IN dustrial security

Projectsamenvatting

Ing. Tijl Deneut
Researcher XiaK, Ghent University
Lecturer Applied Computer Sciences Howest

UNIVERSITEIT GENT
CAMPUS KORTRIJK

howest
De Hogeschool West-Vlaanderen

KU LEUVEN

XiaK

Tijl Deneut

- Researcher / Ethical Hacker
- Werknemer UGent / XiaK
- Lector Howest

UNIVERSITEIT GENT
CAMPUS KORTRIJK

howest
De Hogeschool West-Vlaanderen
Lid van de Associatie Universiteit Gent

KU LEUVEN

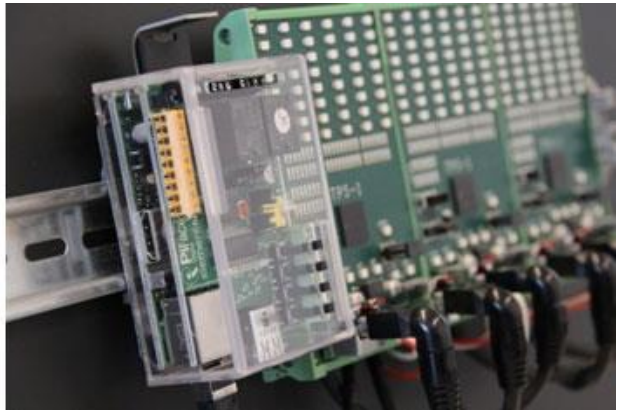
XiaK

Rol binnen het project

- Uitwerken gerichte aanvallen, beveiligingscontroles van bestaande en nieuwe systemen
- Zowel in dienstverlenings- als standalone verband
- Creëren en brengen van opleidingen & awareness sessies

Samenvatting kwetsbaarheden

- Siemens
  - S7-1200, S7-1500 PLC's, Scalance S615 Firewall, Switches …
  - Profinet, S7-Comm & Modbus protocollen
  - 4-tal "nieuwe" kwetsbaarheden (MSF published)
- Phoenix Contact
  - ETH150, ETH390 PLC's, IEC 61131 starterkit (Raspberry Pi) …
  - eCLR, Profinet & OPC-DA protocollen
  - 3-tal "nieuwe" kwetsbaarheden (exploit-db)
- Beckhoff (ook in exploit-db)
  - CX90xx PLC's, CP66xx HMI's, Windows CE
  - AMS, Twincat, UDP discovery protocollen
  - 3-tal "nieuwe" kwetsbaarheden (exploit-db)



Samenvatting opleidingen

- Basis TCP/IP dagcursus (3 sessies)
  - Hoe werkt een netwerk
- Basis VPN dag workshop (incl. hands-on)
  - Welke types VPN zijn er + workshop VPN opzetten
- Basis ICS Security dagcursus + workshop
  - Hoe ICS beveiligen + hoe ICS pentesten

Samenvatting dienstverlening

- N.D.A. stuff
- eWon, TeamViewer, Remote Desktop …
  - Zie later in deze presentatie
- Assistentie eindgebruikers
  - Zie later vandaag

Output

- Medewerking Brochure KU Leuven
  - “Hoe kwetsbaar is mijn industriële infrastructuur voor cyberaanvallers?”

- Publiek maken Online Checklist op **22 / 12 / 2016**
  - checklist.xiak.be (Benedikt Beun)

UNIVERSITEIT GENT CAMPUS KORTRIJK howest De Hogeschool West-Vlaanderen KU LEUVEN XIAK

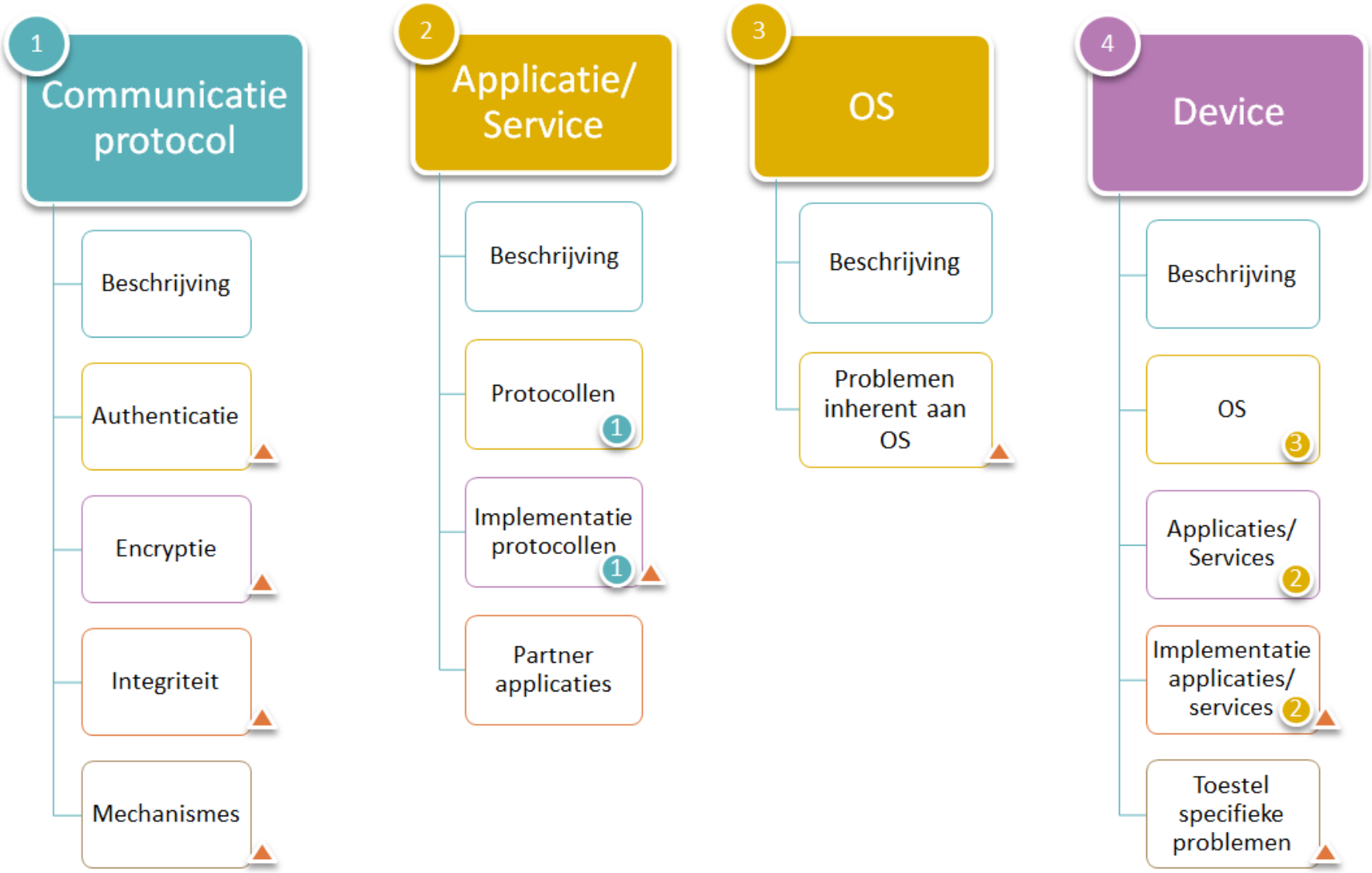
Checklist

- De Industrial Security XiaK Checklist is een online zoekpagina

- Bij bezoek kan ingevuld worden welke toestellen of toesteltypes aanwezig zijn in het bedrijf
  - Kan specifiek, bijv. ILC 150 of S7-1200
  - Of generiek, bijv. PLC of HMI

- Een lijst van gevonden toestellen wordt getoond, bij selectie worden meteen de security **aandachtspunten** getoond

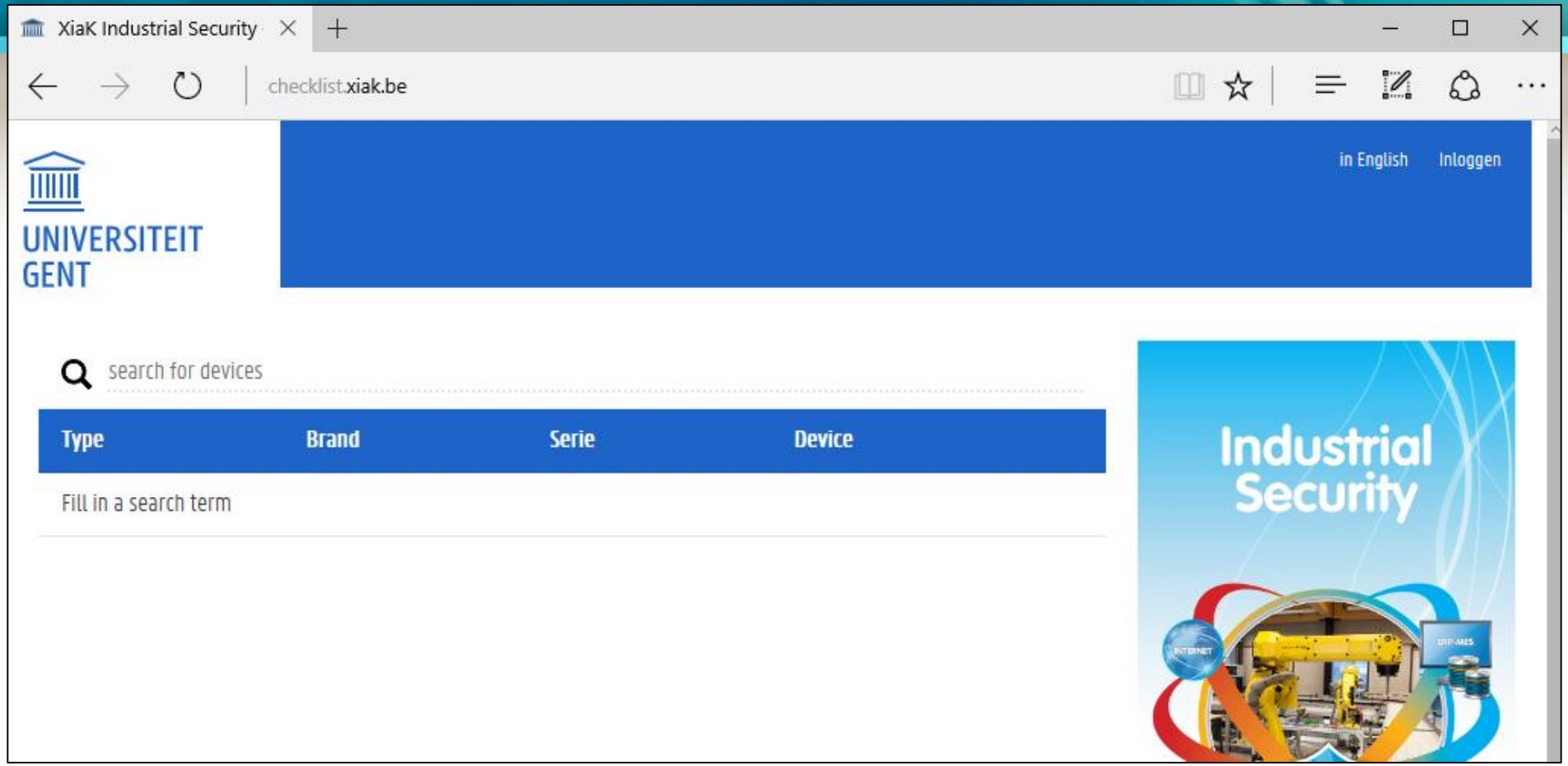
Checklist principeschema



Checklist Features (nu aanwezig)

- Toont kwetsbaarheden alsook oplossingen
- Onthoud de geselecteerde toestellen lokaal (cookies), verwijderen is ook mogelijk
- Zowel Nederlands als Engelstalig
- Mogelijkheid tot aanmaken account om selectie van toestellen te onthouden voor lange tijd

checklist.xiak.be



UNIVERSITEIT GENT
CAMPUS KORTRIJK

howest
De Hogeschool West-Vlaanderen

KU LEUVEN

XiaK

Hold On, eWon?

- Er is (een beetje) nieuws …
- Officiële en exclusieve verdelers (Bintz) werden op 14 Juni 2016 op de hoogte gebracht
- Alles werd toen bevestigd … (door Bintz)

Combineren …

- Dienstverlening
- Onderzoek
- Opleiding

} Draagbare Demonstratie Koffers

We present …

Het opzettelijk kwetsbare bedrijf

UNIVERSITEIT GENT
CAMPUS KORTRIJK

howest
De Hogeschool West-Vlaanderen

KU LEUVEN

XIAK

Staat van dienst

Reeds bij diverse bedrijven ter plaatse gedemonstreerd

Alsook diverse events:

- IOTBE.org, Brugge November 2015
- InfoSecurity, Brussel Juni 2016
- BruCon, Gent Oktober 2016
- eHackB, Brussel December 2016

UNIVERSITEIT GENT
CAMPUS KORTRIJK

howest
De Hogeschool West-Vlaanderen

KU LEUVEN

XiaK


DELL
intel
SOFTWARE
ENGINEERING

Toekomst?

Het werk is nog lang niet af:

- We breiden uit in de diepte, zoeken verder op oude en nieuwe toestellen en technologieën
  - PhoenixContact op Raspberry Pi, Beckhoff met Windows 7 Embedded, Siemens IOT2020 Gateway, …
  - OPC UA

- We breiden ook uit in de breedte:
  - Mitsubishi PLC is aangekomen
  - Schneider Electric PLC is aangekomen
  - Allen Bradley PLC is onderweg

Met de hulp van:

De Workshop Vandaag

Ga zélf aan de slag

- Voer zelf een ICS security audit uit.
- Begeleid aan de hand van een aantal zeer concrete challenges
- Er zijn geen grenzen: het netwerk is afgeschermd en alles heeft reserve kopieën
- Wij voorzien kant-en-klare laptops, reeds verbonden met het netwerk

- Tevens ter beschikking: Het ICS Pentesting Cheat Sheet!

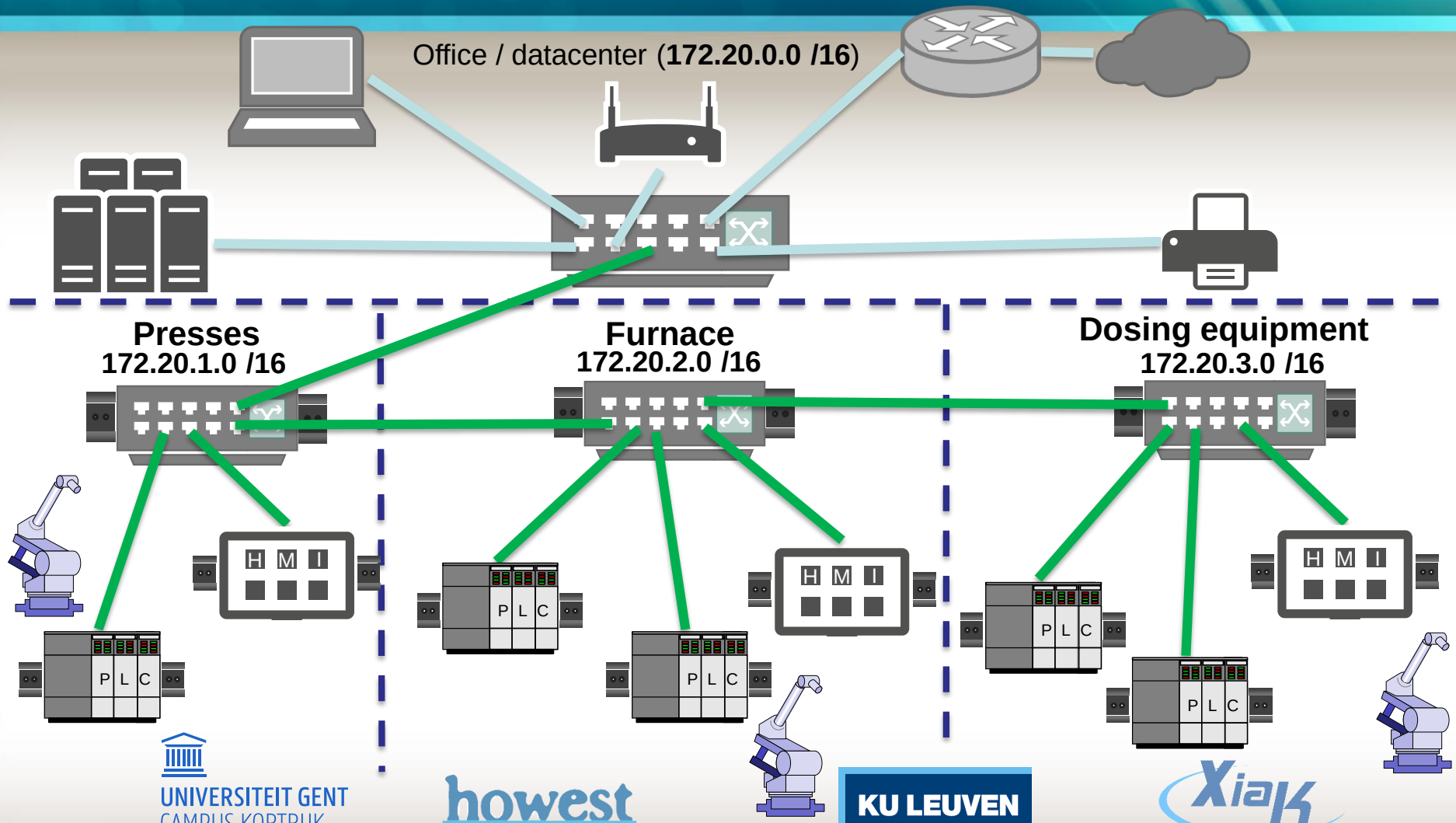
UNIVERSITEIT GENT
CAMPUS KORTRIJK

howest
De Hogeschool West-Vlaanderen

KU LEUVEN

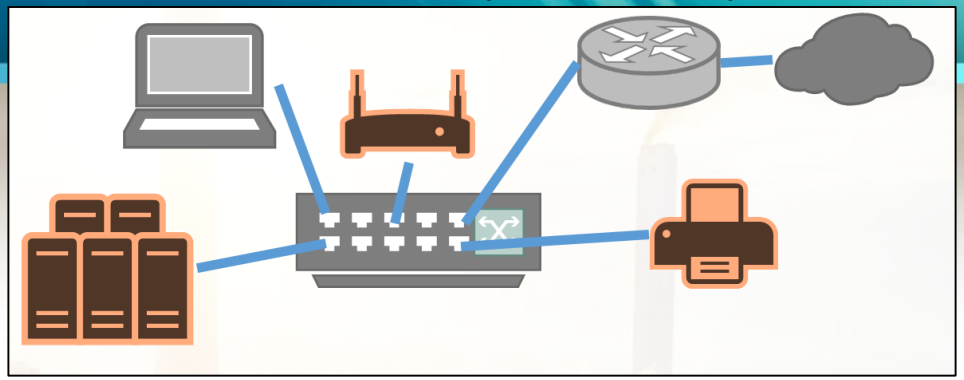
XiaK

Het Fictile Netwerk



Wat kan worden gehackt?

Office / datacenter (**172.20.0.0 /16**)



- Alles natuurlijk ☺

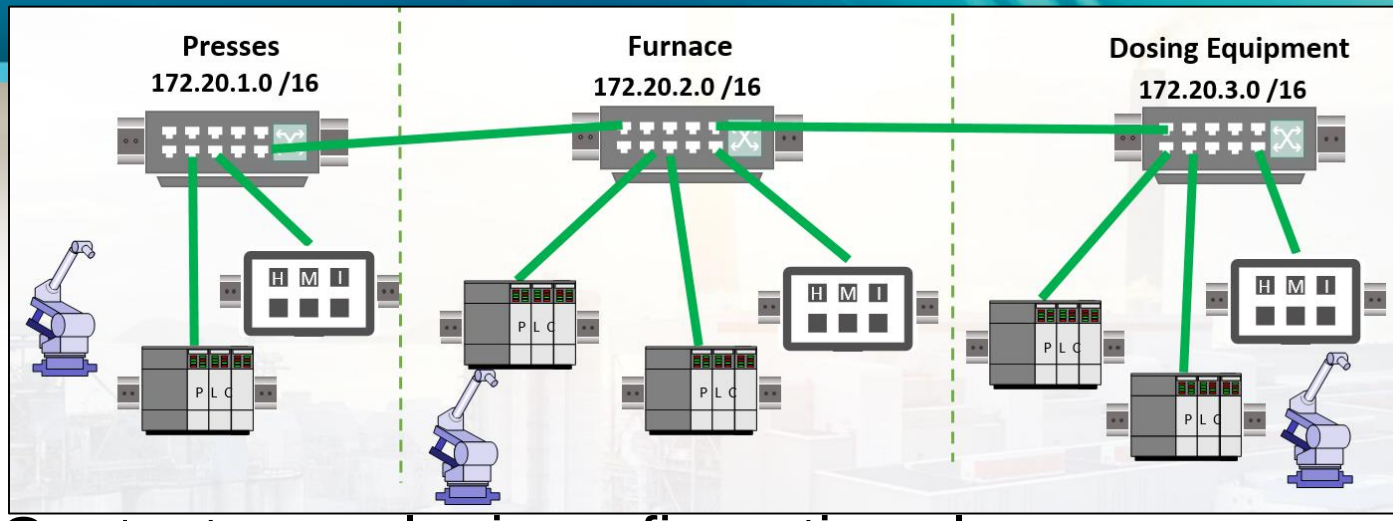
- Het domein (Windows omgeving) is kwetsbaar
  - Ga niet meteen voor de Domein Controller, al is dit wel het doel
  - Vind het zwakke element in tussen Windows machines

- Kan u een tekst printen op de netwerk printer? (1 regel)

- Er is ook een basis kwetsbaarheid op het WiFi AP…

En de ICS kant dan?

- Ook alles ☺



- Bij Phoenix Contact; zowel misconfiguraties als kwetsbaarheden
  - Soms zelfs geen scripts nodig
- Bij Beckhoff zitten er kwetsbaarheden bij PLC én HMI
  - Scripts zijn beschikbaar
- Siemens heeft de meest algemene configuratie

Tot slot: De FicTile Course (1dag)

Programma (onder voorbehoud)

TCP/IP, een introductie

Basisbegrippen, IP & MAC-adressen, hoe gebruiken (Wireshark)

Controle Systemen, een introductie

Protocollen, werkwijzen, hoe gebruiken (Programmeren) …

--- PAUZE ---

Pentesting, een introductie

Verschil tussen IT en OT pen testing, tips & tricks

De FicTile challenge, volledige hands-on

UNIVERSITEIT GENT
CAMPUS KORTRIJK

howest
De Hogeschool West-Vlaanderen

KU LEUVEN

XIAK

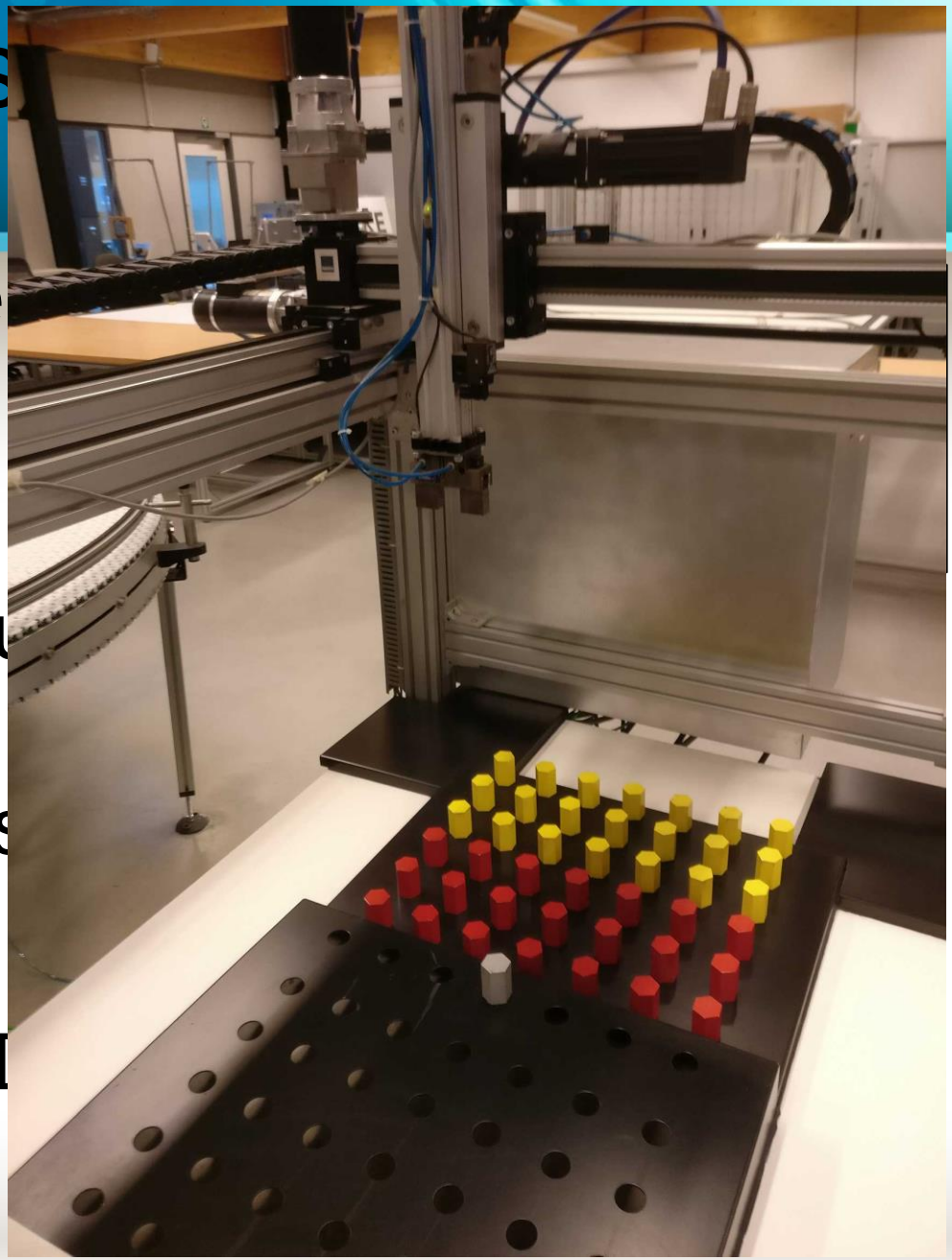
Voorjaar 2017: *IN*dustrial security Workshop

- Locatie: Labo XiaK, UGent Campus Kortrijk
- Het volledig FicTile demobedrijf staat paraat en wordt ingezet om aan de hand van scenario's een verhaal te brengen
- En dit in combinatie met virtueel elke opstelling in het labo aanwezig: robotten, opstellingen en games

UNIVERSITEIT GENT CAMPUS KORTRIJK howest De Hogeschool West-Vlaanderen KU LEUVEN XiaK

Slot demons

- Eén dergelijke opste
  De Vier-Op-Een-Rij
- Wordt in labo's gebru
  leren werken met en
  bovenop OPC (DA) s
- Na een kleine OPC-D



UNIVERSITEIT GENT
CAMPUS KORTRIJK

howest
De Hogeschool West-Vlaanderen
Lid van de Associatie Universiteit Gent