Introducing ...

1. Internationale dag
2. voor alle studenten
3. Contact
4. Internationale professionele wereld
5. Specifieke aspecten van een internationale carrière
6. Opleidingen en vakgebeiden in een internationaal licht
7. Industrie 4.0
Industrie 4.0, Industrial Internet, Smart Manufacturing indicate the level of Digitalisation of Manufacturing. Legacy and Smarter Devices are being connected to drive Operational Efficiency. Smarter production will allow Mass Customization.
The potential of I4.0

- 10-40% reduction of maintenance costs
- 3-5% increase of overall productivity
- 20-50% reduction in time to market
- Up to 85% increase of forecasting accuracy
- 10-20% reduction of costs for quality
- 20-50% reduction of inventory costs
- 30-50% reduction of total machine downtime
- 45-55% increase of productivity in technical professions

Source: German Innovation Center for I4.0, 2017

Industrie 4.0?

Physical

- Smart factory
  - Assets are equipped with sensors and integrated for greater transparency and planning capabilities
- Smart products
  - The product thinks for itself and remains in contact with the manufacturer even after it is sold

Digitization

- Smart operations
  - The smart factory enables flexible production planning and control
- Data-driven services
  - The integration of products, manufacturers, and customers opens up new markets for services

Business objectives

- Operational excellence
  - Enhanced efficiency through greater automation
  - Customized products at the cost of a mass-produced product
- Expanded service portfolio
  - Higher revenues from digitally refined products
  - Access to new markets

Virtual

Source: VDMA, Impuls, 2015 – Readiness
Industrie 4.0?

Source: VDMA, Impuls, 2015 – Readiness
... towards a Smart World
... towards a Smart World

Connectivity & sensing  Advanced analytics  Robotics & Automation  Process digitization

| Massive influx of data & connectivity of systems | Use of greater portion of data via Advanced Analytics and machine learning | Automation (or semi-automation) of major portions of value chain | Mobile tools for field-force and management support |

| 90% | 10\(^{15}\) | 50% | 250k x |
| Data in the world today has been created in the last two years | More computer operations per second than since the 1960s | Reduction in cost of robots since 1990 vs 80% increase in US labour costs | More RAM in iPhone 5 than in the Apollo 11 computer |

© 3IF.be, 2019, Private & Confidential, Closed User Group Distribution. p 15

Source: BI Intelligence, 2015

© 3IF.be, 2019, Private & Confidential, Closed User Group Distribution. p 16

Enterprise and Industrial IoT: a Future Identity Disruptor?

- Surveillance
- Lightning
- Plant Irrigation
- Doors – Access Control
- Heating
- Cooling
- Office Equipment
- Window Shields
- Smoke and other Sensors
- Projection Public Announce

IoT... manufacturing to lead, logistics early adopter

Top Industries With Investments In IoT Solutions

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturing</td>
<td>$160</td>
<td>$180</td>
<td>$200</td>
<td>$220</td>
<td>$240</td>
<td>$260</td>
</tr>
<tr>
<td>Transportation And Warehousing</td>
<td>$140</td>
<td>$160</td>
<td>$180</td>
<td>$200</td>
<td>$220</td>
<td>$240</td>
</tr>
<tr>
<td>Information</td>
<td>$120</td>
<td>$140</td>
<td>$160</td>
<td>$180</td>
<td>$200</td>
<td>$220</td>
</tr>
<tr>
<td>Wholesale Trade</td>
<td>$100</td>
<td>$120</td>
<td>$140</td>
<td>$160</td>
<td>$180</td>
<td>$200</td>
</tr>
<tr>
<td>Health Care And Social Assistance</td>
<td>$80</td>
<td>$100</td>
<td>$120</td>
<td>$140</td>
<td>$160</td>
<td>$180</td>
</tr>
<tr>
<td>Retail Trade</td>
<td>$60</td>
<td>$80</td>
<td>$100</td>
<td>$120</td>
<td>$140</td>
<td>$160</td>
</tr>
<tr>
<td>Finance and Insurance</td>
<td>$40</td>
<td>$60</td>
<td>$80</td>
<td>$100</td>
<td>$120</td>
<td>$140</td>
</tr>
<tr>
<td>Utilities</td>
<td>$20</td>
<td>$40</td>
<td>$60</td>
<td>$80</td>
<td>$100</td>
<td>$120</td>
</tr>
<tr>
<td>Mining</td>
<td>$0</td>
<td>$20</td>
<td>$40</td>
<td>$60</td>
<td>$80</td>
<td>$100</td>
</tr>
<tr>
<td>Real Estate And Rental And Leasing</td>
<td>$-20</td>
<td>$0</td>
<td>$20</td>
<td>$40</td>
<td>$60</td>
<td>$80</td>
</tr>
<tr>
<td>Construction</td>
<td>$-40</td>
<td>$0</td>
<td>$20</td>
<td>$40</td>
<td>$60</td>
<td>$80</td>
</tr>
<tr>
<td>Professional, Scientific, And Technical Services</td>
<td>-60</td>
<td>-40</td>
<td>-20</td>
<td>0</td>
<td>20</td>
<td>40</td>
</tr>
</tbody>
</table>

Source: BI Intelligence, 2015
Everything connected

Every Company is a digital company
5G and IoT are game changers

Public safety
Utilities
Shipping
Mining

29 billion devices (… and counting)

Connected devices (billions)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Wide-area IoT</td>
<td>0.4</td>
<td>0.5</td>
<td>0.6</td>
<td>0.7</td>
<td>0.8</td>
<td>0.9</td>
<td>1.0</td>
<td>1.1</td>
<td>1.2</td>
</tr>
<tr>
<td>Short-range IoT</td>
<td>5.2</td>
<td>5.3</td>
<td>5.4</td>
<td>5.5</td>
<td>5.6</td>
<td>5.7</td>
<td>5.8</td>
<td>5.9</td>
<td>6.0</td>
</tr>
<tr>
<td>PC/laptop/tablet</td>
<td>1.6</td>
<td>1.7</td>
<td>1.8</td>
<td>1.9</td>
<td>2.0</td>
<td>2.1</td>
<td>2.2</td>
<td>2.3</td>
<td>2.4</td>
</tr>
<tr>
<td>Mobile phones</td>
<td>7.3</td>
<td>7.4</td>
<td>7.5</td>
<td>7.6</td>
<td>7.7</td>
<td>7.8</td>
<td>7.9</td>
<td>8.0</td>
<td>8.1</td>
</tr>
<tr>
<td>Fixed phones</td>
<td>1.4</td>
<td>1.5</td>
<td>1.6</td>
<td>1.7</td>
<td>1.8</td>
<td>1.9</td>
<td>2.0</td>
<td>2.1</td>
<td>2.2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Year</th>
<th>2016</th>
<th>2017</th>
<th>2018</th>
<th>2019</th>
<th>2020</th>
<th>2021</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 billion</td>
<td>0.4</td>
<td>0.5</td>
<td>0.6</td>
<td>0.7</td>
<td>0.8</td>
<td>0.9</td>
<td>1.0</td>
</tr>
<tr>
<td>29 billion</td>
<td>5.2</td>
<td>5.3</td>
<td>5.4</td>
<td>5.5</td>
<td>5.6</td>
<td>5.7</td>
<td>5.8</td>
</tr>
</tbody>
</table>

© 3IF.be, 2019, Private & Confidential, Closed User Group Distribution. p 20
Source: Ericsson 5G, 2017
Challenges of digital Technologies

- Security: New technology and its number of various interfaces lead to new potential security lacks in a company.
- Investments: Conversion to digital technologies can be expensive, this can be a problem especially for SMEs.
- Privacy: Through increasing collection of data caused by digital technologies, new risks and challenges for protecting privacy are created.
- Lack of competence: New technologies require knowledge for using and handling them, otherwise they will not be accepted and the usage will not be efficient.
- Management Culture: Digital networking requires the openness and transparency of information. Strict hierarchies weak the potential of innovations in a company.

We Are

3IF.be

Industrial IoT, Industrie 4.0 & Industrial Internet

Industry & Technology Experts

Digital Transformation for Manufacturers & Technology Providers

- Assessments, Road Mapping and Advisory
- Knowledge Transfer & Competence Building
- Proof of Concept & Project Development Support
- Industrie 4.0, Industrial Internet, IoT expert network
- International Technology Promotion
- Education and Training

Data Analytics
Industrial Internet
Internet of Things
Industrie 4.0
Digital Twin
Mass customization
Preventive Maintenance
Industrial Cloud
Augmented Reality
3IF.be in a nutshell

1. **Non-profit, government supported, digital transformation support action for manufacturing**
2. **Stimulate** (economic) developments of industrial internet, industrie 4.0 and IIoT in Flanders, and support the viability of the Industry
3. **Inform** manufacturers and suppliers on use cases and technological developments to fully benefit of the technological opportunities ahead
4. **Support** the digital transformation with information sessions, workshops, trainings and advisory services
5. **Connect** suppliers with users of technology
6. **Identify and Create I4.0 ecosystems**, with Flemish technology providers
7. **Support** industry initiatives with digital, technology and best practice expertise and experiences
8. **Cost+ operations**, aimed to raise developments

© 3IF.be, 2019, Private & Confidential, Closed User Group Distribution. p 23

---

### 3IF.be SMART SPECIALISATION PLATFORM

- **Targeted Support**
  - By regions and countries
  - R&D in logistics regions
  - Staying to Excellence
  - Higher Education institutions
  - Past projects
  - Digital Growth
    - Digital Innovation Hubs
      - Digital Innovation Hubs Catalogue
    - ICT Monitoring
    - Digital Agenda Toolbox
    - Digital Agenda PKI
    - Digital Growth and ICT

- **Digital Innovation Hubs**

  The European Commission launched on 19 April 2019 the first industry-related initiative of the Digital Single Market package: Building on and complementing the various national initiatives for digitising industry, the Commission will act to trigger further investments in the digitisation of industry and support the creation of better framework conditions for the digital industrial revolution. One of the more important pillars of the Digital Europe Industry effort is the activity to develop a network of Digital Innovation Hubs (DIHs).

  - A first version of the Digital Innovation Hubs catalogue is now online.

  Digital Innovation Hubs are one-stop-shops that help companies to become more competitive with regard to their business/production processes, products or services using digital technologies. They are based upon technology infrastructure (competence centres) and provide access to the latest knowledge, expertise and technology to support their customers with piloting, testing and experimenting with digital innovations. DIHs also provide business and financial support to implement these innovations, if needed across the value chain. As proximity is considered crucial, they act as a first regional point of contact, a doorway, and strengthen the innovation ecosystem. A DIH is a regional multi-partner cooperation (including organisations like R&D, universities, industry associations, chambers of commerce, incubator/accelerator, regional development agencies and even governments) and can also have strong linkages with service providers outside of their region.
# Industrie 4.0 Trainings & Certification Program

## Course 1: Concepts of the Industry

**Target group:** Any functional and hierarchical division employees, which is eager to develop a comprehensive knowledge to solve new digital challenges.

**Requirements:** None

<table>
<thead>
<tr>
<th>Modules</th>
<th>digitalized</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Development of the Industry 4.0 concept</td>
<td>1. Wrap-Up course 1</td>
</tr>
<tr>
<td>2. Basics of digitalization</td>
<td>2. Quality management 4.0</td>
</tr>
<tr>
<td>3. Big Data</td>
<td>3. Maintenance 4.0</td>
</tr>
<tr>
<td>4. Internet of Things and Services</td>
<td>4. After sales service 4.0</td>
</tr>
<tr>
<td>5. Industry 4.0 Matrix</td>
<td>5. Business analytics and data mining</td>
</tr>
<tr>
<td>6. Horizontal and vertical integration</td>
<td>6. Ecosystems 4.0</td>
</tr>
<tr>
<td>7. Research &amp; Development 4.0</td>
<td>7. Horizontal and vertical integration II</td>
</tr>
<tr>
<td>8. Production 4.0</td>
<td>8. Robotics 4.0</td>
</tr>
<tr>
<td>10. Business model innovation 4.0</td>
<td>10. Employment and workplace 4.0</td>
</tr>
</tbody>
</table>

**Case Studies:** Yes

**Interactive single and group tasks:** Yes

**Online Exam and Case Study Exam:** Yes

## Course 2: Advanced concepts of the Industry

**Target group:** Course 1 graduates.

**Requirements:** Completion of Course 1

<table>
<thead>
<tr>
<th>Modules</th>
<th>digitalized</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Wrap-Up course 1</td>
<td>1. Wrap-Up course 2</td>
</tr>
<tr>
<td>2. Quality management 4.0</td>
<td>2. Human machine collaboration</td>
</tr>
<tr>
<td>3. Maintenance 4.0</td>
<td>3. Assistance Systems, Augmented reality and Virtual Reality</td>
</tr>
<tr>
<td>4. After sales service 4.0</td>
<td>4. Cloud computing and service orientation</td>
</tr>
<tr>
<td>5. Business analytics and data mining</td>
<td>5. Software system environment</td>
</tr>
<tr>
<td>6. Ecosystems 4.0</td>
<td>6. Change management for 14.0</td>
</tr>
<tr>
<td>7. Horizontal and vertical integration II</td>
<td>7. IT security</td>
</tr>
<tr>
<td>8. Robotics 4.0</td>
<td>8. Continuous and digital engineering</td>
</tr>
<tr>
<td>10. Employment and workplace 4.0</td>
<td>10. Digital implementation management</td>
</tr>
</tbody>
</table>

**Case Studies:** Yes

**Interactive single and group tasks:** Yes

**Online Exam and Case Study Exam:** Yes

## Course 3: The Digital Factory

**Target group:** Course 1 and 2 graduates.

**Requirements:** Completion of Course 1 and 2

<table>
<thead>
<tr>
<th>Modules</th>
<th>digitalized</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Wrap-Up course 2</td>
<td>1. Wrap-Up course 2</td>
</tr>
<tr>
<td>2. Human machine collaboration</td>
<td>2. Human machine collaboration</td>
</tr>
<tr>
<td>4. Cloud computing and service orientation</td>
<td>4. Cloud computing and service orientation</td>
</tr>
<tr>
<td>5. Software system environment</td>
<td>5. Software system environment</td>
</tr>
<tr>
<td>7. IT security</td>
<td>7. IT security</td>
</tr>
<tr>
<td>8. Continuous and digital engineering</td>
<td>8. Continuous and digital engineering</td>
</tr>
<tr>
<td>10. Digital implementation management</td>
<td>10. Digital implementation management</td>
</tr>
</tbody>
</table>

**Case Studies:** Yes

**Interactive single and group tasks:** Yes

**Online Exam and Case Study Exam:** Yes

---

### 3IF.be in-depth and systematic curriculum

[Image of curriculum details]

---

**Course 1 Module 1**

**digitalisation and industry 4.0**

**driver licence**

Copyright © 2018

german innovation centre for industry 4.0

All rights reserved
Advantages of digital technologies

- Cost savings
- Scalability
- Circuit in software possible
- No error propagation
- High integration density
- Small and handy
- Uniform = multi-functionality
- Ease of use
... learn that IoT Devices are a Cyber Target!

Source: LSEC

**Personas - Desired Future Vision 2025**

1. **Autonomous Smart Factories**: (Digital Platforms for) optimised and sustainable manufacturing including advanced human-in-the-loop workspaces
2. **Hyperconnected Factories**: (Digital Platforms for) networked enterprises in complex, dynamic supply chains and value networks
3. **Collaborative Product-Service Factories**: (Digital Platforms for) data-driven product-service engineering in knowledge intensive factories
4. **Small-scale Digitised Factories** (Digital Platforms for) mission-focused digitisation for SME-driven sustainable manufacturing

**Digitisation PATHWAYS from the industrial reality towards Factories of the Future (personas)**

### Pathway within the Persona ‘Autonomous smart Factories’

<table>
<thead>
<tr>
<th>LEVEL I: Spreadsheets, text editors and paperwork</th>
<th>LEVEL II: Software and data silos</th>
<th>LEVEL III: Basic connectivity</th>
<th>LEVEL IV: Off-line optimisation</th>
<th>LEVEL V: Realtime optimisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXCEL/WORD Based ERP</td>
<td>Dedicated ERP Software Implemented</td>
<td>MOM-ERP systems connected</td>
<td>Autonomous/Online/Realtime Manufacturing Process Optimisation on factory level</td>
<td>Platform enabled optimisation</td>
</tr>
<tr>
<td>EXCEL/WORD Based MOM</td>
<td>Dedicated MOM Software Implemented</td>
<td>MOM and SCADA/PLC systems connected</td>
<td>Off-line Manufacturing Process Optimisation on machine level</td>
<td>Humans actively connected</td>
</tr>
<tr>
<td>Manual data acquisition</td>
<td>Data acquisition/monitoring/analysis (SCADA) – isolated systems</td>
<td></td>
<td>Off-line Digital Manufacturing Process Optimisation on factory level</td>
<td></td>
</tr>
</tbody>
</table>

© 3IF.be, 2019, Private & Confidential, Closed User Group Distribution. p 31

Supported by the European Commission through the Factories of the Future PPP (Grant Agreement Number 723777)
Fitting with other architectures, e.g. IIRA - ISF

Manufacturing system perspective

Relation to RAMI 4.0? Recommendations to RAMI 4.0?
Introducing 3IF.be and 3IF.be Fieldlab

1. 3IF.be is the platform supporting the digital transformation of manufacturing companies in Flanders since 2014.
2. A joint undertaking for collective innovation support by LSEC and Sirris with the support of the Flemish Government.
3. Developing guidance documents, use cases and knowledge transfer. Supporting groups of companies and sectors on Industrie 4.0 and Industrial Internet and providing individual guidance to selected companies.
4. Operating a fieldlab on Condition Based maintenance and Industrial Data Space, aiming to proof the concept and the business value of digitalization.
5. Collaborating with IMEC, Flanders Make, Essencia, Flanders Food, Sirris, VOKA, WTCM, the Flemish Government and others in promoting the developments of Industrie 4.0 in Flanders.

The potential of I4.0

- 10-40% reduction of maintenance costs
- 3-5% increase of overall productivity
- 20-50% reduction in time to market
- Up to 65% increase of forecasting accuracy
- 5% reduction of inventory costs
- 30-50% reduction of total machine downtime
- 45-55% increase of productivity in technical professions
3IF.be key achievements

1. Number of organisations reached: 20,000+
2. Nr of Companies in interactions: 300+
3. Nr of Companies in Fieldlab: 50+
4. Companies transforming: 196
5. Variety of sectors:
   1. Process Manufacturing: Petro-Chemical, Pharma & Life, Food Production, Automotive, Building Products, ICT
   2. Discrete Manafacturing: Make, Chemicals, Consumer, Agriculture, Food Production
6. Events, Seminars, promotional activities: +100/yr
8. Documentation – Papers: +500
9. 3IF.be Business Cases - White Pap.: 30

3IF.be Fieldlab: Condition Based Maintenance

© 3IF.be, 2019, Private & Confidential, Closed User Group Distribution. p 37

© 3IF.be, 2019, Private & Confidential, Closed User Group Distribution. p 38
3IF.be & 3IF.be Fieldlab

1. 3IF.be is the platform supporting the digital transformation of manufacturing companies in Flanders since 2014.
2. Developing guidance documents, use cases and knowledge transfer. Supporting groups of companies and sectors on Industrie 4.0 and Industrial Internet and providing individual guidance to selected companies.
3. Operating a fieldlab on Condition Based maintenance and Industrial Data Space, aiming to proof the concept and the business value of digitalization.
4. Collaborating with technology companies and manufacturing companies to realize Fieldlab use cases.

© 3IF.be, 2019, Private & Confidential, Closed User Group Distribution. p 39
Collecting from different Data Collectors

Aluminium powder coating plant  Sandwich panel production line  ATV 900 – already “Smart”
Definition Maintenance 4.0:
“Data captured by sensors and analyzed by software about operating states allow the prediction of the optimum maintenance timing. Thus, forthcoming standstills can be recognized, processes be accelerated and production failures be avoided.”

The potential of maintenance as value creation process rather than a cost factor has to be recognized and employees have to be sensitized to new technologies and processes.

3IF.be Fieldlab benefits for partners and users

1. Digital Factories & Users: proven cases and pre-selected and test technologies, use case experiences, business models, collective data analysis and reporting, selected advisory and support. Visibility and internal support for additional proof of concept cases and digital transformation. View on proven technologies and use cases. Economies of scale and scope in analysis and documentation.

2. Strategic Partners: IoT & Connected Sensors and actuators, connecting technologies, digital platforms for data capturing and modelling and orchestration, analysis platforms and technologies, reporting platforms and advisory: use cases development, system integration, joint innovation, market & competitive analysis.
Maintenance, Avoid Risk & Guarantee Safety

Deep Horizon disaster was related to inaccurate information, poor communication and decision making.

Accurate Asset Information is key
Analytics can help

Reliability = a high Mean Time-Between-Failures (MTBF) and a short Mean Time-To-Repair (MTTR)

Maintenance i4.0

“Good morning conveyor belt, how are you today?”

“I’m on my way.”

“Morning, I really don’t feel well today... Some kind of disruption is on its way.”

“That’s what I thought. I will send a service technician over there.”
Maintenance i4.0

PdM Maturity Matrix

Source: PwC, PdM 4.0, 2018
Use Case C&C Machine Monitoring CBM - iMaintenance

one of the main Aluminium joinery technologies provider in Belgium:

1. monitor the power consumption of the machine for three different motors, and also we’ll monitor the alarm contact, together with the safety-chain supervising
2. send data in the cloud application, trigger will send a message to the target list recipients
3. monitor ambient conditions, define baseline and report on potential changes
4. provide monitoring application to both factory and supplier and improve on efficiency – reducing outages, cost of material and waste
5. avoid outages
3IF.BE FIELDLAB: Condition Based Maintenance Business Value

Potential Revenue

Gross Available Time (24/7/365)
Scheduled Operating Time
Operating Available Time
Net Operating Time
Effective Operating Time
Actual Revenue

Operating Loss
Operative Loss

Availability Loss: Planned Downtimes
Utilization Loss: Unscheduled Disruptions
Rate Loss: Constrained Operation
Quality Loss: Defects, Yield, Transitions

Project Performance Management
Asset Performance Management

Plan
Design
Procure
Build
Operate
Maintain
Retire & Recycle

Revenue
OPEX
Net Income

Capital Costs (CAPEX)

ROI

Source: 3IF, Versasense 2017

Maintenance i4.0

Higher customer satisfaction 8%
New revenue stream 1%
16% Lifetime extension of aging asset

47% Uptime improvement
17% Cost reduction
11% Reduction of safety, health, environment & quality risks

© 3IF.be, 2019, Private & Confidential, Closed User Group Distribution. p 51

© 3IF.be, 2019, Private & Confidential, Closed User Group Distribution. p 52
Some of the devices we use in the demo sessions
Cloud Challenges (on and beyond security)

Cloud & Digital Platforms – Normalizing regulatory requirements
Digitalisation is both an enabler and a driving force behind innovative business models.

A key ability for innovative business models is to be able to combine data in one "ecosystem".

Digital services follow common architecture principles:

- Services are decoupled from physical platforms/products
- The architecture levels are decoupled
- Products become platforms and vice versa
- "Ecosystems" develop around platforms
- Innovation takes place cooperatively
FIELDLAB: Reaping Business Value through Industrial Data Space

57% today worry about revealing valuable data and business secrets.
59% today fear the loss of control over their data.
55% today feel inconsistent processes and systems as a (very) big obstacle.
32% today fear that platforms do not reach the critical mass, so that data exchange will be interesting.

Industrial Data Space Approach

More Data Security
Improvement of Sovereignty
Optimising Processes and Cost Structures

Self determined control of data flows in a peer to peer approach:

Endless Connectivity – standard for data flows between all kinds of data endpoints
Comprehensive security functions providing a maximum level of trust
Usage control and enforcement for data flows

© 3IF.be, 2019, Private & Confidential, Closed User Group Distribution. p 59

80+ Companies and Organisations
5 Working Groups
20+ Use Cases
1 Ecosystem

www.industrialdataspace.org
Digital Manufacturing

32%

of IIoT devices connect directly to Internet, bypassing traditional IT security layers.

* 32.4% via Internet DMZ (Gateway) (Level 5–4)
* 32.4 via Controlled DMZ (Level 3–0)
* N/A - Safety Zone

Source: 2018 SANS Industrial IoT Security Survey, Shaping IIoT Security Concerns
Recent Attack examples with industrial impact

**Threat Graph Data**

<table>
<thead>
<tr>
<th>Type</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events per Day</td>
<td>9/36</td>
<td>24/8</td>
</tr>
<tr>
<td>Peak Events per Second</td>
<td>1.8M</td>
<td>3.8M</td>
</tr>
<tr>
<td>Average Events per Second</td>
<td>1.0M</td>
<td>3.0M</td>
</tr>
</tbody>
</table>

- Detect intrusions in under one minute,
- Perform a full investigation in under 10 minutes
- Eradicate the adversary from the environment in under 60 minutes

*Source: Stormshield, The Register*

Recent events

Source: ZDNet, Sep 16th - 2018
Hacking a Ukrainian Power Plant

Source: https://www.wired.com/story/russian-hackers-attack-ukraine/

Industrial Controls in Belgium

- **Query Shodan**
  - "Industrial Control Systems"
    - Predefined ports, strings
    - + some popular strings/vendors

- **api.search(expr);**
  - Per result api.host(ip_str, history=False)
    - Hostname, domain, open ports
    - SQLite Database
    - Only if combination of host+port+transport isn’t already there;

- **Extract product and device information;**
  - Shodan info (device_type, product_name, vendor_id, shodan_module)
  - Simple banner parsing (also from Shodan)
    - 1° Product name ; 2° HTTP Banner ; 3° First strings in Shodan data object
Key Experiences from IoT in the Home ...

Case Study of Some Common Home IoTs

Protocol Level Vulnerabilities

- Nearly Every Device
  - Need to automate compliance checks on all devices firmware, device would take an experienced analyst days
Why is Identity Protection important for enterprises?

300% increase in identity attacks over the past year.

Azure Active Directory metrics over 800,000 high usage tenants

Source: EEMA / Kim Cameron

CyberSecurity Challenges with Digital Manufacturing

© 3IF.be, 2019, Private & Confidential, Closed User Group Distribution. p 71

Source: Secudea, 3IF Conference, 09/18
Cybersecurity for Industrial Control Environments: basics (1/2)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEC 62443</td>
<td>Level 0</td>
<td>Level 1</td>
<td>Level 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIST 800-82</td>
<td>Level 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEAE 17</td>
<td>Level 1</td>
<td>Level 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Cybersecurity for Industrial Control Environments: basics (2/2)

1) Risk based approach
2) Process, People, Technology
3) CIA: Confidentiality, Integrity, Availability
4) Prevent, Detect, Respond, Mitigate, Recover
5) ICS:
   a. Zoning / segmentation / isolation: per criticality, per function, per supplier, but prevent overzoning
   b. Different Levels / segmentation
      a. Physical
      b. Logical
      c. Human
   c. Supply Chain
   d. Define Threat
   e. Simulation
ICS Cybersecurity Incidents Reported

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage of ICS Computers Attacked</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturing</td>
<td>31.0%</td>
</tr>
<tr>
<td>Engineering</td>
<td>24.5%</td>
</tr>
<tr>
<td>Education</td>
<td>14.5%</td>
</tr>
<tr>
<td>Food &amp; beverage</td>
<td>9.7%</td>
</tr>
<tr>
<td>Energy</td>
<td>4.9%</td>
</tr>
<tr>
<td>Utilities</td>
<td>3.9%</td>
</tr>
<tr>
<td>Oil &amp; gas</td>
<td>3.0%</td>
</tr>
<tr>
<td>Construction</td>
<td>2.9%</td>
</tr>
<tr>
<td>Telecom</td>
<td>1.5%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>1.2%</td>
</tr>
<tr>
<td>Mining</td>
<td>0.9%</td>
</tr>
<tr>
<td>Logistics</td>
<td>0.6%</td>
</tr>
<tr>
<td>ICS software</td>
<td>0.6%</td>
</tr>
<tr>
<td>Building automation</td>
<td>0.3%</td>
</tr>
<tr>
<td>Transportation</td>
<td>0.3%</td>
</tr>
</tbody>
</table>

Source: Kaspersky, ICS ISAC, 2018

Risk Management: Robots in Manufacturing Environments

Report from the Workshop on Cybersecurity for Manufacturing Environments

held on 17th October 2018, BluePoint Centre, Brussels, Belgium

https://tinyurl.com/ymbqkqs3


Source: LSEC, EC, 2018
Challenges in Cybersecurity for Manufacturing

- Any device can be tricked
- Prominent difference between OT & IT
- ICS sensitivity – instability
- Human error threats
- Cybersecurity experts are scarce
- Organisational solutions limited
- Data is flowing beyond company borders
- Digitization happens across the supply chain
- Transition towards service and data driven business models
- Safety-critical system

Source: CCITT, 2016
Cybersecurity Robots Research In Progress

1. Missing Cybersecurity Risk Management & Policy from robot producer to robot operators
2. Not integrated with current Cybersecurity Operations & ICT Standards
3. Robots often standalone, but Cybersecurity considerations for manufacturing apply
4. Missing Cybersecurity by Default, Design & Lifecycle Security
5. Commands in clear text
6. All Systems Architectures Cybersecurity attack surfaces: challenges both direct, through PLC’s, IoT or combined
7. Major Cybersecurity challenges:
   1. Lack of Isolation, Application Security, Patching
   2. Privileged access – controller takeover, compromise
   3. Man In The Middle – data and production integrity, tampering
   4. Embedded System Challenges – state alteration
   5. Lack of encryption

Source: Meacademic, Politecnico, LSEC, 2019
Robots are used to perform complex and critical tasks in all the major industry sectors.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 825196.

Ulrich Seldeslachts
LSEC – 3IF.eu / CyberSecurity for Robots
Objectives

- Improve agility & innovation capability of European manufacturing companies (focus on SMEs) through robotics and IoT
- Build a network of Digital Innovation Hubs beyond the project life-time
- Provide critical mass of use cases to demonstrate new robotic technologies & added-value in different sectors
- Create a digital access point to facilitate access to knowledge, collaboration and networking

Three thematic areas

**INTERNET OF THINGS**
Industrial Internet of Things, digital twins, digital tools & platforms

**ROBOTICS**
Interaction/ collaboration & system reconfiguration

**CYBERSECURITY**
Trust, data sharing, data privacy & system error recovery
Robot Programming: Clear Text

[Image of robot programming interface]

Source: KUKA, 2019

---

Robot Programming: Web interface - IoT

[Image of robot programming web interface]

1. [Diagram element]
2. [Diagram element]
3. [Diagram element]
4. [Diagram element]
5. [Diagram element]
6. [Diagram element]
7. [Diagram element]

Source: Mecademic, 2018
Example Attack 1: Controller Take-Over

1) Configuration tampering
2) User-perceived robot state alteration
3) Robot State alteration
4) Production logic tampering
5) Calibration parameter tampering

... IoT Security Standard: ETSI TS 103 645 v1.1

Cyber security provisions for consumer IoT
1. No universal default passwords
2. Implement a means to manage reports of vulnerabilities
3. Keep software updated
4. Securely store credentials and security-sensitive data
5. Communicate securely
6. Minimize exposed attack surfaces
7. Ensure software integrity
8. Ensure that personal data is protected
9. Make systems resilient to outages
10. Examine system telemetry data
11. Make it easy for consumers to delete personal data
12. Make installation and maintenance of devices easy
13. Validate input data
Cybersecurity – strategy: process, people, technology

1) secure your environment
   a. Restrict Internet Access
   b. Segregate critical systems from general IT environment
   c. Reduce attack surface and vulnerabilities
   d. Physically secure the environment

2) know and limit access
   a. Prevent compromise of credentials
   b. Manage identities and segregate privileges

3) detect and respond
   a. Detect anomalous activity to system or transaction records
   b. Plan for incident response and information sharing

Cybersecurity highlights – Controls

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-factor Authentication</td>
<td>User Account Management</td>
<td>Token Management</td>
<td>Malware Protection</td>
<td>Software Integrity</td>
<td>Database Integrity</td>
<td>Cyber Incident Response Capability</td>
</tr>
<tr>
<td>Transaction Business Controls</td>
<td>Personnel Vetting Process</td>
<td>Physical and Logical Password Storage</td>
<td>Intrusion Detection</td>
<td>Penetration Testing</td>
<td>Scenario Risk Assessment</td>
<td></td>
</tr>
</tbody>
</table>

Supported by the European Commission through the Factories of the Future PPP (Grant Agreement Number 723777)
Digital Platforms in financial services

Source: CA, ING, Nordea, TESOBE, LSEC 2018
Cloud Challenges (on and beyond security)

What is 5G?

Virtual network slices...

... based on a common set of physical resources
Access – Connectivity – Computing – Storage

A common network platform supporting multiple industries and use cases
Living on the Edge: architecture perspective

Closing the Digital Twin loop

Collaboration platform: Teamcenter
Digital Production Line

Logistic Validation
Identified AI cybersecurity risks: (CIA-based)

1. Data poisoning
2. Adversarial attacks
3. Model stealing (model extraction attack)
4. Video Forgery

*IBM Research has recently released an open source library called Adversarial Robustness Toolbox ("ART")*
However, new evolutions: Avatars – Impersonization - DeepFakes
AI for CyberSecurity

Collecting Data with a Purpose

Objective

Source type

Source location

Source identification

Source attributes

Other parameters
Be a domain expert
Understand your data. Know good vs bad when you see it.

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>User</th>
<th>Session</th>
<th>Device</th>
<th>Application</th>
<th>IP Address</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-Mar</td>
<td>10:05</td>
<td>Alice</td>
<td>1</td>
<td>iPhone 8</td>
<td>Exchange</td>
<td>1.2.3.4</td>
<td>US</td>
</tr>
<tr>
<td>3-Mar</td>
<td>15:07</td>
<td>Alice</td>
<td>2</td>
<td>iPhone 8</td>
<td>Exchange</td>
<td>1.2.3.5</td>
<td>US</td>
</tr>
<tr>
<td>3-Mar</td>
<td>16:45</td>
<td>Alice</td>
<td>3</td>
<td>Windows 10</td>
<td>Salesforce</td>
<td>2.2.2.1</td>
<td>US</td>
</tr>
<tr>
<td>4-Mar</td>
<td>10:23</td>
<td>Alice</td>
<td>4</td>
<td>Windows 10</td>
<td>Salesforce</td>
<td>2.2.2.1</td>
<td>US</td>
</tr>
<tr>
<td>4-Mar</td>
<td>2:04</td>
<td>Alice</td>
<td>5</td>
<td>Linux</td>
<td>Sharepoint</td>
<td>13.22.12.12</td>
<td>RU</td>
</tr>
<tr>
<td>5-Mar</td>
<td>11:30</td>
<td>Alice</td>
<td>6</td>
<td>iPhone 8</td>
<td>Exchange</td>
<td>1.2.3.4</td>
<td>US</td>
</tr>
</tbody>
</table>

- Alice doesn’t normally log in at 2 AM
- This is not a familiar device for Alice
- Alice doesn’t normally use SharePoint
- We have never seen Alice log in from Russia
- There are 132 other users from different tenants using this IP address

Source: EEMA / Kim Cameron
Automating the process and the need for AI

Cyber Threat Intelligence (CTI)

12 Mn attacks on our 200 physical honeypot sensors (1,000 logical Sensors)

10 Mn mails analyzed against spam

1.000 virus & malware filtered

1.000 requests to Telekom CERT

>6 BN data records of our DNS Server evaluated regarding cyber attacks

100,000 indications about abuse of private customer access

21 vulnerability advisories

20 MN malicious codes in our malware library
Intermediate Conclusion Cyber Security Experiences with data, analysis, ML and AI

- We're not there yet.
- 99.9999% of defenders don’t know what’s on their own networks.
- Bulk observation and analysis of data, faster than an analyst
  - Identification of Anomalies, Dynamic Classification, Mining Behavior
  - Higher level of confidence than vanilla correlation
  - Focusing Analyst time on the areas most likely to relate to an incident
  - Making Analysts more effective, saving manual work
- Can only support activity, won’t create, expand or drive – yet
- Garbage in, garbage out; need to learn on meaningful input
- Continuous analogical vs Discrete volatile data
  - Most of IA tooling work on continuous/analogical data Image, sounds, language
  - Our data is by essence discrete and volatile
- Some applications
  - Family identification
  - Scoring
  - Anomalies and correlations

From DevOps to AIOps – via DevSecOps


112

© Leaders in Security – LSEC – CIMA, 2019, Public – Closed User Group Distribution, p 113

113
**LSEC – European Cyber Security Catalyst**

*European Network of Security Professionals, Research and Industry*

LSEC is an international IT- & Information Security cluster, a not for profit organization that promotes Information Security and the expertise in Europe. Founded by the University of Leuven, supported by European and Flemish Communities and leading a PAN European Private partnership that interacts with Public Institutions, LSEC connects security experts, research institutes and universities, government agencies, end users, funding bodies and technical experts and is a catalyst in cyber security innovations. LSEC activities aim to raise cyber security awareness, support innovation and improve the competitiveness of the IT- Security market.

**Unite stakeholders, stimulate collaboration, enable high tech entrepreneurship**

LSEC provides an international platform that unites security stakeholders, stimulates collaboration and enables high tech entrepreneurship. This will help researchers understand industry needs, help Industry access the IT security research that they need, and help ensure that fundamental research is translated to sustainable solutions.
**LSEC – European Cyber Security Catalyst**

**Bring together the IT Security Expertise in Europe**

With a broad membership base of over 365+ security specialized organizations, and more than 10,000 individual Information security professionals, LSEC accesses over 25,000 security stakeholders on a regular basis. With operations in the Netherlands, Belgium, Luxembourg and the UK, LSEC leads a PAN European Partnership with other security clusters that interacts with private partners, policy makers and public administration.

**Strategic partners**

LSEC has a strategic partnership with other European Cyber Security Clusters and Industry Associations. We’ve teamed up with ISSE, EEMA and The European Trust Foundation, because of joint interests and experience sharing, providing a channel for collaboration and joint developments.


Technology for Social Challenges

- Cyber Range is the next generation cloud platform for acquiring and assessing cybersecurity competences through gamification and social interaction
  - Cloud-based hands-on content creation and sharing platform
  - Community access
  - Learning and assessment platform
  - Gamified learning
  - Cyber competitions

Source: Intrinsic ID, 2018
Vendor Risk Management

Know your exposure

Know your partners

This provides an overview of your partners and their score.

Source: Ceeyu, October 2018

Technology Innovation: Device ID

How to secure IoT devices connecting to the cloud?

Perimeter secured by hardware access control

Secure derivation of authentication key pair

Data Encryption and Authentication

Device-unique root key from unclonable Silicon Fingerprint

Device-unique Certificate

Provisioning PC & Certificate Authority

Cloud Service

Source: Intrinsic ID, 2018
Security Fieldlab & Security for Manufacturing

PARTNERSHIP MEMBERS

GLOBAL EPIC
Global Executive of Guepardis Partnership in Innovation and Cybersecurity

https://globalepic.org
Industrie 4.0, Industrial Internet and Industrial IoT in Flanders

Are You..?
Manufacturer, Industrial Processor or Technology Provider
Small & Medium Sized
Going Smart, Digital and Connected

Q or C
Ulrich Seldeslachts
ulrich@lsec.eu
+32 475 71 3602