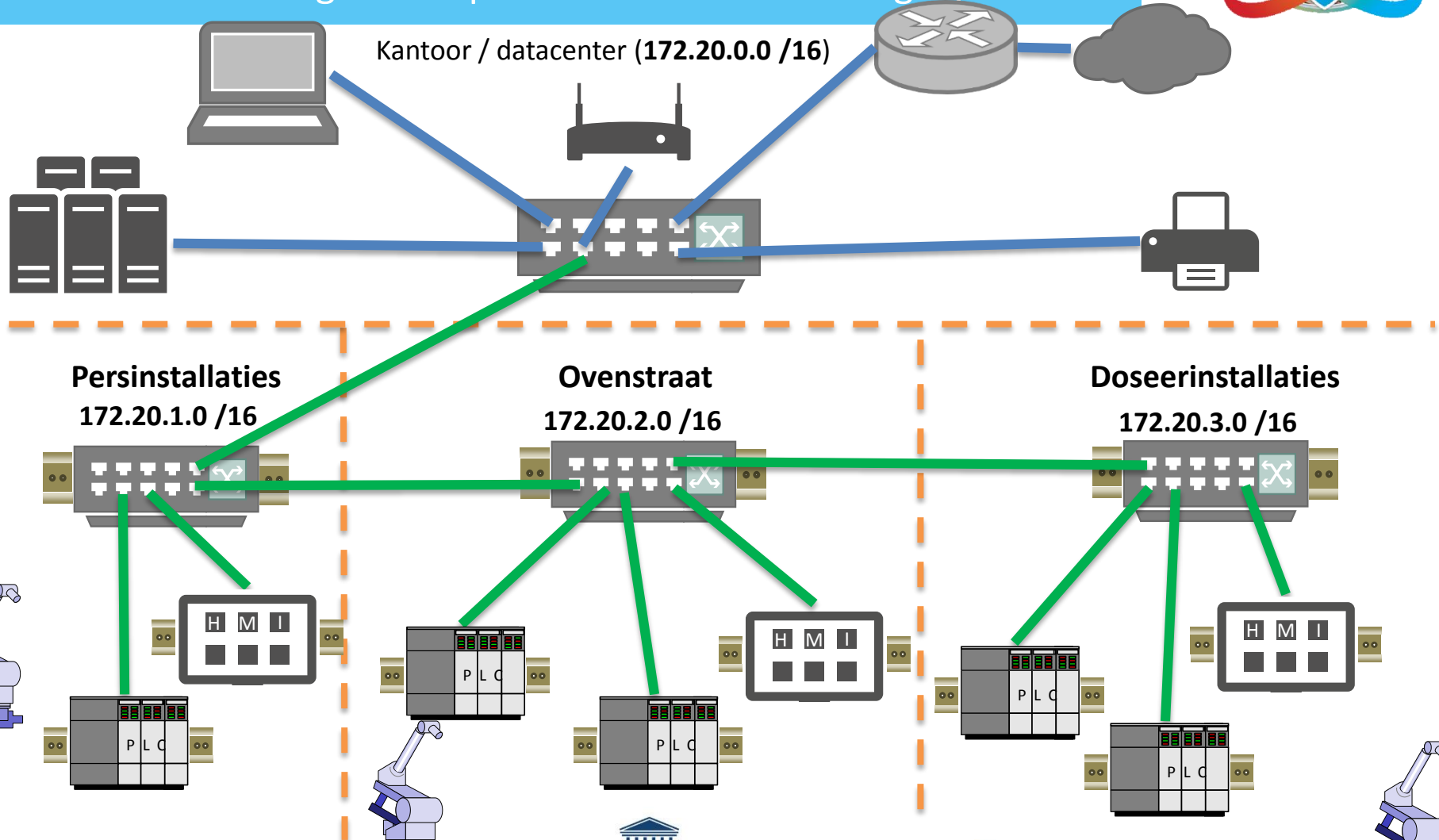
Optie 1 Routers inschakelen voor elke hal of zelfs machine

- Doorlaten/blokkeren verkeer configureerbaar per router
- Broadcast verkeer stopt aan de router
- Vrij duur, afhankelijk van grootte van netwerk (zéker industriële routers)
- Eventueel extra bekabeling, afhankelijk van infrastructuur
- Bij migratie moet elk toestel afzonderlijk aangepast te worden

Workshop - 15 maart 2016



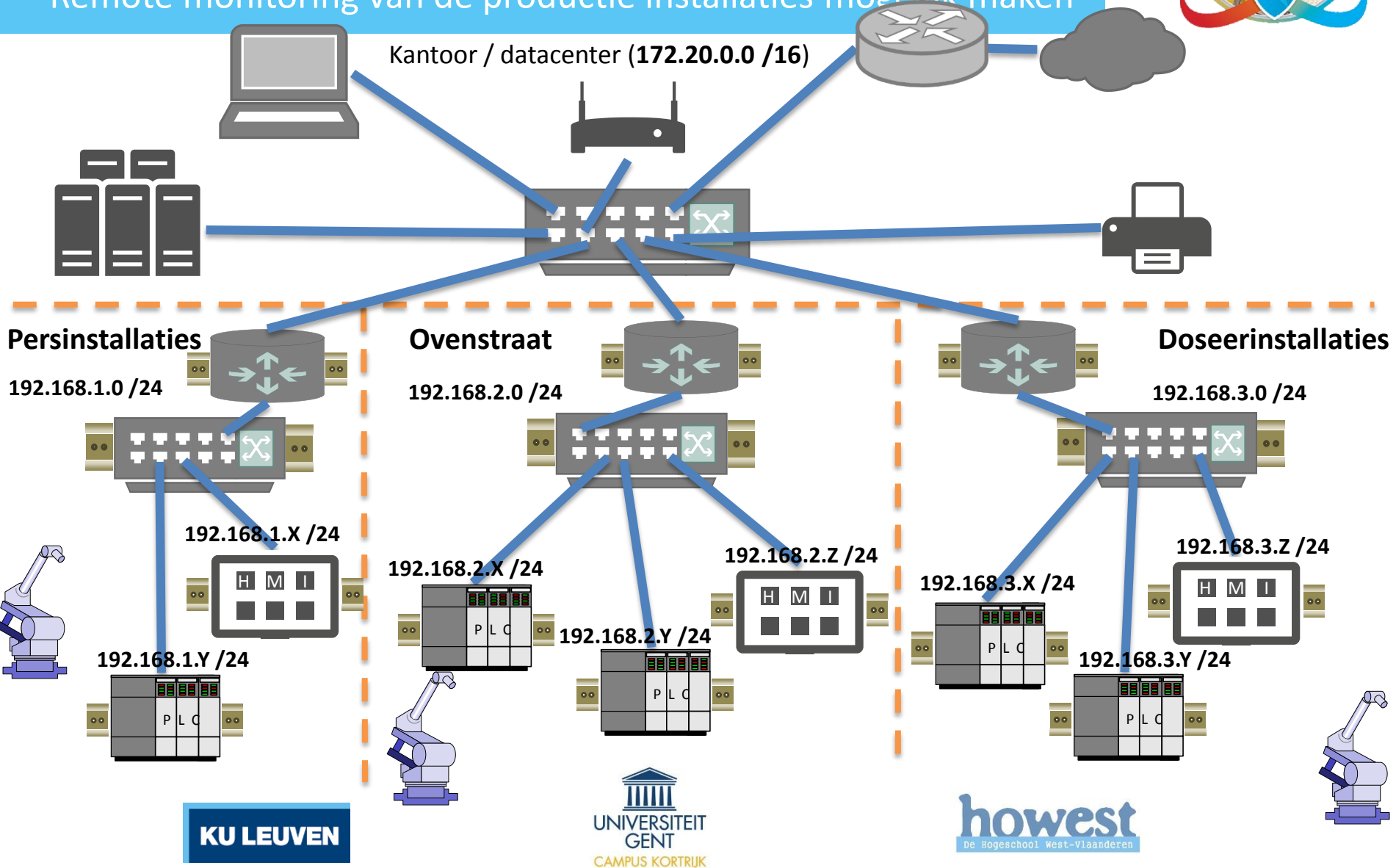
Remote monitoring van de productie installaties mogelijk maken



Workshop - 15 maart 2016



Remote monitoring van de productie installaties mogelijk maken





Remote monitoring van de productie installaties mogelijk maken

Oplossing: netwerksegmentatie

Optie 2 Gebruik maken van VLANs

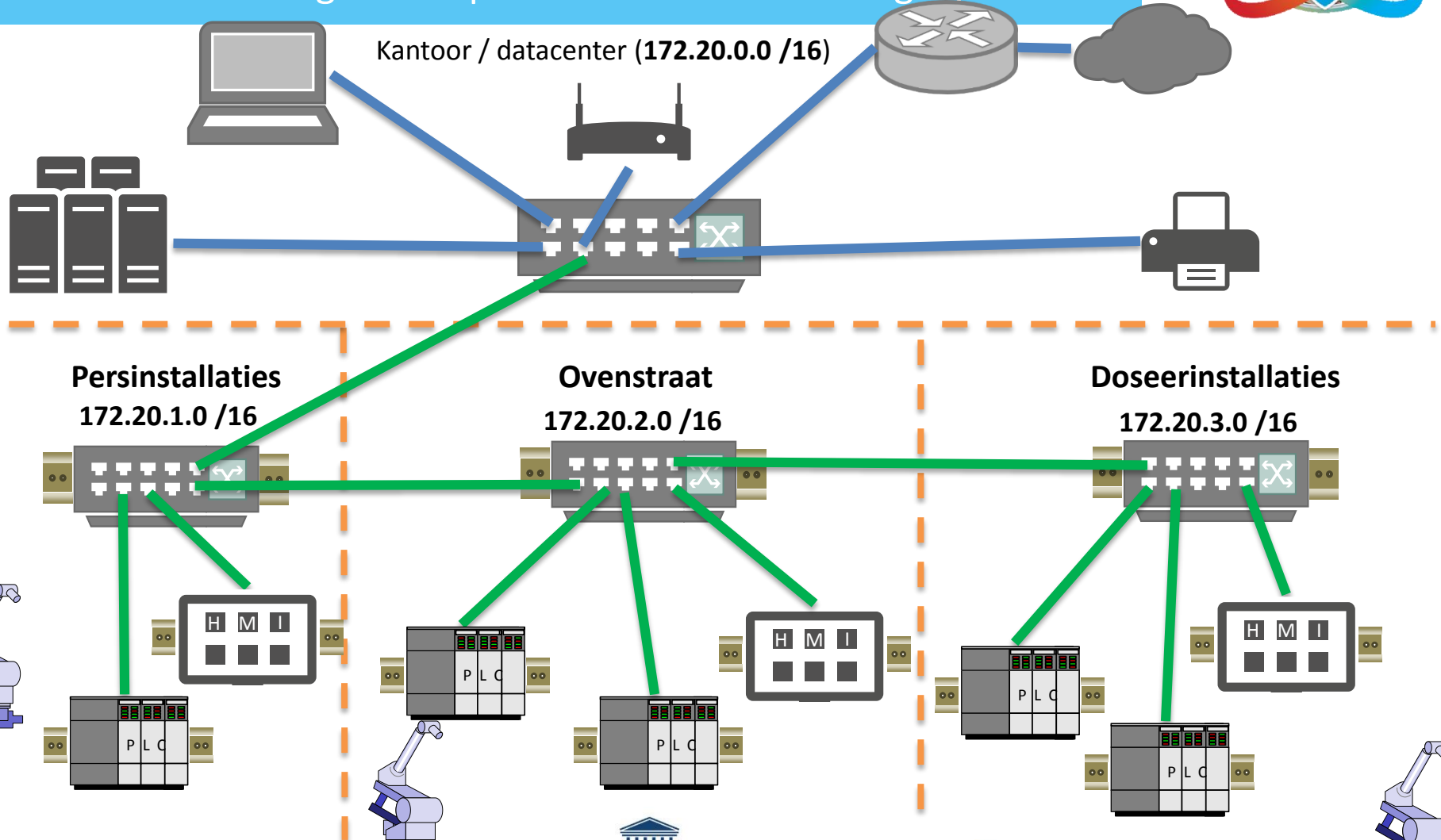
(Fysieke onderverdeling op switch niveau)

- Doorlaten/blokkeren verkeer configureerbaar op één plaats
- Broadcast verkeer beperkt tot VLAN
- Switches moeten dit ondersteunen (managed switches)
- Moet op voorhand doordacht worden, eventueel wel snm wijzigen

Workshop - 15 maart 2016



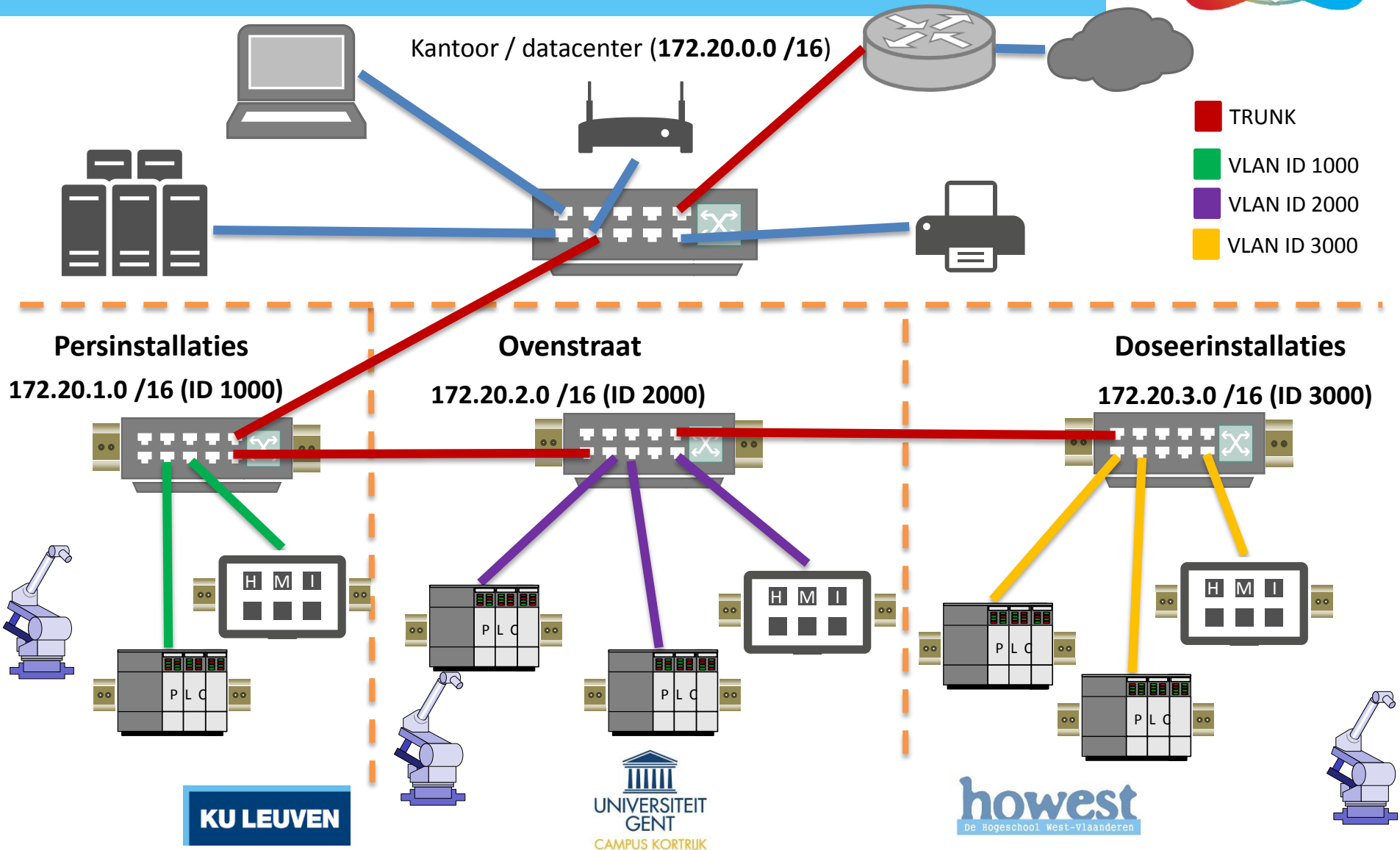
Remote monitoring van de productie installaties mogelijk maken



Workshop - 15 maart 2016



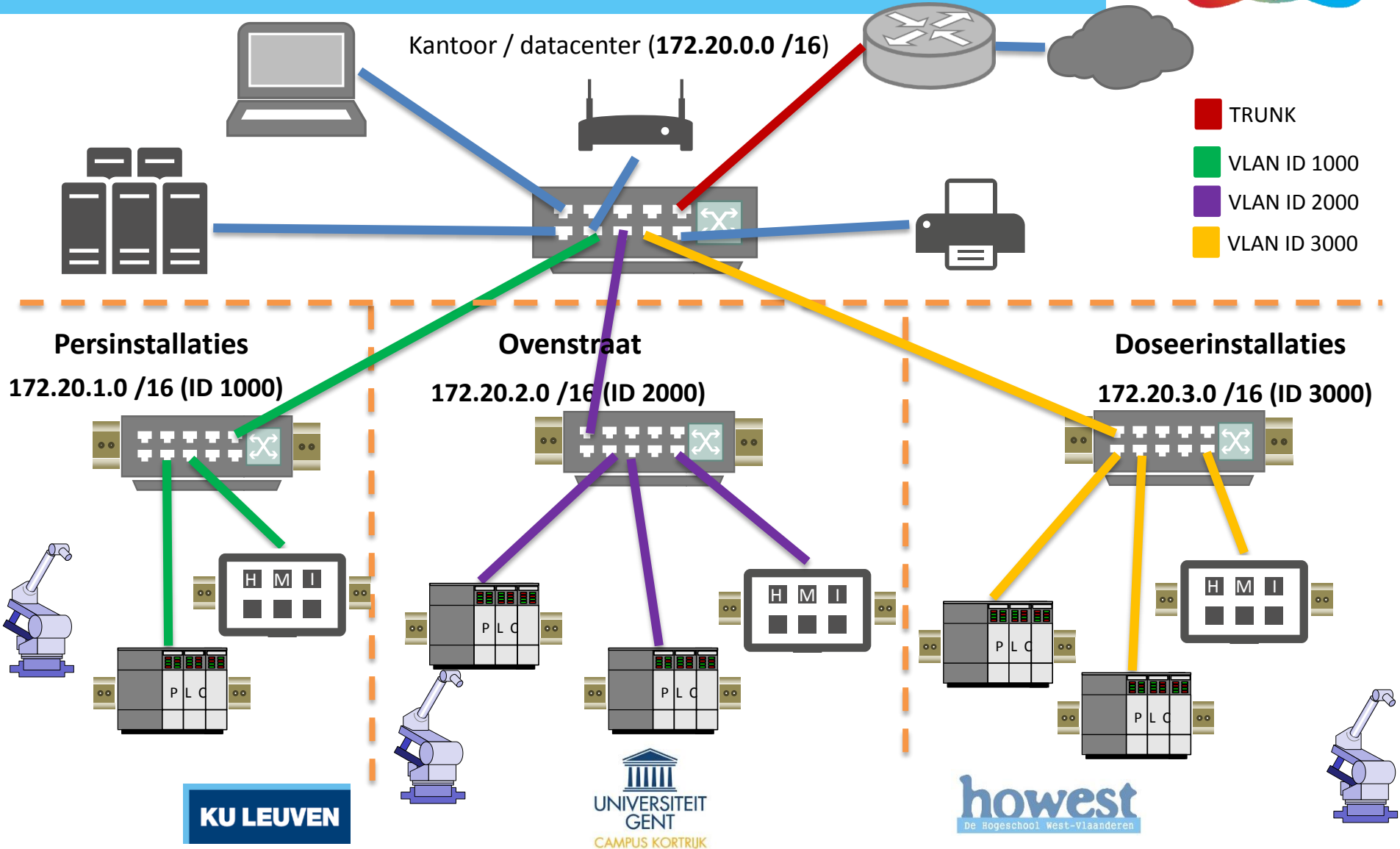
Remote monitoring van de productie installaties mogelijk maken



Workshop - 15 maart 2016



Remote monitoring van de productie installaties mogelijk maken



Workshop - 15 maart 2016



Beheer van Security Kwetsbaarheden in Industriële Netwerken

“Remote monitoring werkt niet meer”



Tijl Deneut
IT Manager

KU LEUVEN

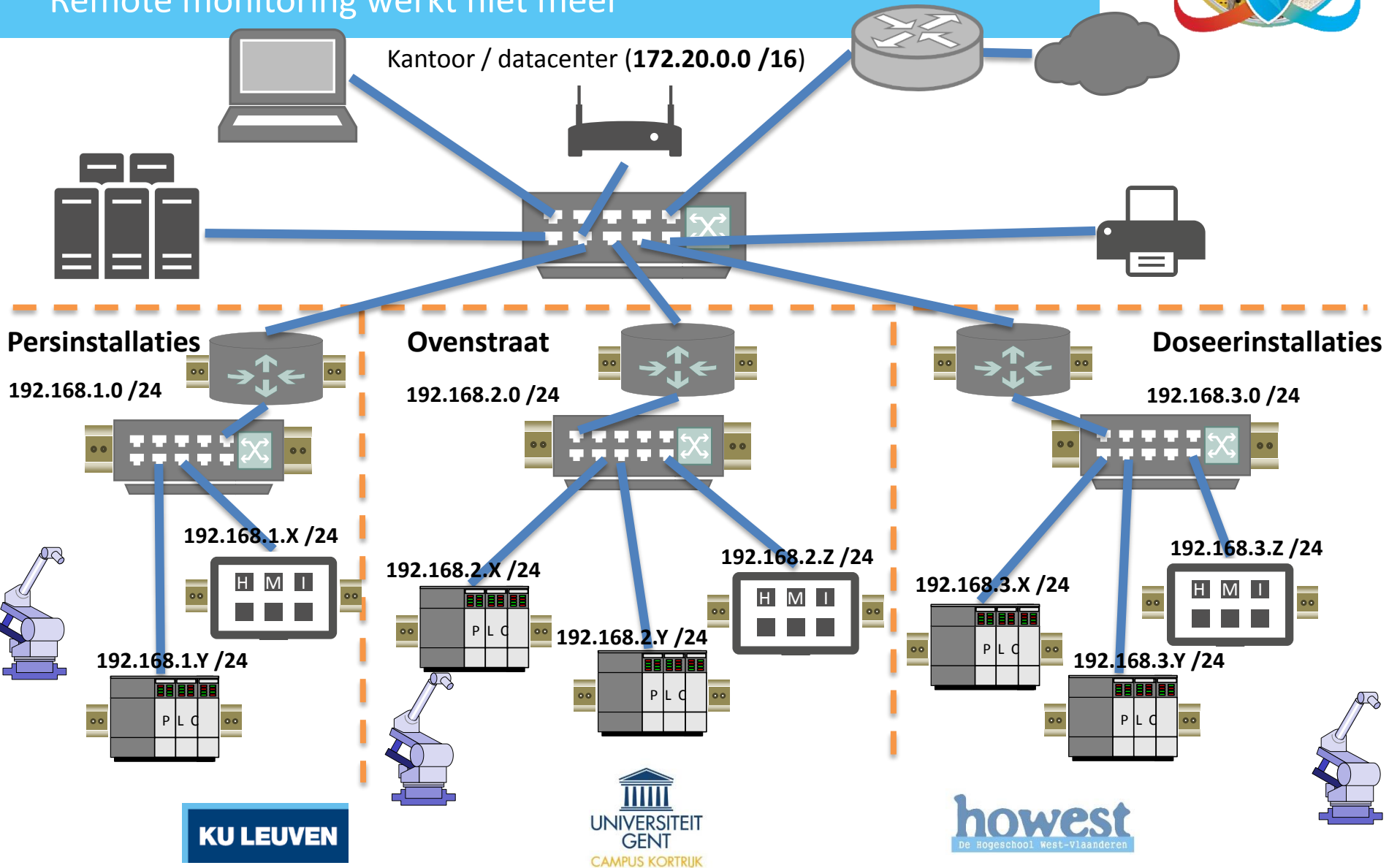

**UNIVERSITEIT
GENT**
CAMPUS KORTRIJK

howest
De Hogeschool West-Vlaanderen

Workshop - 15 maart 2016



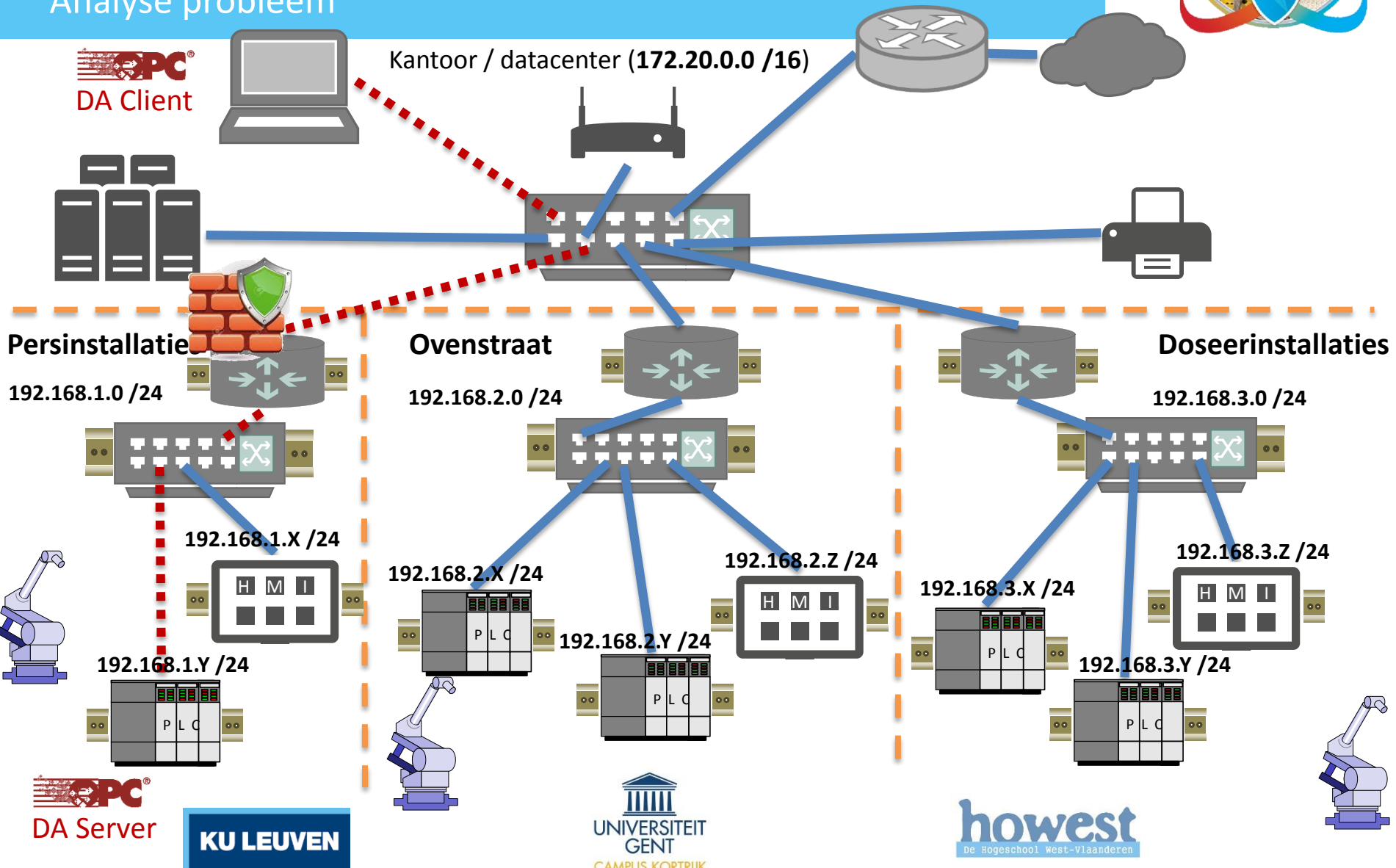
Remote monitoring werkt niet meer



Workshop - 15 maart 2016



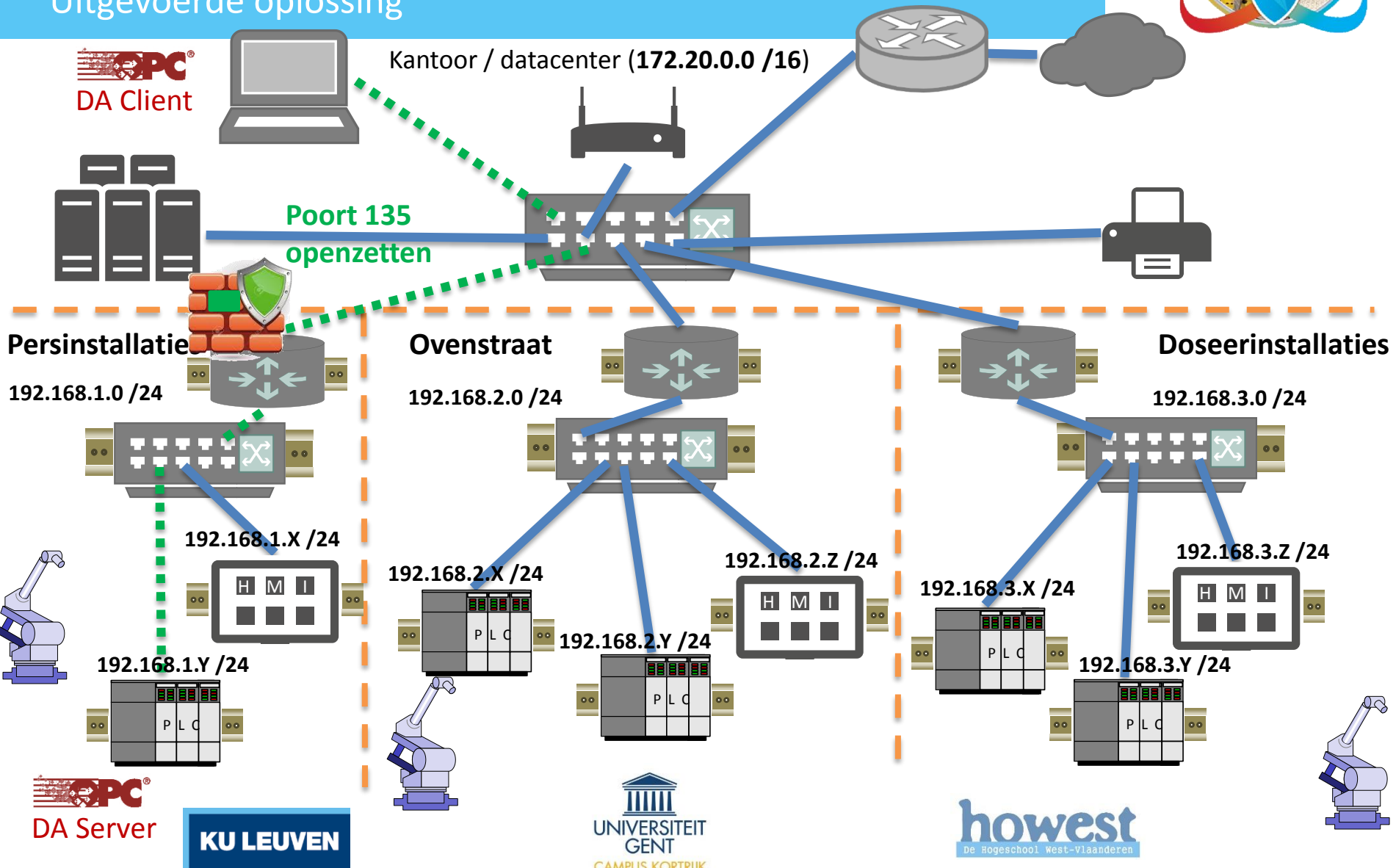
Analyse probleem



Workshop - 15 maart 2016



Uitgevoerde oplossing



Workshop - 15 maart 2016

Beheer van Security Kwetsbaarheden in Industriële Netwerken



“Hacker dreigt met blootstellen van
confidentiële recepturen”



Tijl Deneut
IT Manager

KU LEUVEN

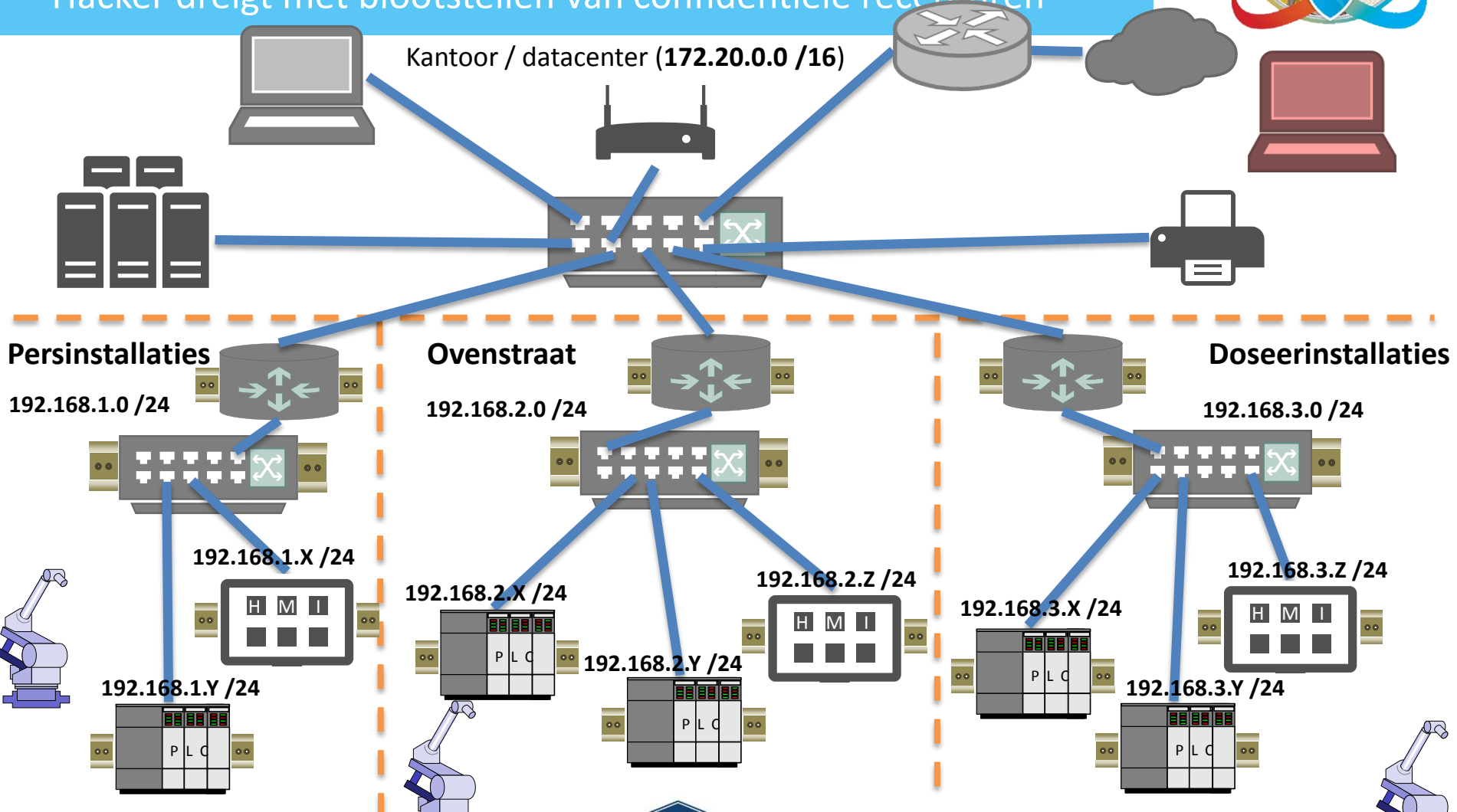

**UNIVERSITEIT
GENT**
CAMPUS KORTRIJK

howest
De Hogeschool West-Vlaanderen

Workshop - 15 maart 2016



Hacker dreigt met blootstellen van confidentiële recepturen





Conclusies

- ✓ Wacht niet op problemen, maar anticipeer zo veel mogelijk

Reactieve -> **Preventieve aanpak**

- ✓ Monitor het eigen netwerk continu
 - Checklist bij aanpassingen (technologie/component)
 - Scan/test uw eigen netwerk
 - Audit systeem

=> **Doelstelling TETRA project**

Workshop - 15 maart 2016



Vragen?



Johannes Cottyn

Johannes.Cottyn@ugent.be

Tijl Deneut

Tijl.Deneut@howest.be

T: 056 241 221

www.XiaK.be

