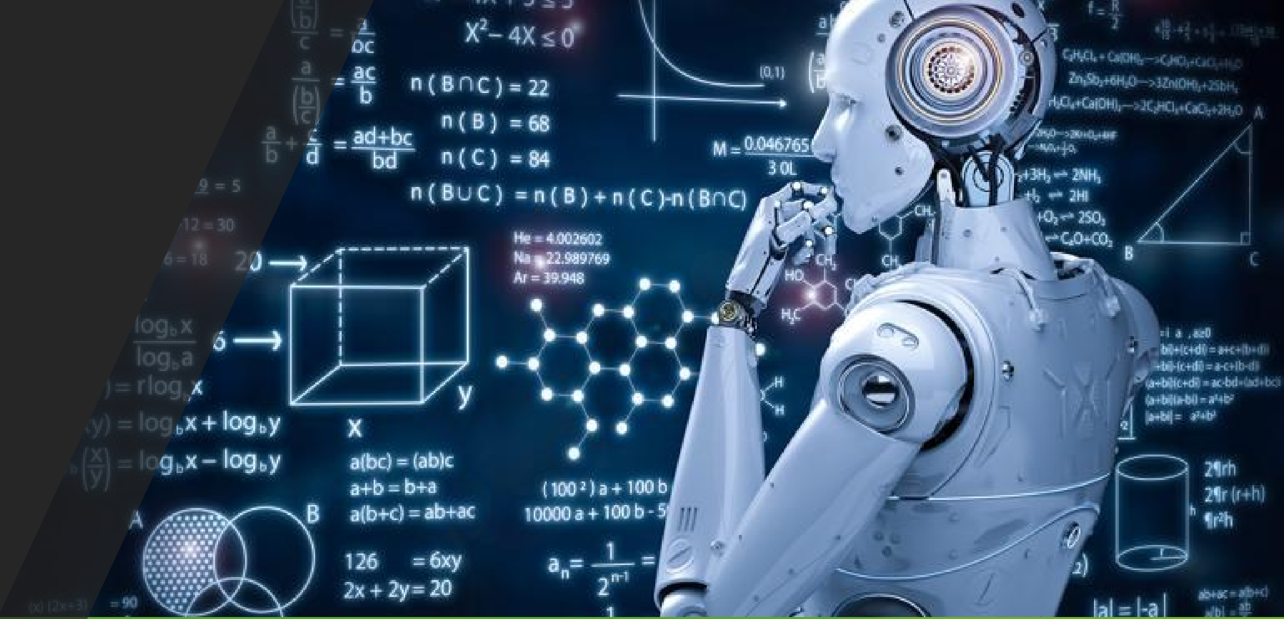
Industrial Cloud Security and Machine Learning



Prof. Dr. Christoph Reich

rch@hs-furtwangen.de

Institute for Data Science, Cloud Computing and IT Security

Idacus.hs-furtwangen.de

Hochschule Furtwangen University

IARIA

HOCHSCHULE FURTWANGEN UNIVERSITY | HFU

Profile
Prof. Dr. Christoph Reich

- professor at the faculty of computer science at Furtwangen University
- teaches: network technologies, IT security, machine learning, and distributed systems
- CISO of the HFU
- since 2009 head of the institute Data Science, Cloud Computing and IT Security

Institute for Data Science, Cloud Computing und IT-Sicherheit (IDACUS)

Facts:

- head: Prof. Dr. Christoph Reich (rch@hs-furtwangen.de)
- 4 Professors and 13 researchers
- 8 PhDs, 12 masters, 18 bachelors
- actual 12 research projects
- idacus.hs-furtwangen.de

Research area:

- Distributed system
- Cloud Computing
- IT security
- IoT/Industry 4.0
- Maschine Learning

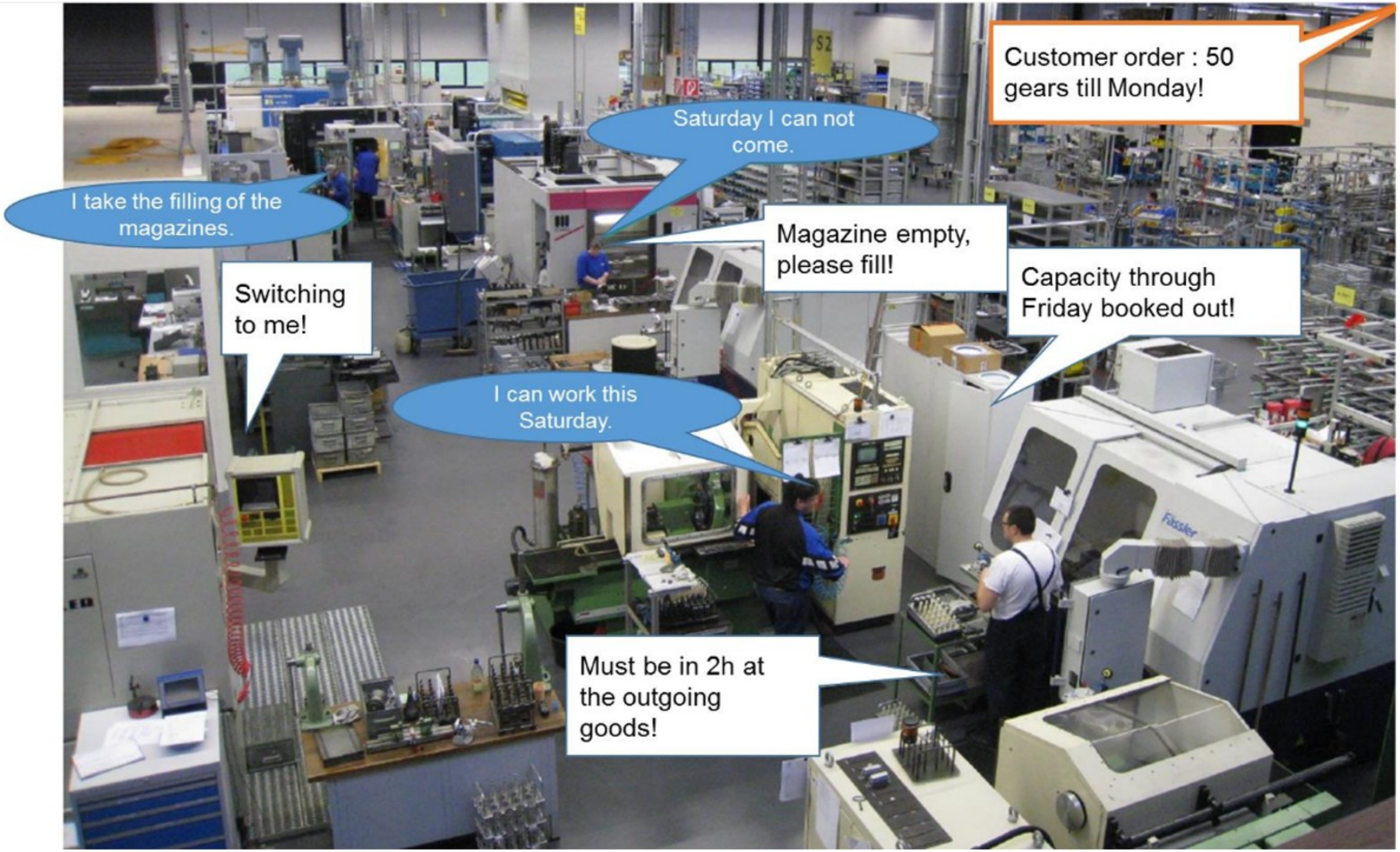
Agenda

- Smart-Factory, Use Cases
- Machine Learning
  - Halfback, SensoGrind, HMT
  - (data quality, model quality, devOps)
  - Machine Learning Operations (12min)
- Security IoT and ML
- Architecture
- Blockchain-Accountability (12min)
- Security Monitoring of HPC containers (12min)

Smart Factory

https://www.it-zoom.de/it-mittelstand/e/auf-dem-weg-zur-smart-factory-28622/

Smart Factory

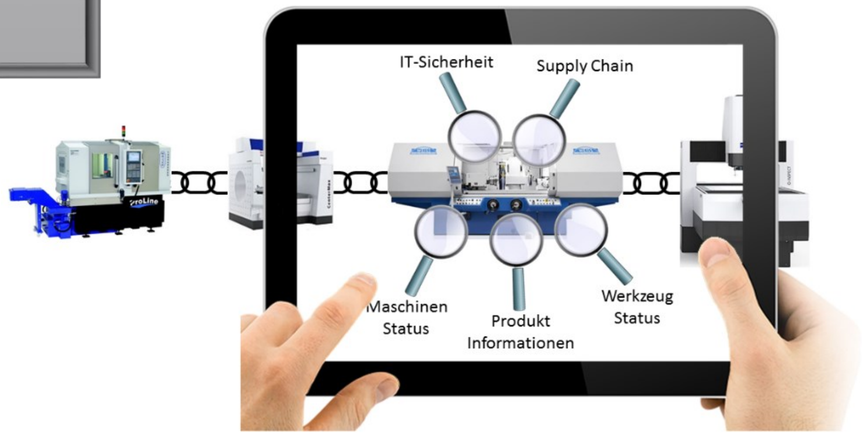


Legend:

Applications in Industry 4.0 (CPS)

Process optimization, condition monitoring, remote monitoring, remote maintenance, predictive maintenance, quality control, quality prediction, etc.

Smart Products: How to connect products, self-diagnosis, tracking, etc.

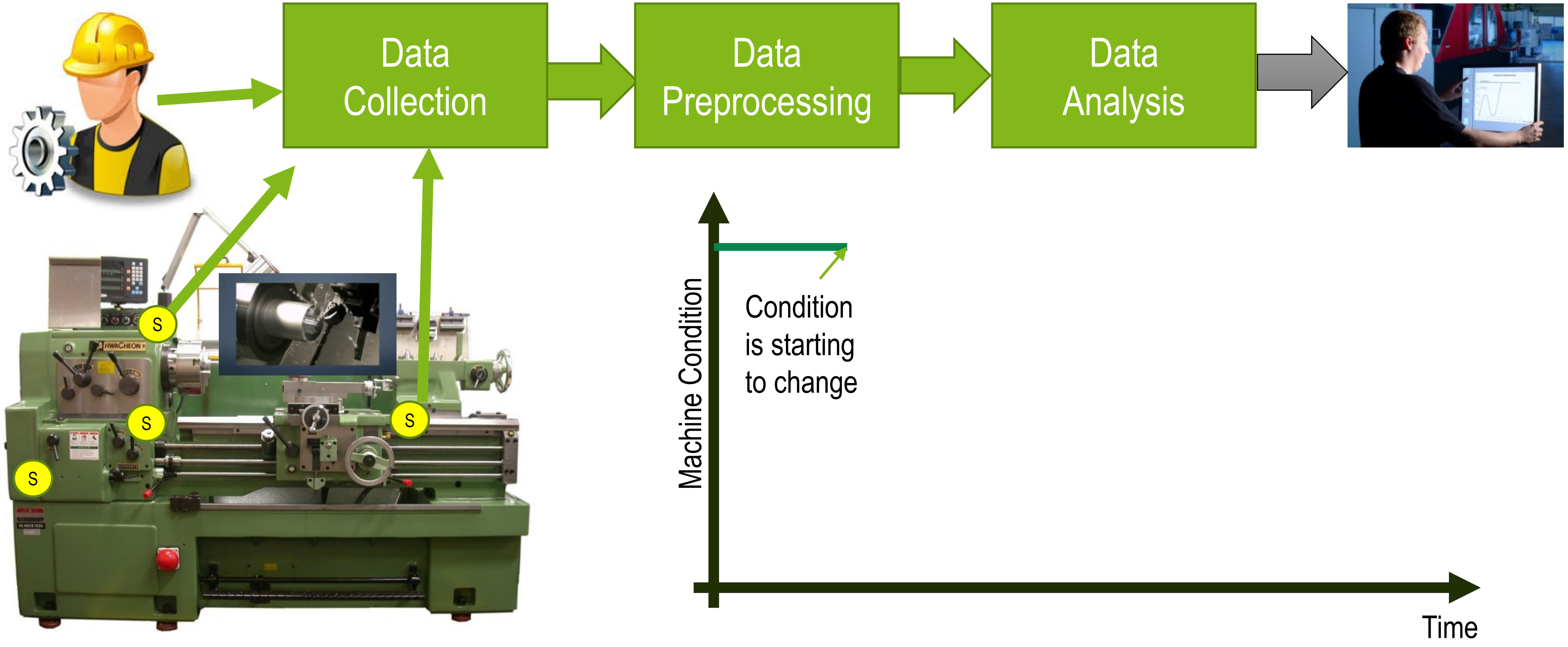


Industrial manufacturing: monitoring, self-diagnosis, one lot production, flexible production, etc.

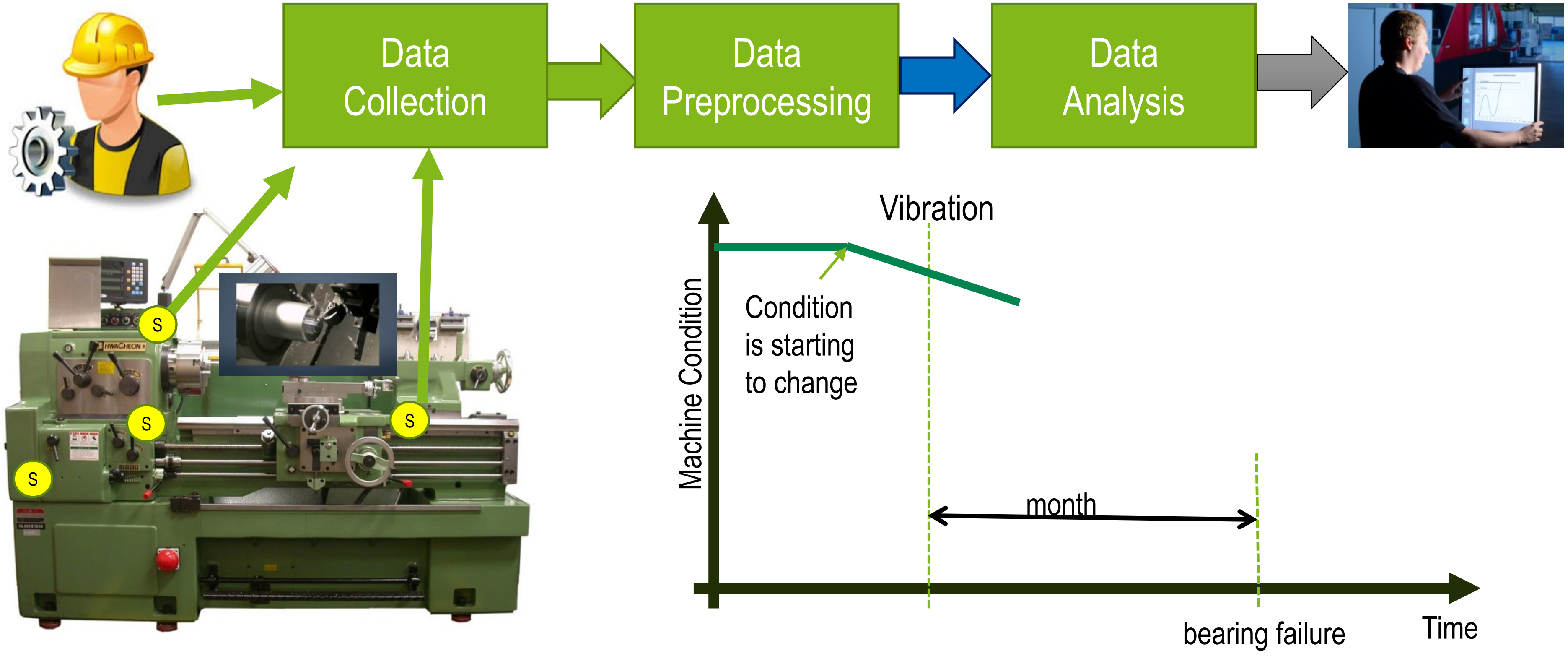
Machine Learning

Research Project A: Predictive Maintenance

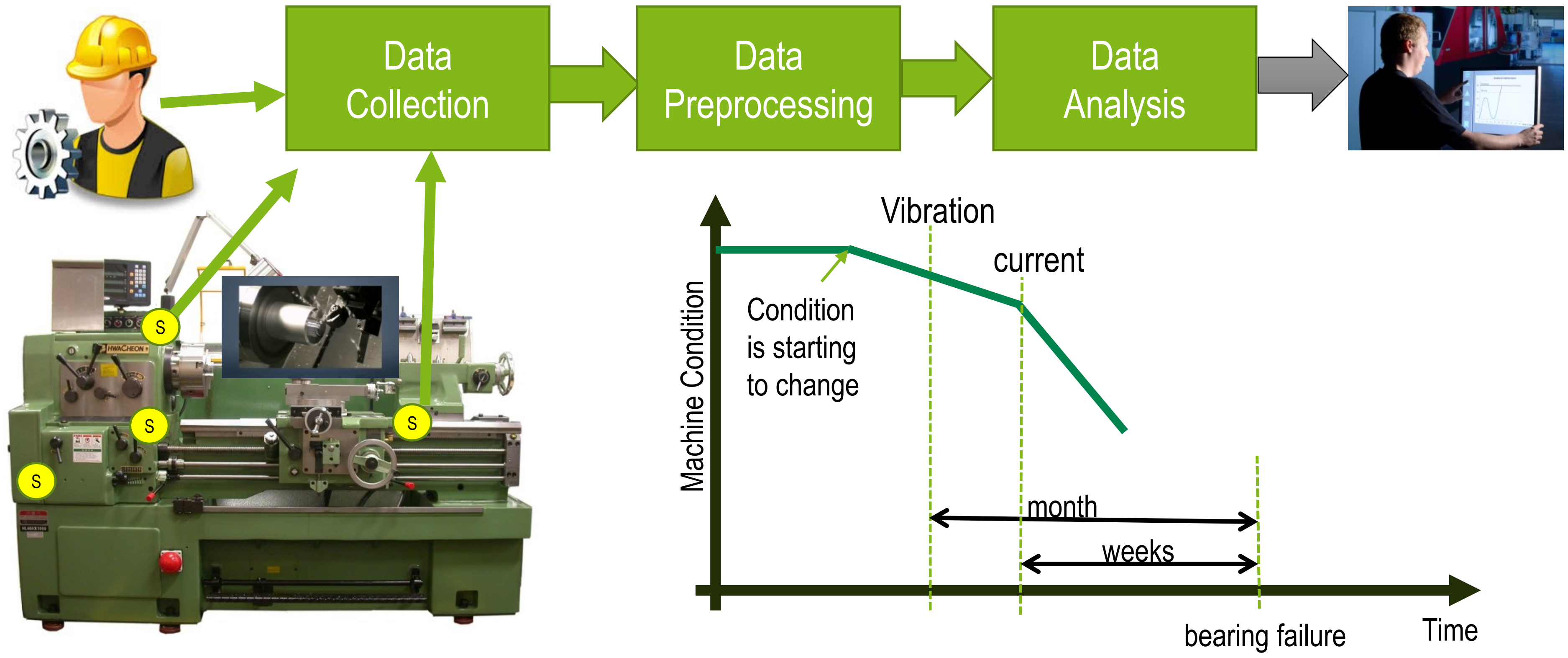
Predictive Maintenance



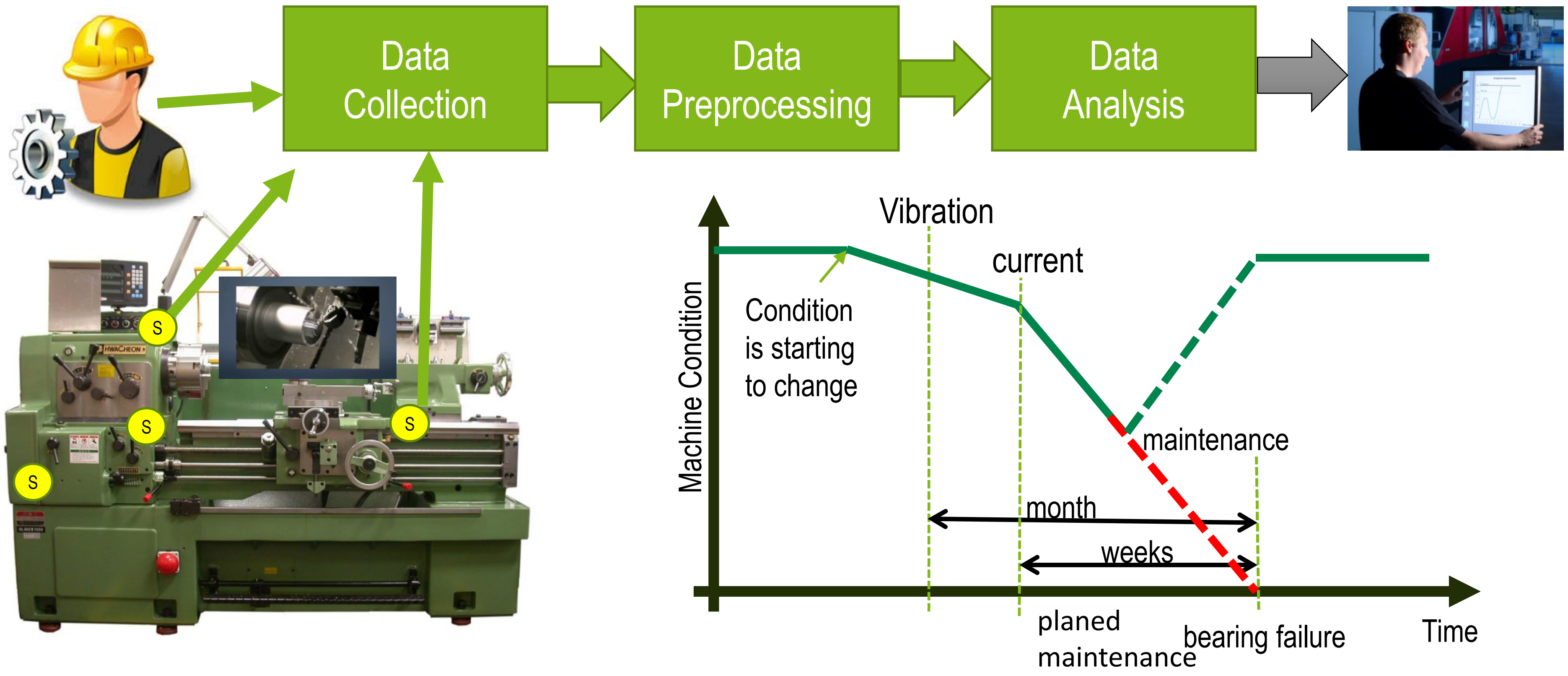
Predictive Maintenance



Predictive Maintenance



Predictive Maintenance



HOCHSCHULE FURTWANGEN UNIVERSITY HFU

Fonds européen de développement régional (FEDER)
Europäischer Fonds für regionale Entwicklung (EFRE)

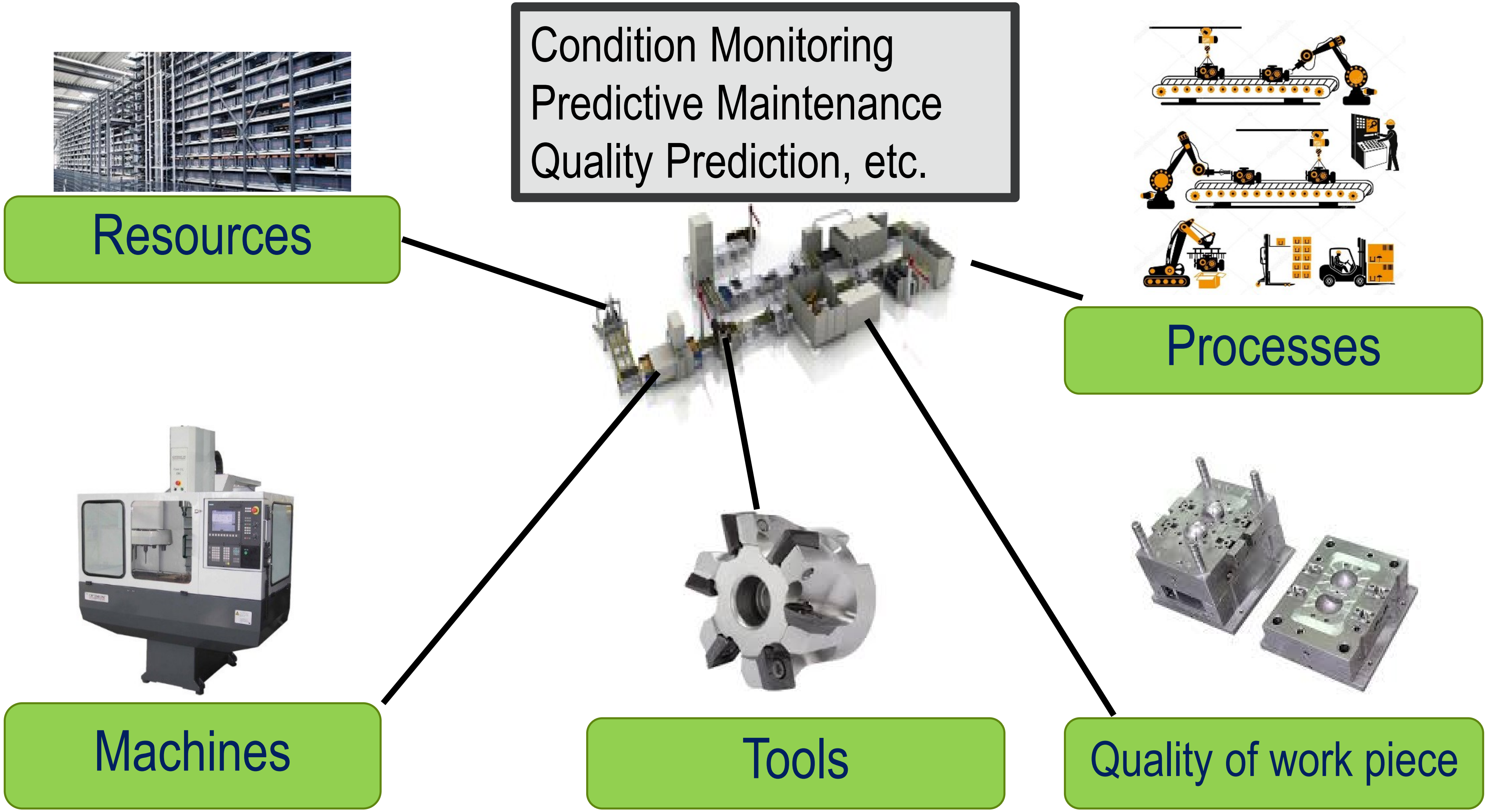
interreg Oberrhein Rhin Supérieur

HALFBACK

Highly Aviailable Smart Factories in the Cloud

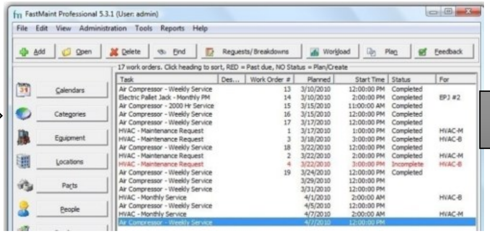
04/2017 - 03/2020

Goal: High Availability Production



AI Methods

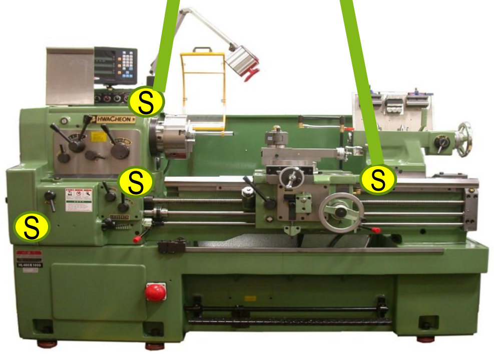
Data Collection



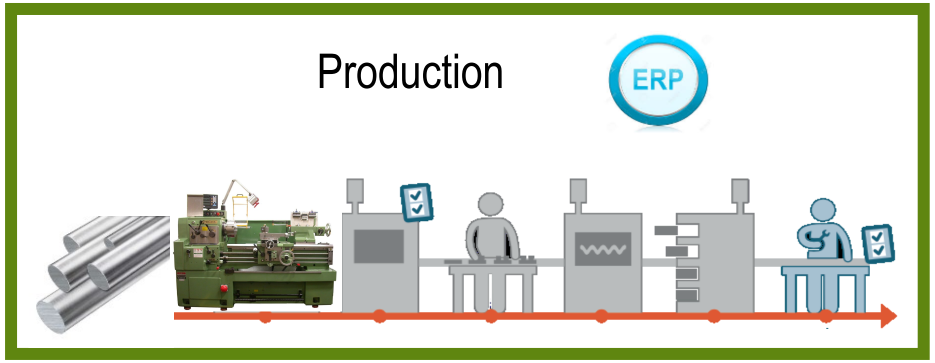
Preprocessing

Analysis

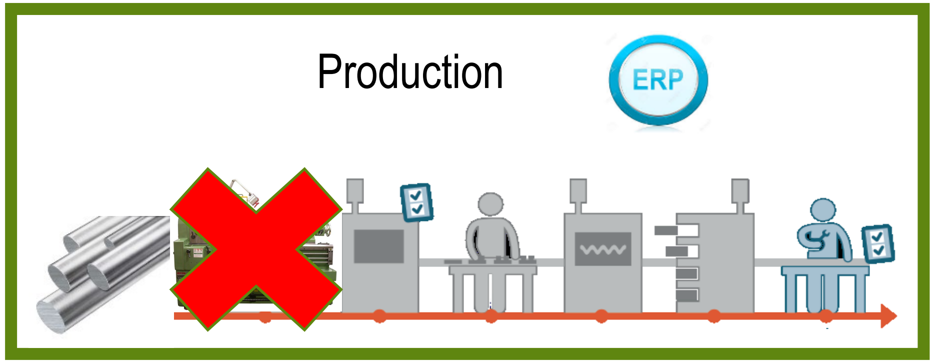
Quality Prediction
Predicitve Maintenance



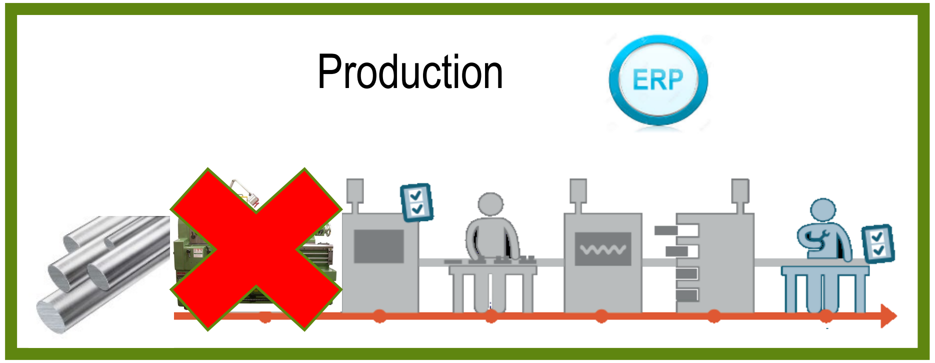
Problem	Approach	Predcition
Time for machine failure	Chronical mining	Machine failure events
Time for machine failure	Neural networks	Machine compontent failure
Visual surface defects	Convolutional neural networks	Detection of Surface failure



KMU



SME

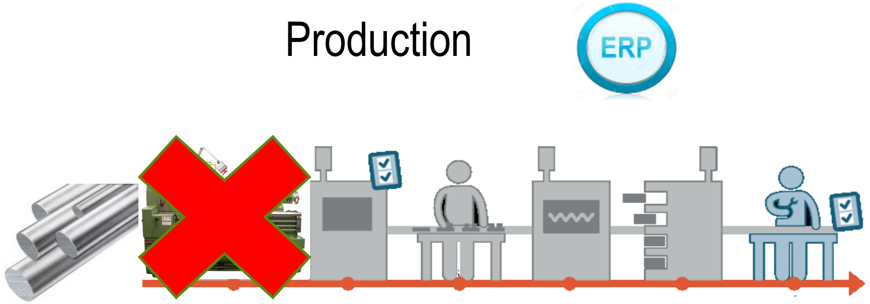

Production
ERP

SME


Frankfurt
Germersheim
Landau
Palatinate
Karlsruhe
Stuttgart
Paris
Strasbourg
Baden-Baden
Alsace
RHINE
Black Forest
FRANCE
GERMANY
Colmar
Dijon
Mulhouse
Basel
Zürich
SWITZERLAND

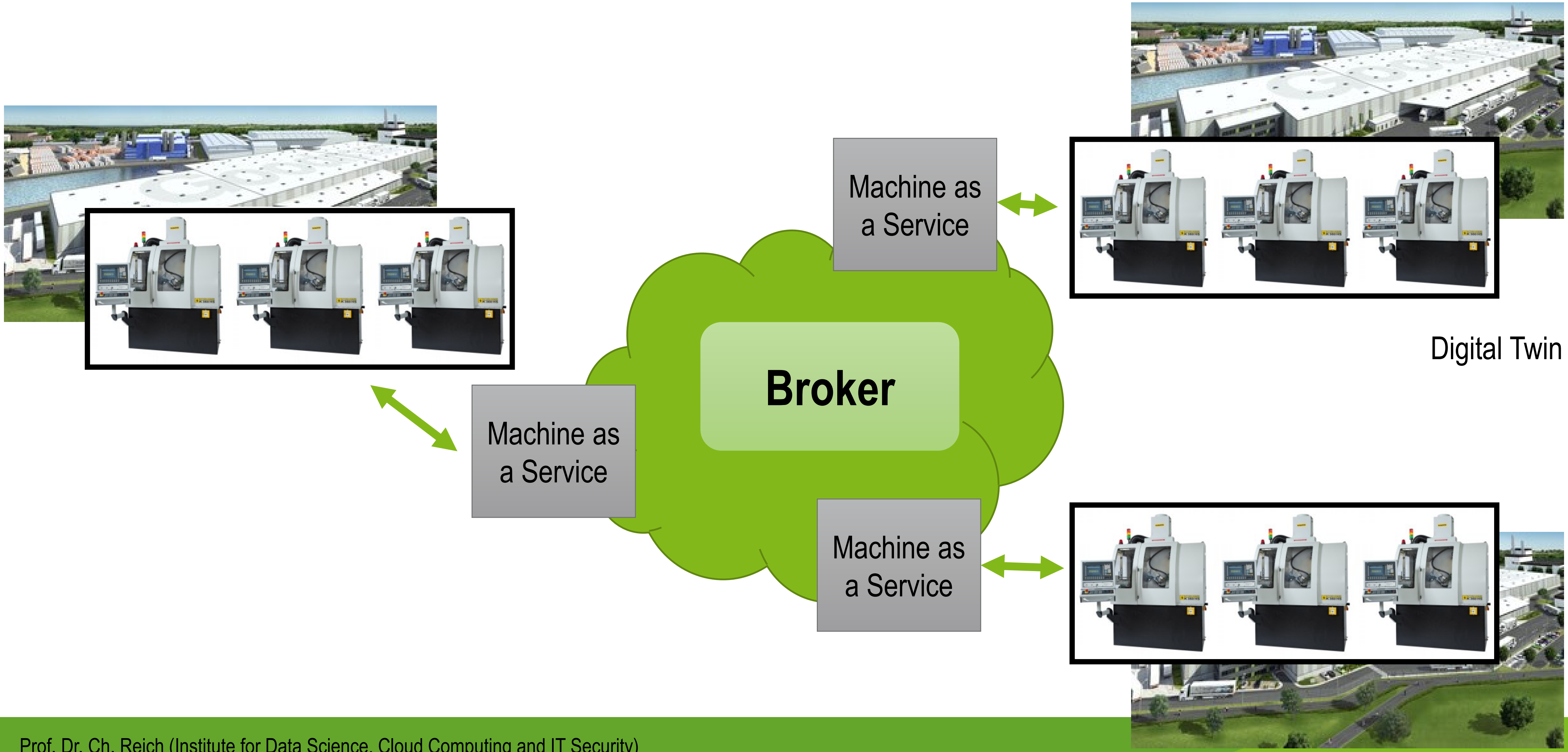
Machine Broker

Production



SME

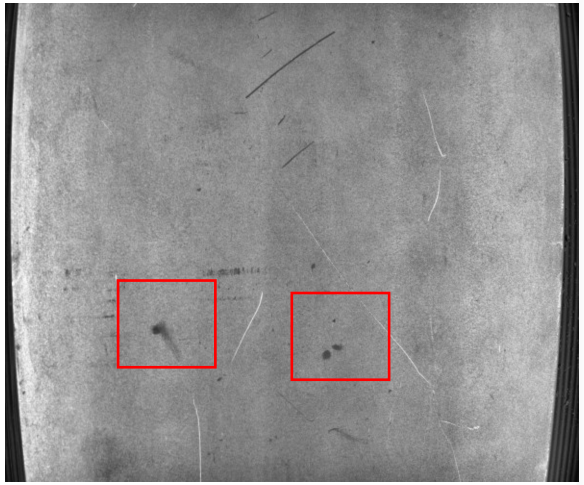
Broker/Machine as a Service



Research Project B: Quality Control with a SME

Metal Surface Defect Detection

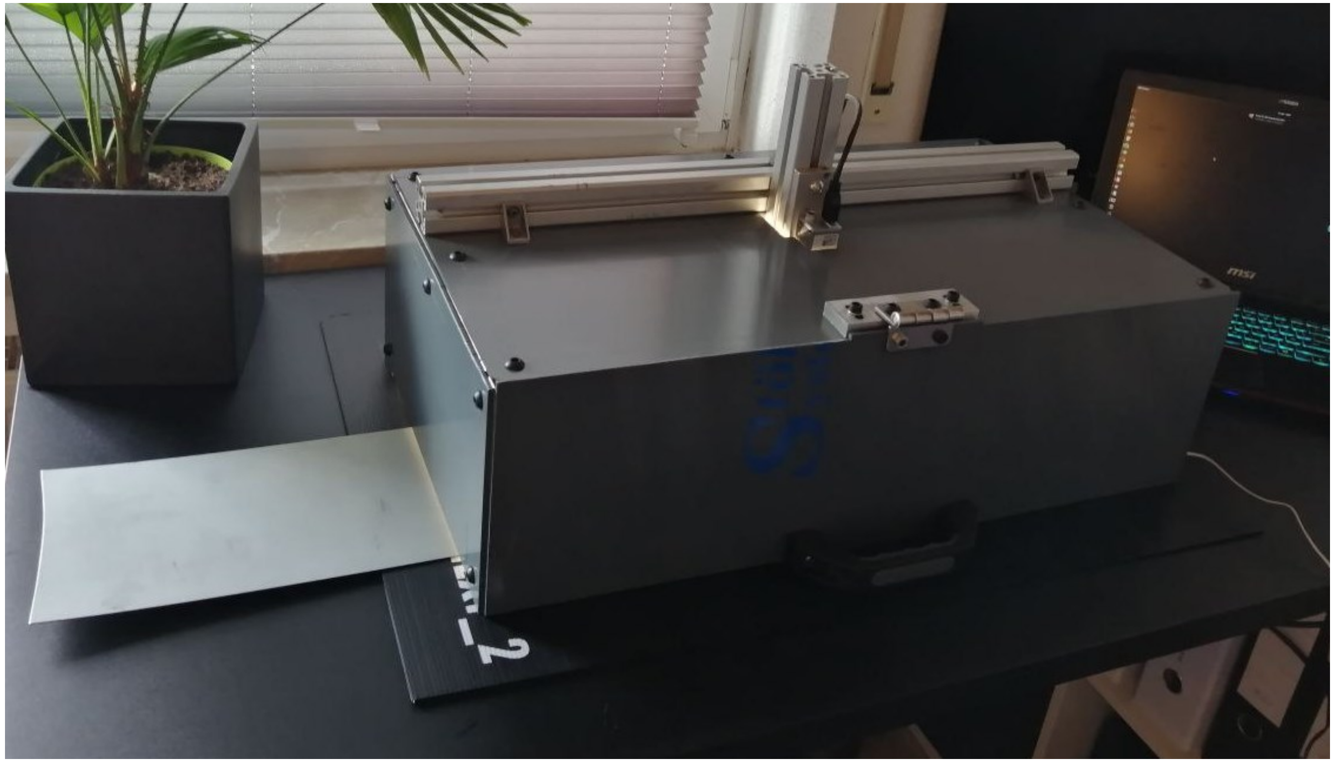
coil

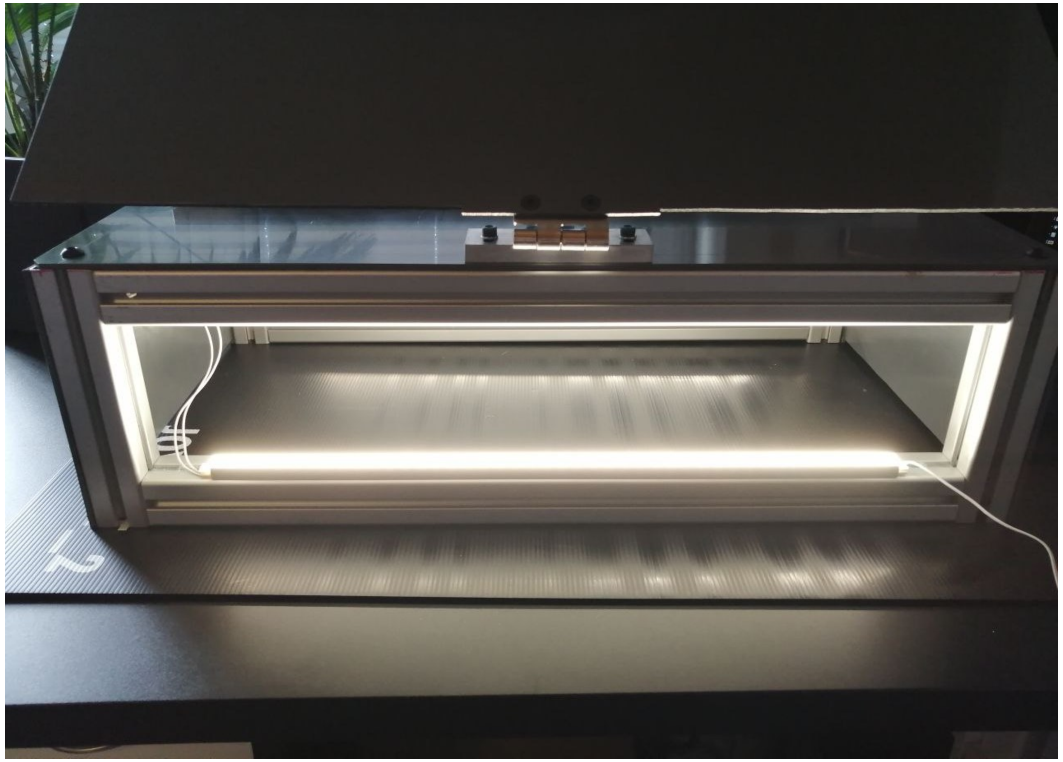


ML Workflow: From Data to Model

Image Collection

First Images, for Proof of Concept

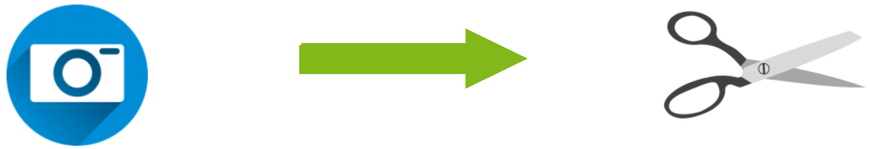




- 109 images 1200x1920px

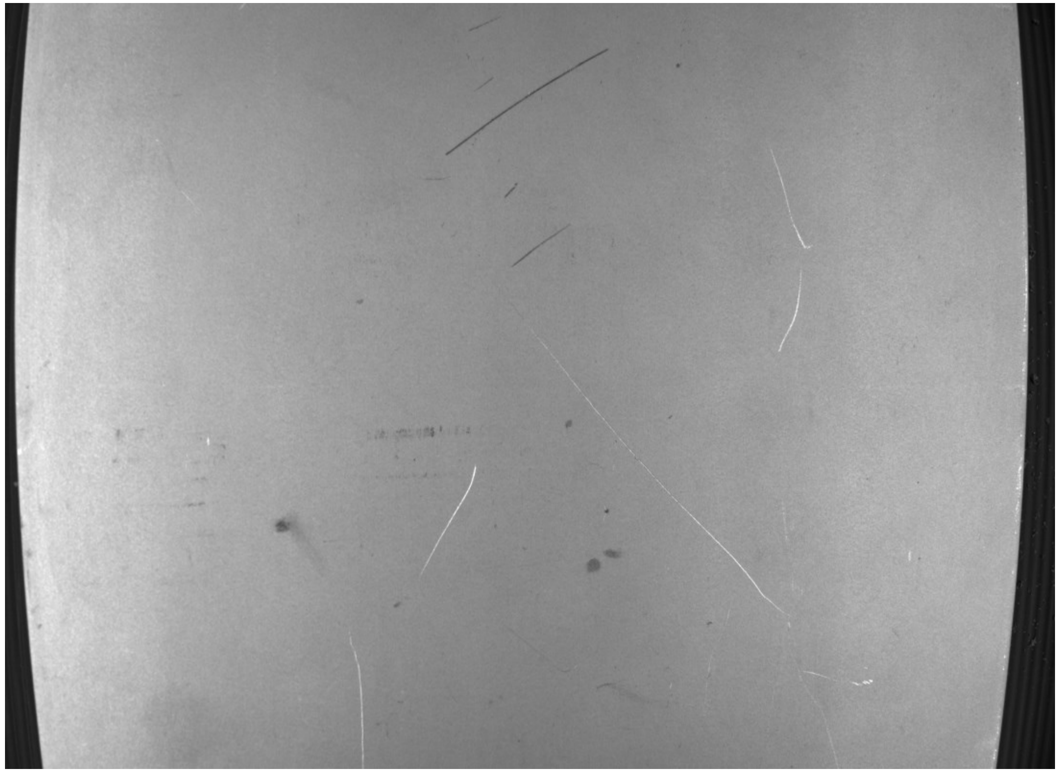
ML Workflow: From Data to Model

Image Collection → **Image Cutting**

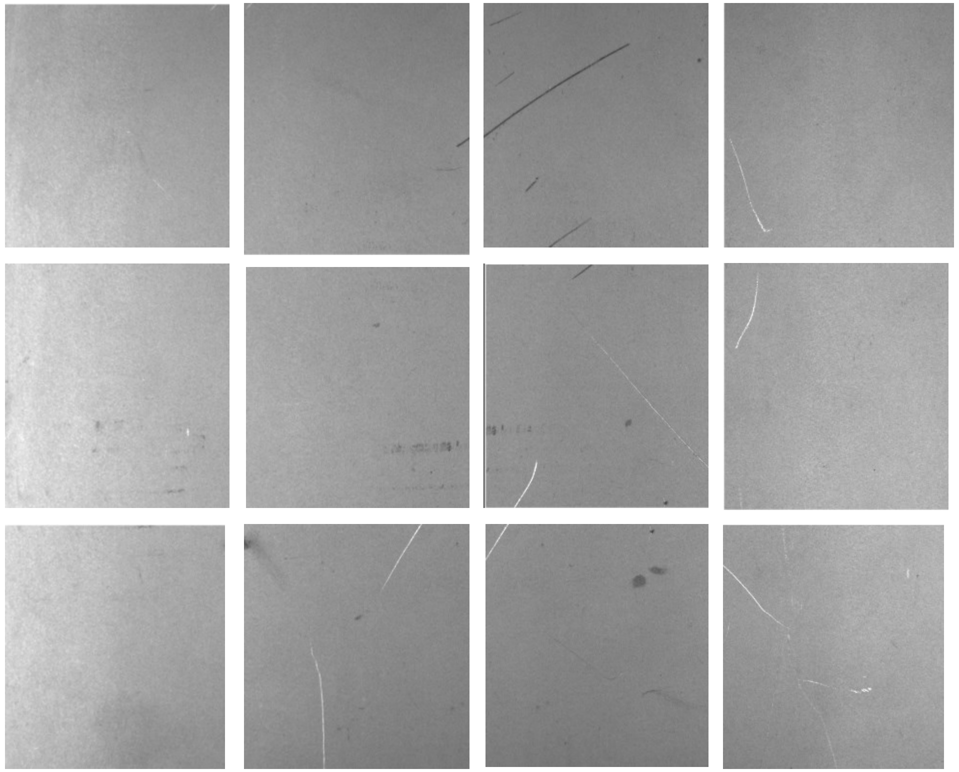


Cutting

- Original image **1920x1200px**



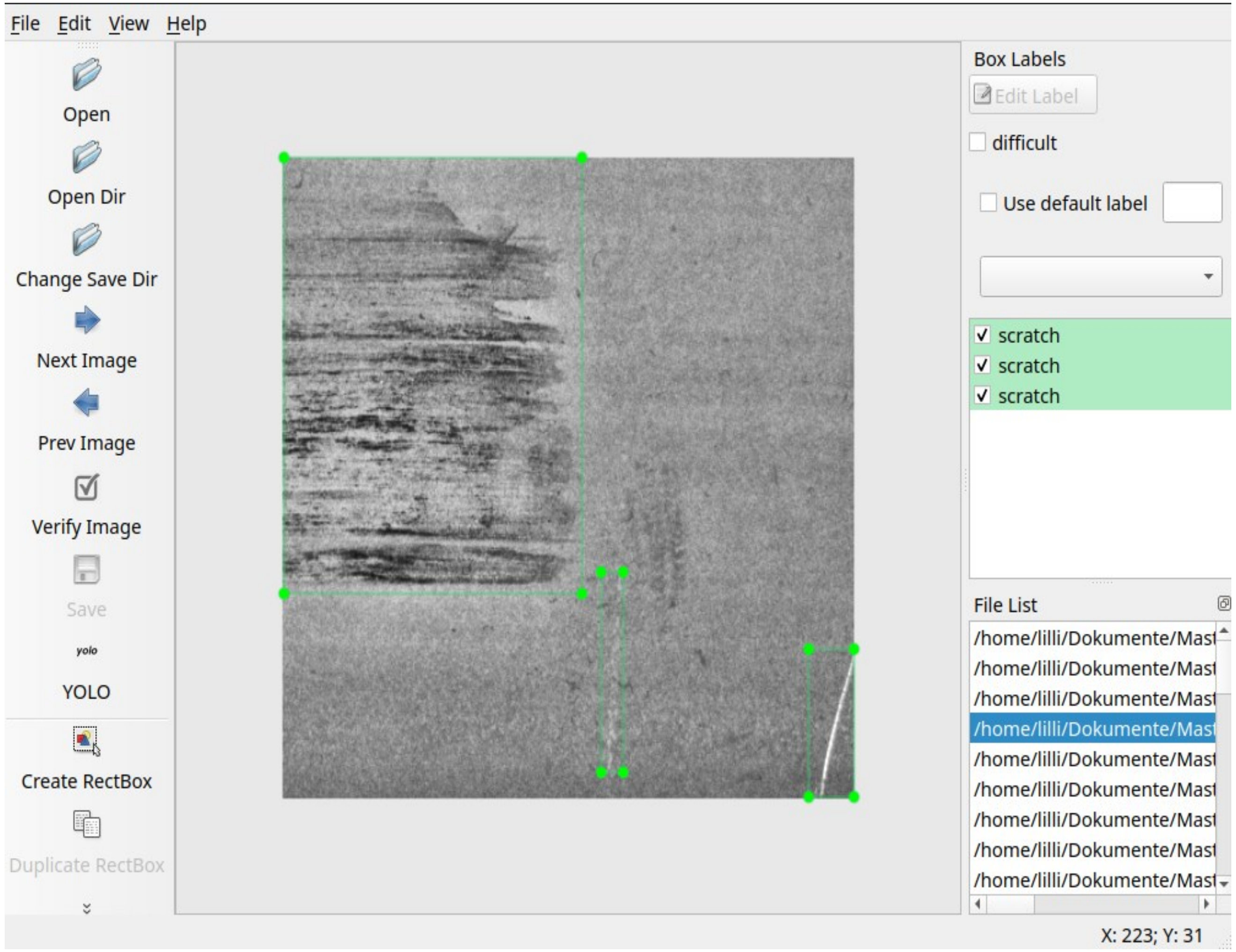
cutting image to **416x416px**



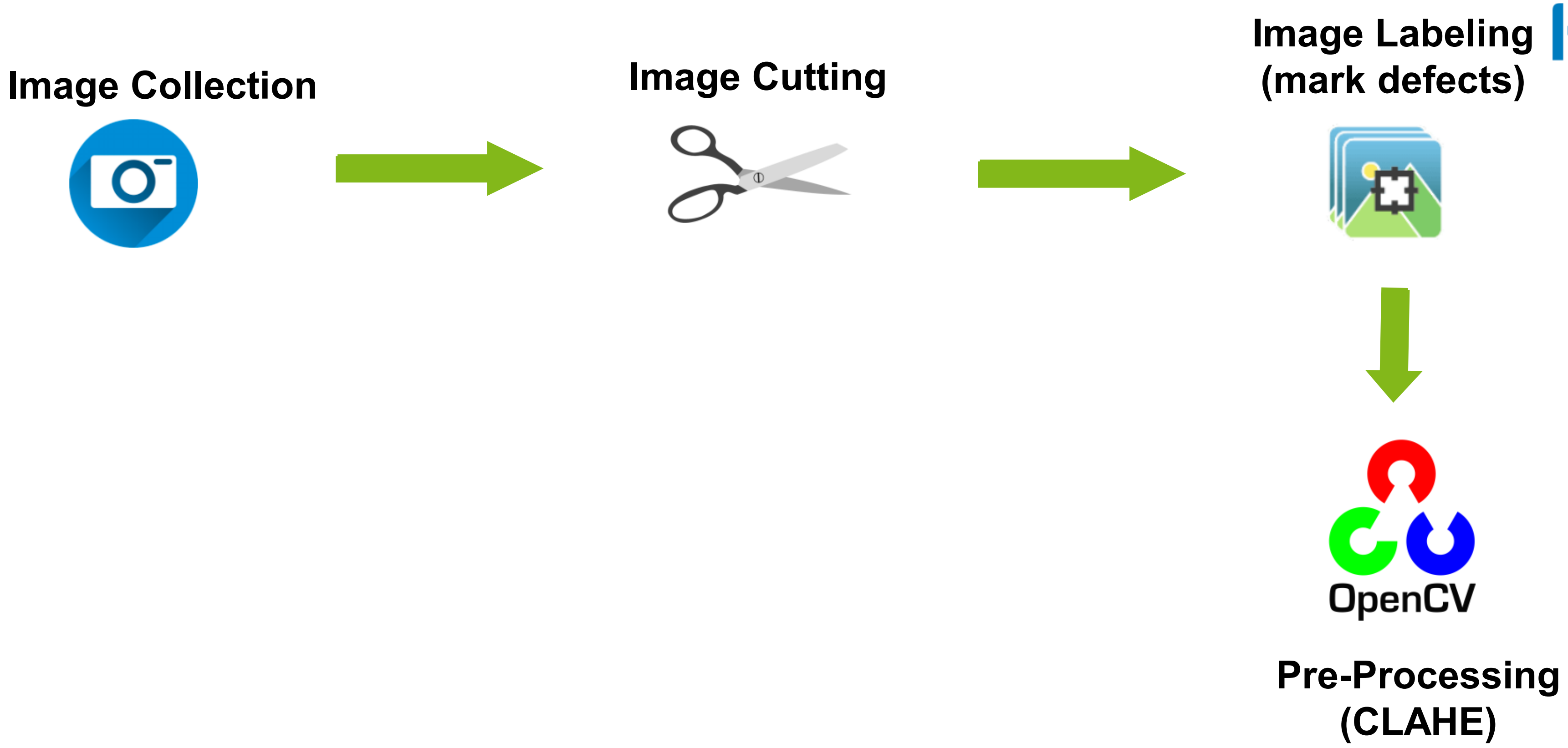
ML Workflow: From Data to Model

Labeling

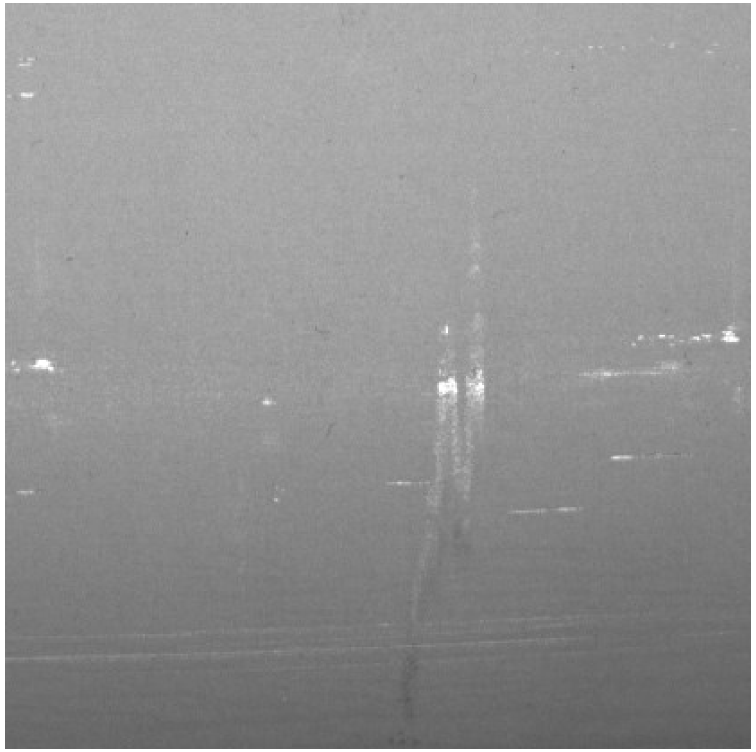
- Marking of defects in the images
- Throw away bad images (e.g. blured images)



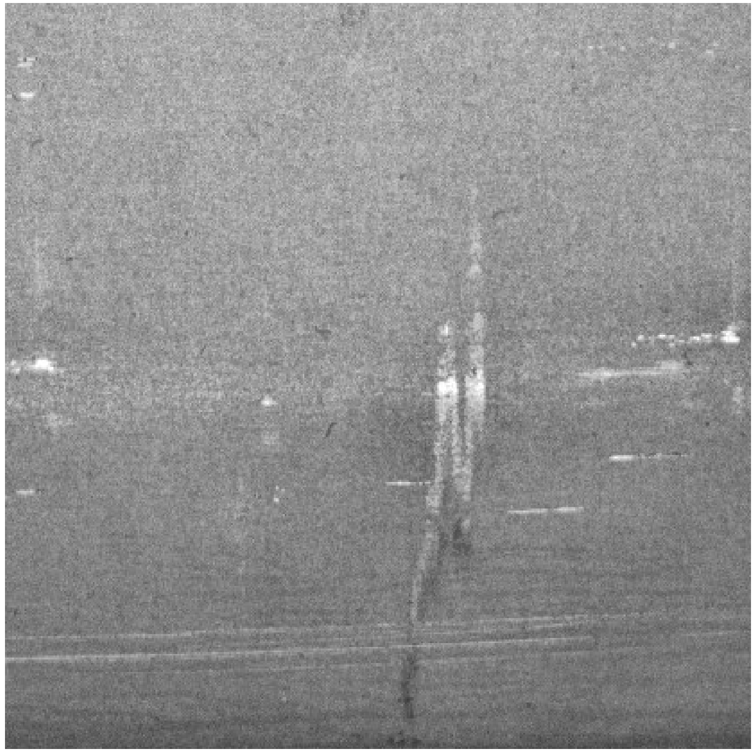
ML Workflow: From Data to Model



Verbesserung durch Datenvorverarbeitung: Contrast Limit Adaptive Histogram Equalization (CLAHE)

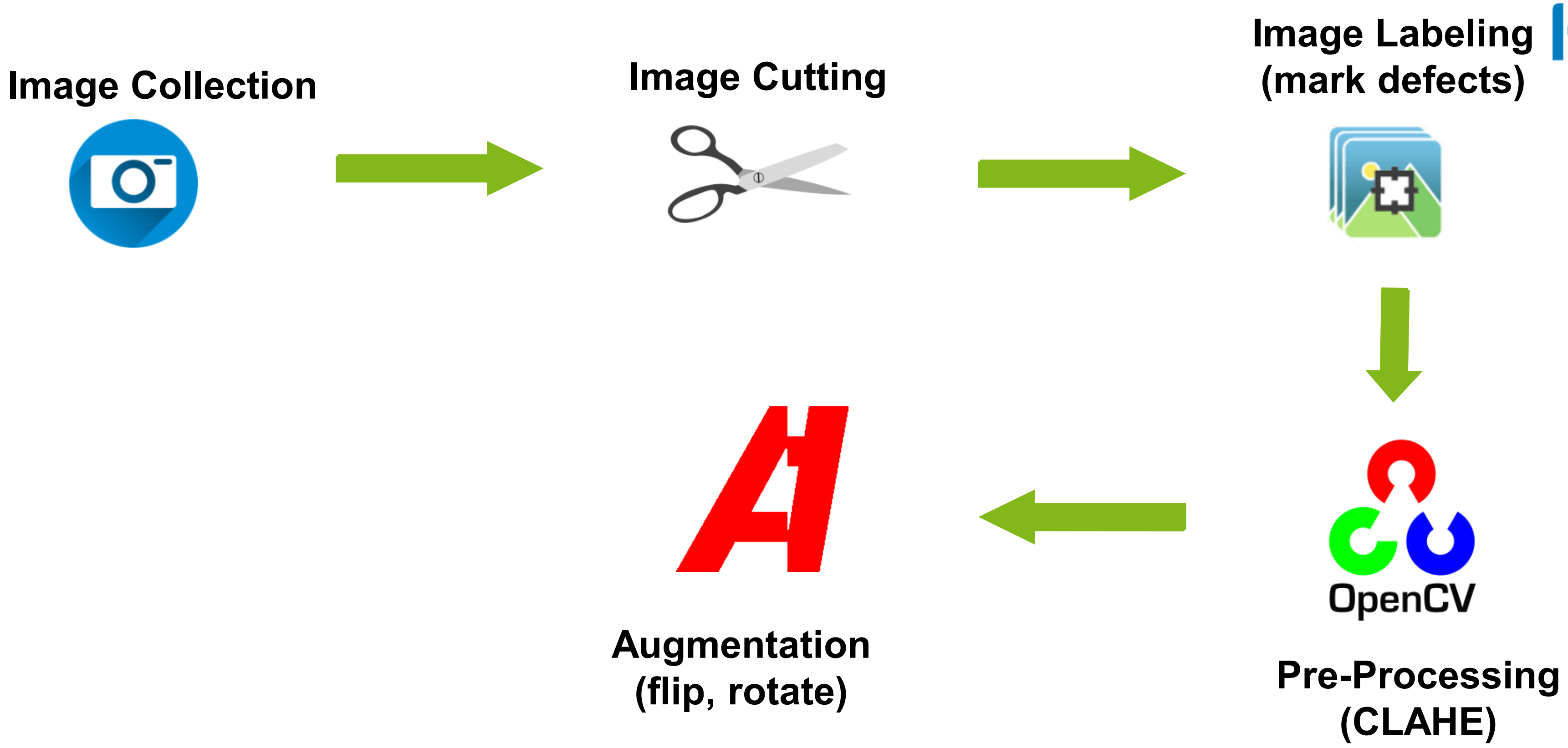


Original



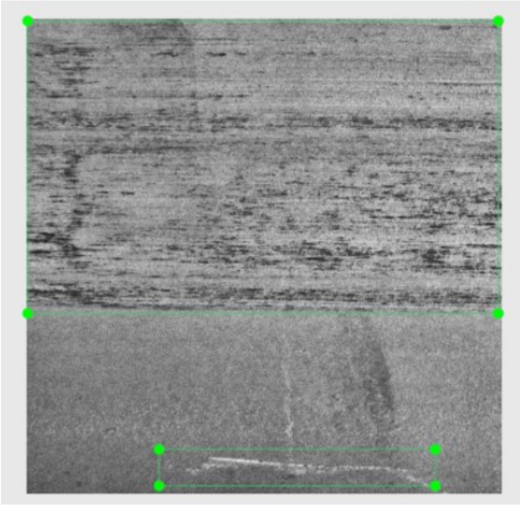
after CLAHE Filter

ML Workflow: From Data to Model

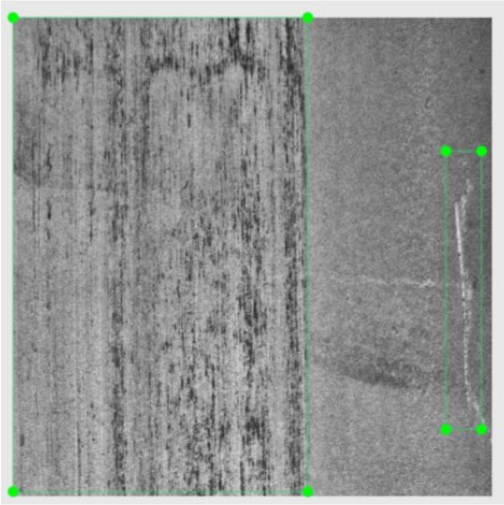


Augmentierung

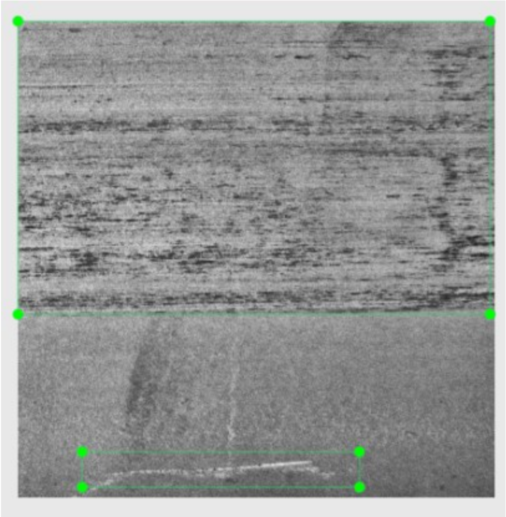
- Für jedes Foto wurden drei weitere Fotos erstellt durch Augmentierung
- Welche Augmentierung dabei verwendet wird, wird per Zufall entschieden
- Durch das Augmentieren mit dem Programm Albuments werden alle Bounding Boxen automatisch mit gedreht / gespiegelt



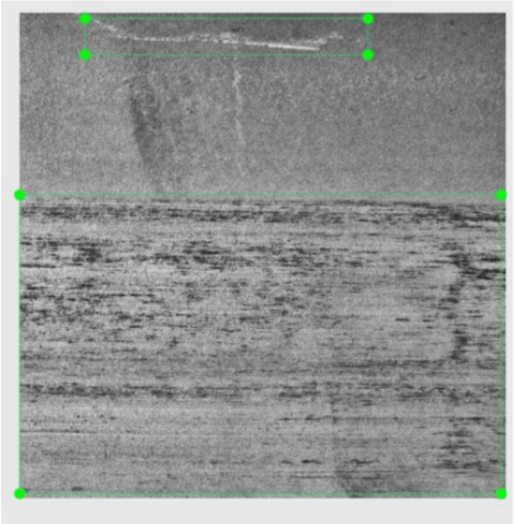
Original



Drehung 270°

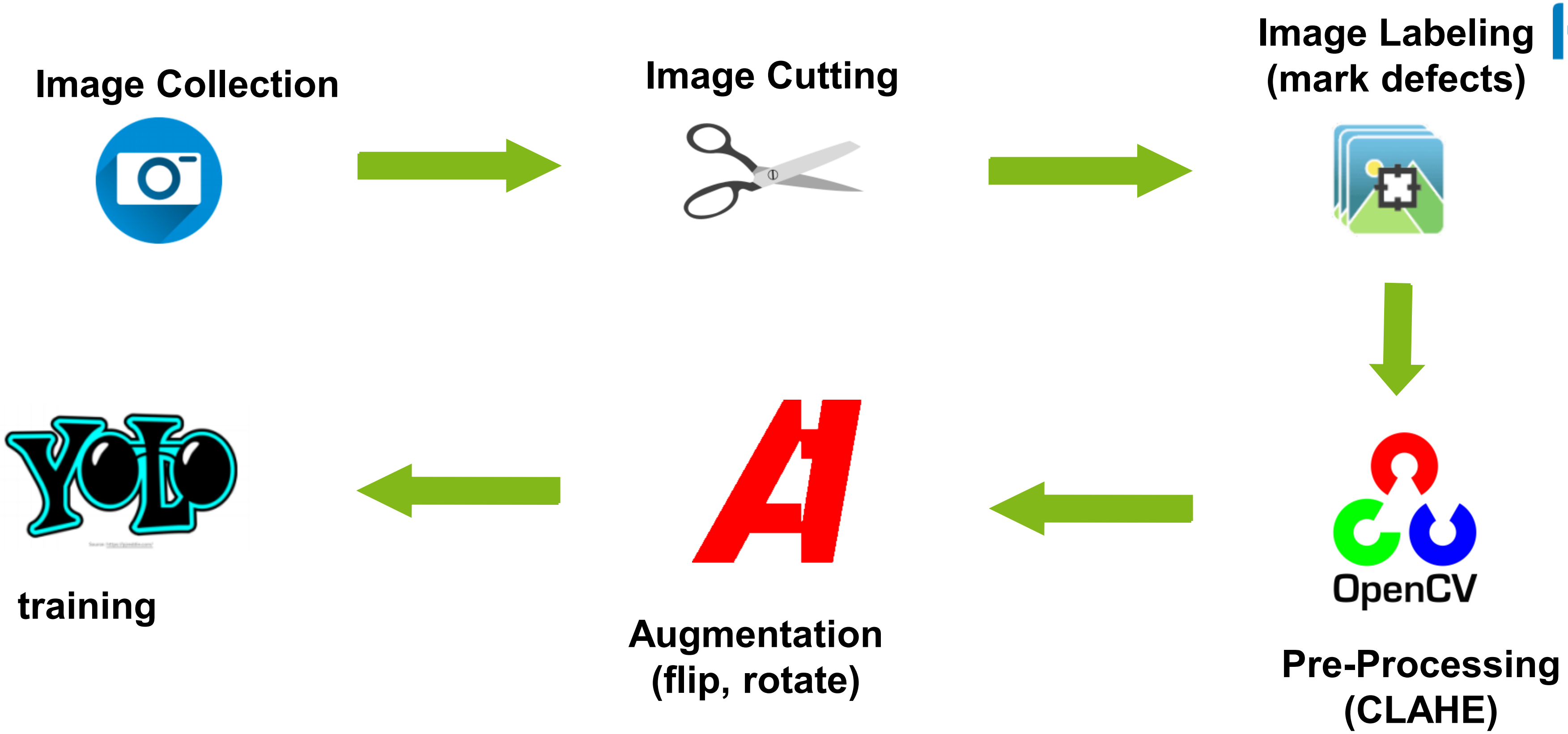


Gespiegelt vertikal



Drehung 180°

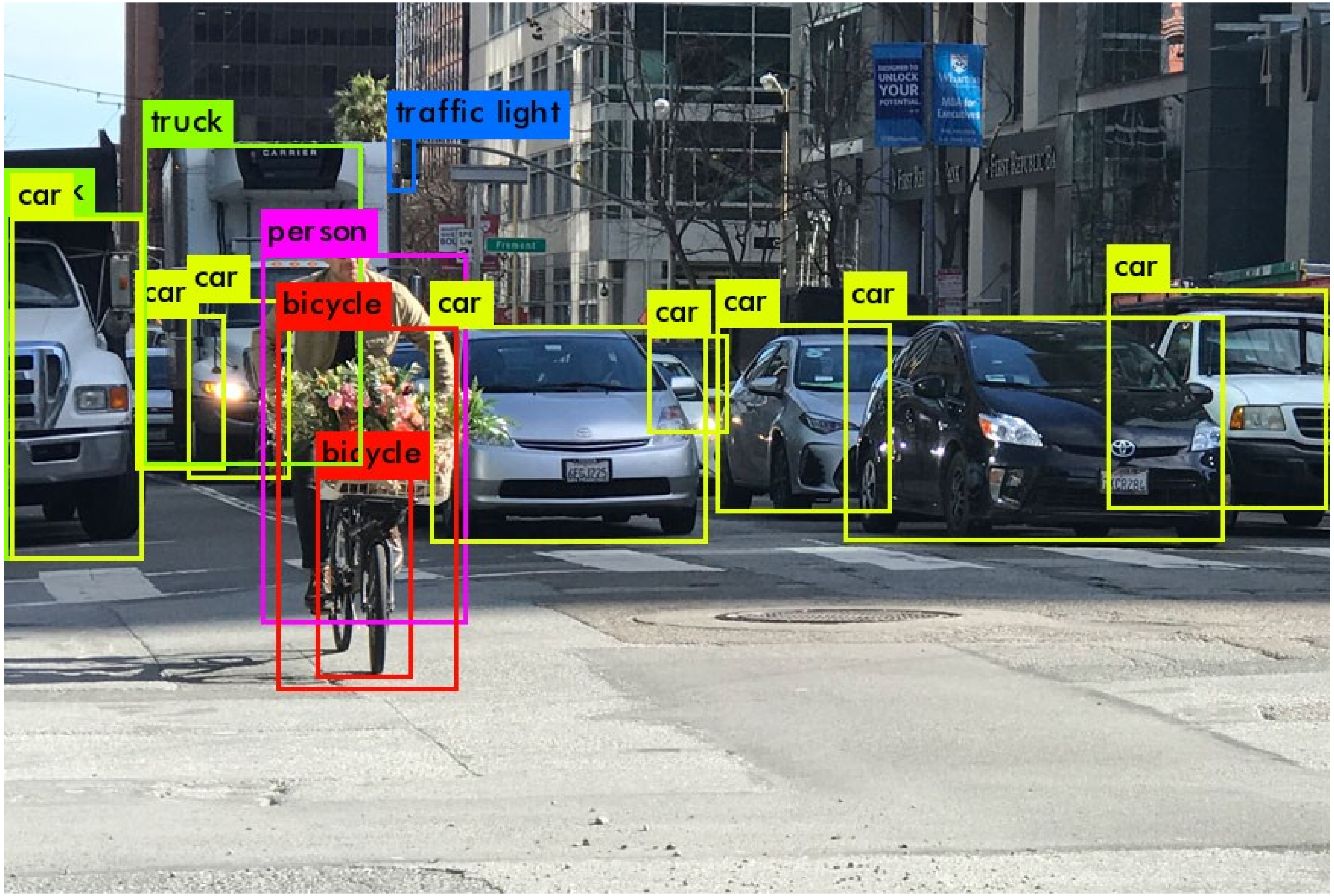
ML Workflow: From Data to Model

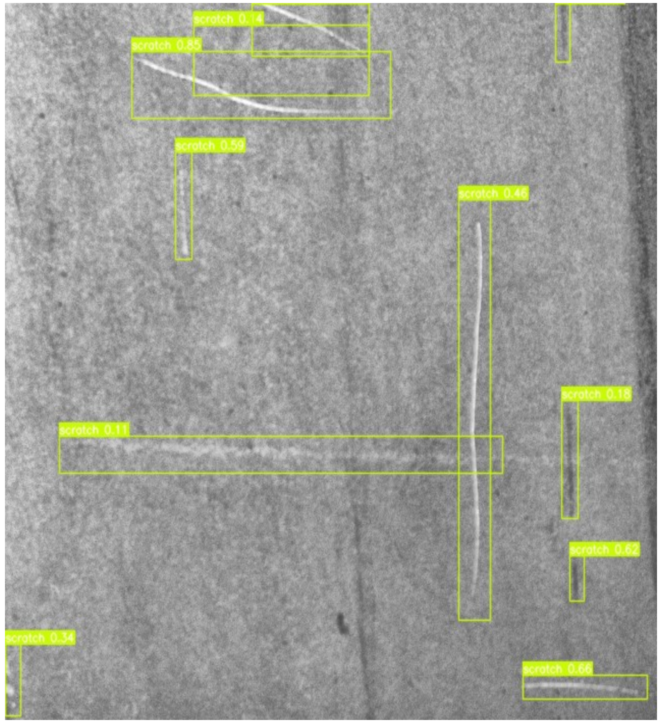


YOLO (You Only Look Once)

HOCHSCHULE FURTWANGEN UNIVERSITY HFU

HMT DIE REINSTE PRÄZISION™

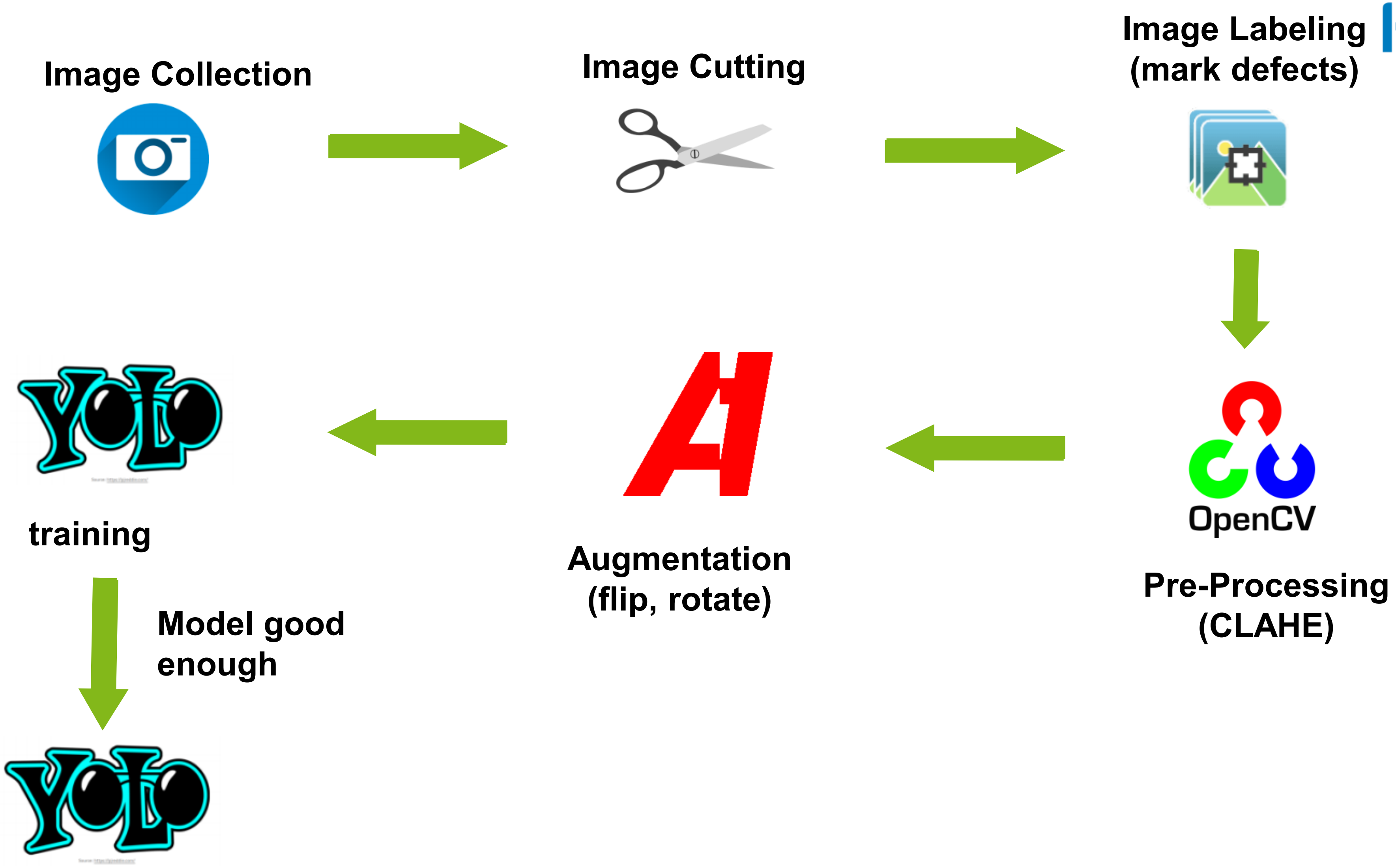




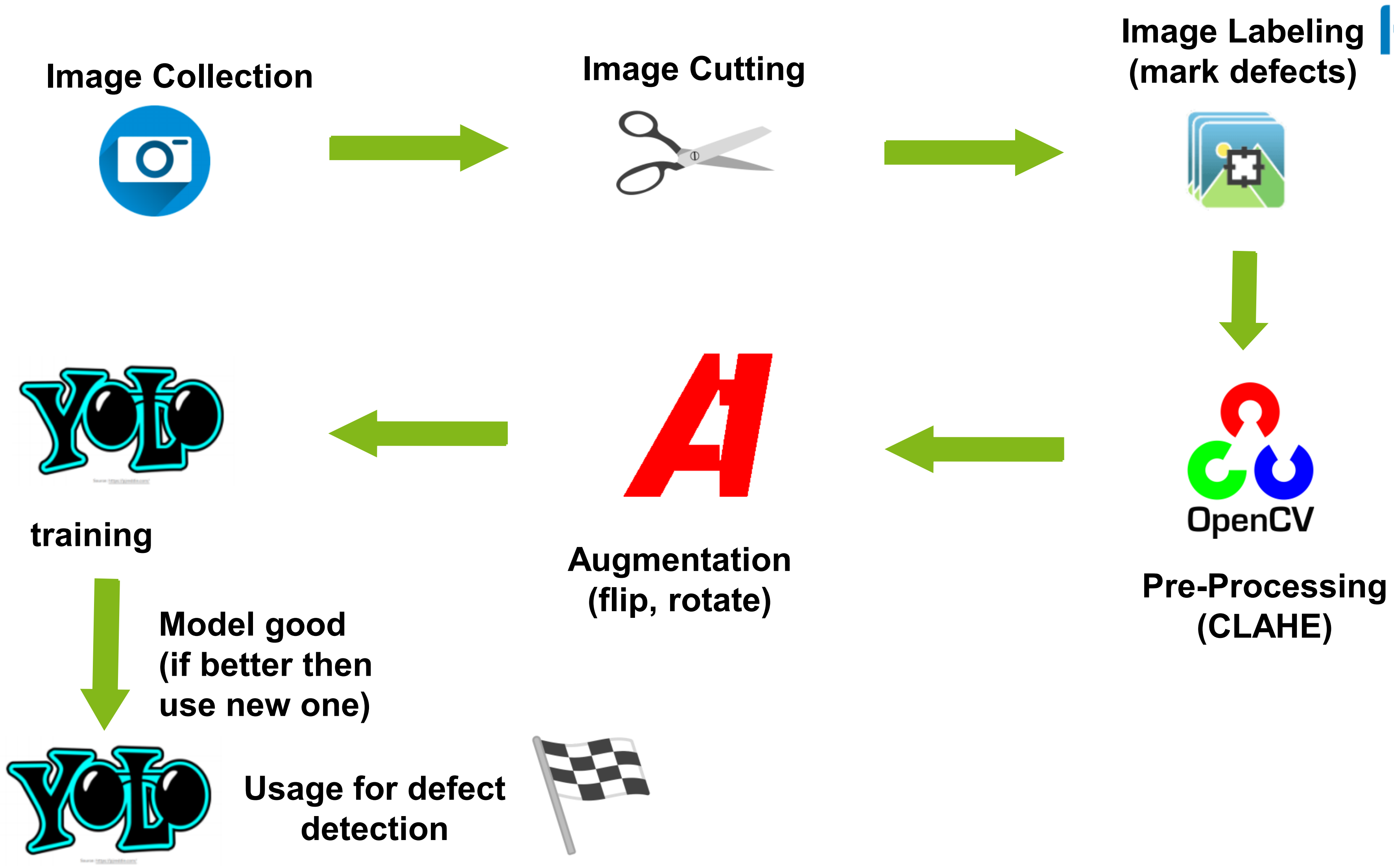
ML Workflow: From Data to Model

HOCHSCHULE FURTWANGEN UNIVERSITY HFU

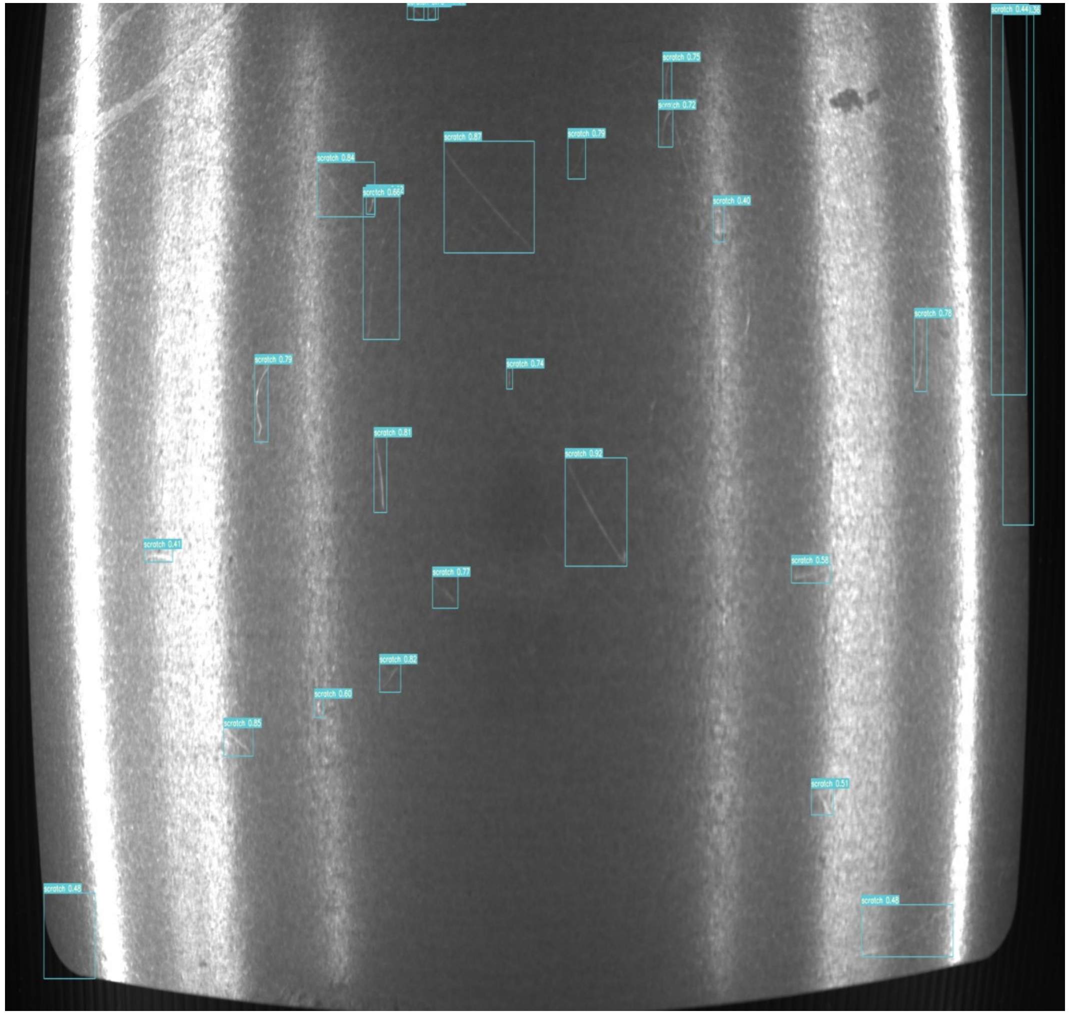
HMT DIE REINSTE PRÄZISION™

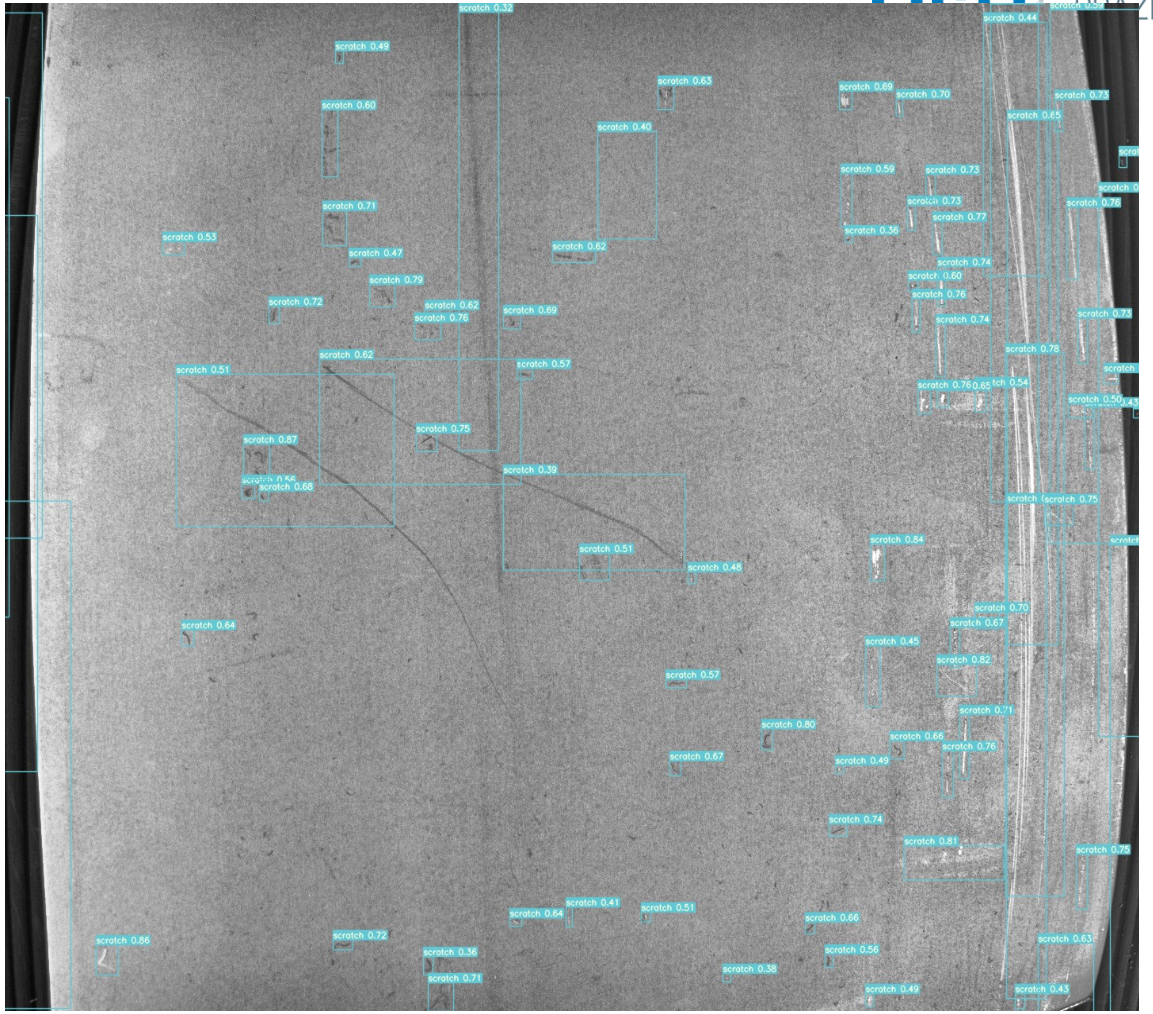


ML Workflow: From Data to Model



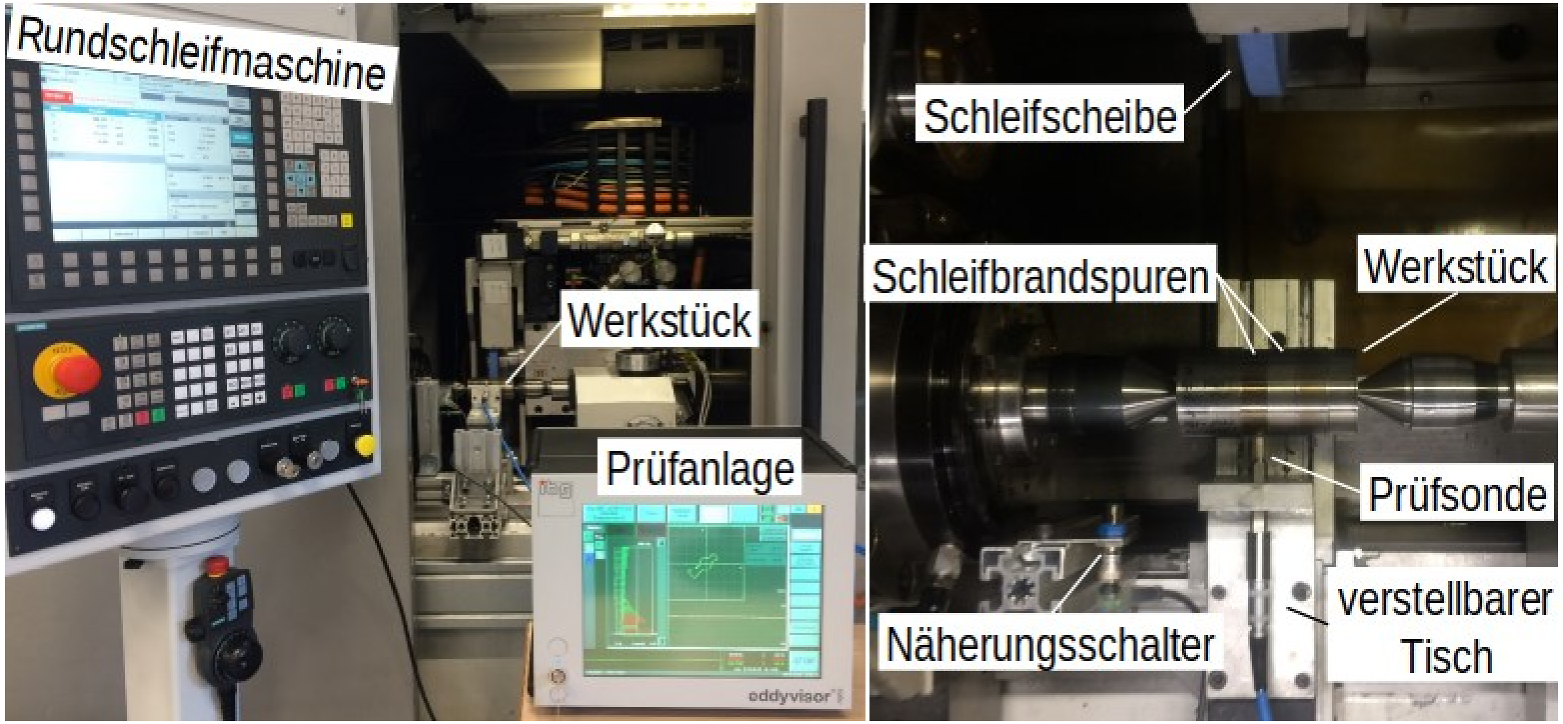
Results





Research Project C: Prozess Optimization

SensorGrind

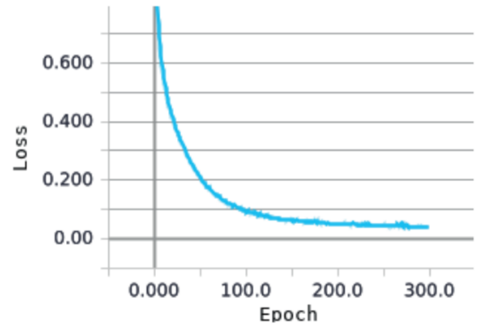


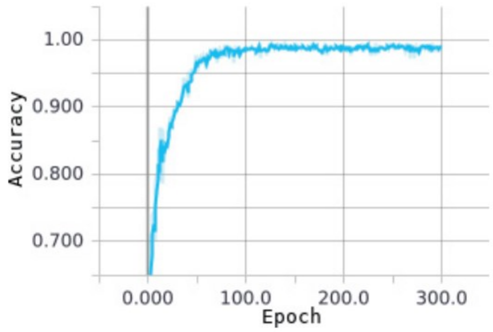
Grind Burn Prediction & Data Augmentation

Smart SysTech 2019 · June 4 – 5, 2019 in Magedeburg, Germany

Grinding Burn Prediction with Artificial Neural Networks based on Grinding Parameters

Christian Reser and Christoph Reich
Institute for Cloud Computing and IT Security
Furtwangen University of Applied Science
Furtwangen, Germany
{christian.reser, christoph.reich}@hs-furtwangen.de

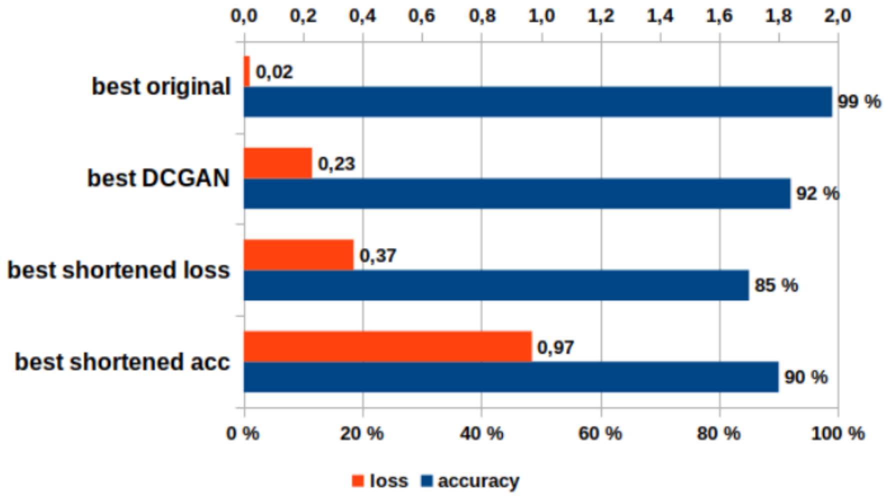




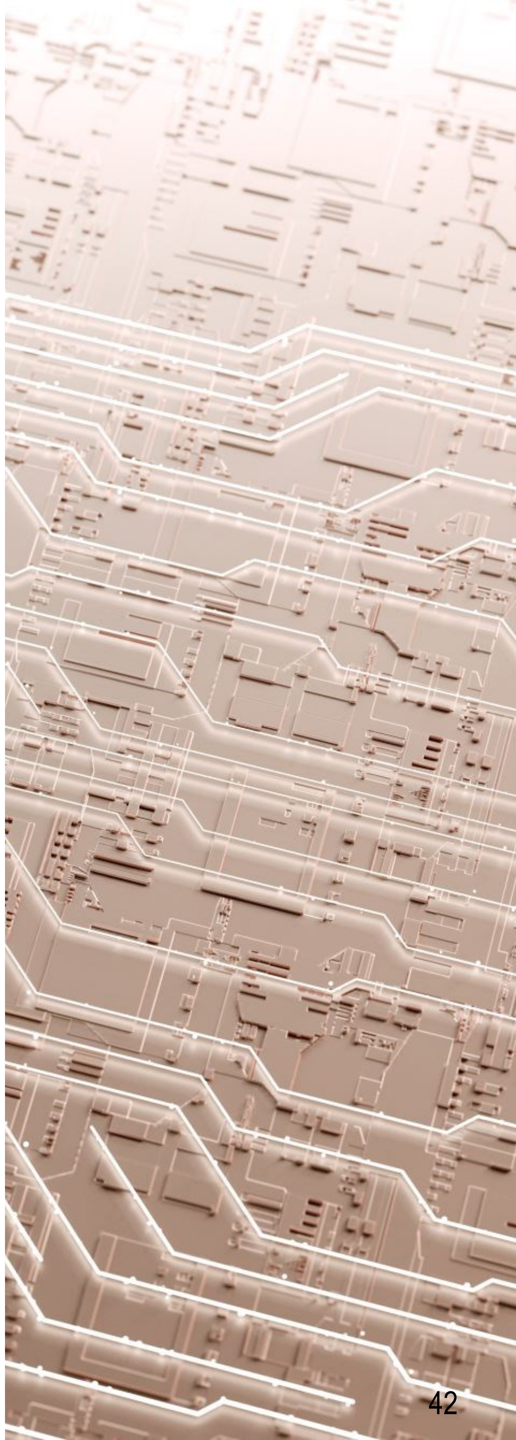
DATA ANALYTICS 2020 : The Ninth International Conference on Data Analytics

DCGAN-Based Data Augmentation for Enhanced Performance of Convolution Neural Networks

Christian Reser and Christoph Reich
Institute for Data Science, Cloud Computing and IT Security
Furtwangen University of Applied Science
Furtwangen, Germany
Email:{christian.reser, christoph.reich}@hs-furtwangen.de



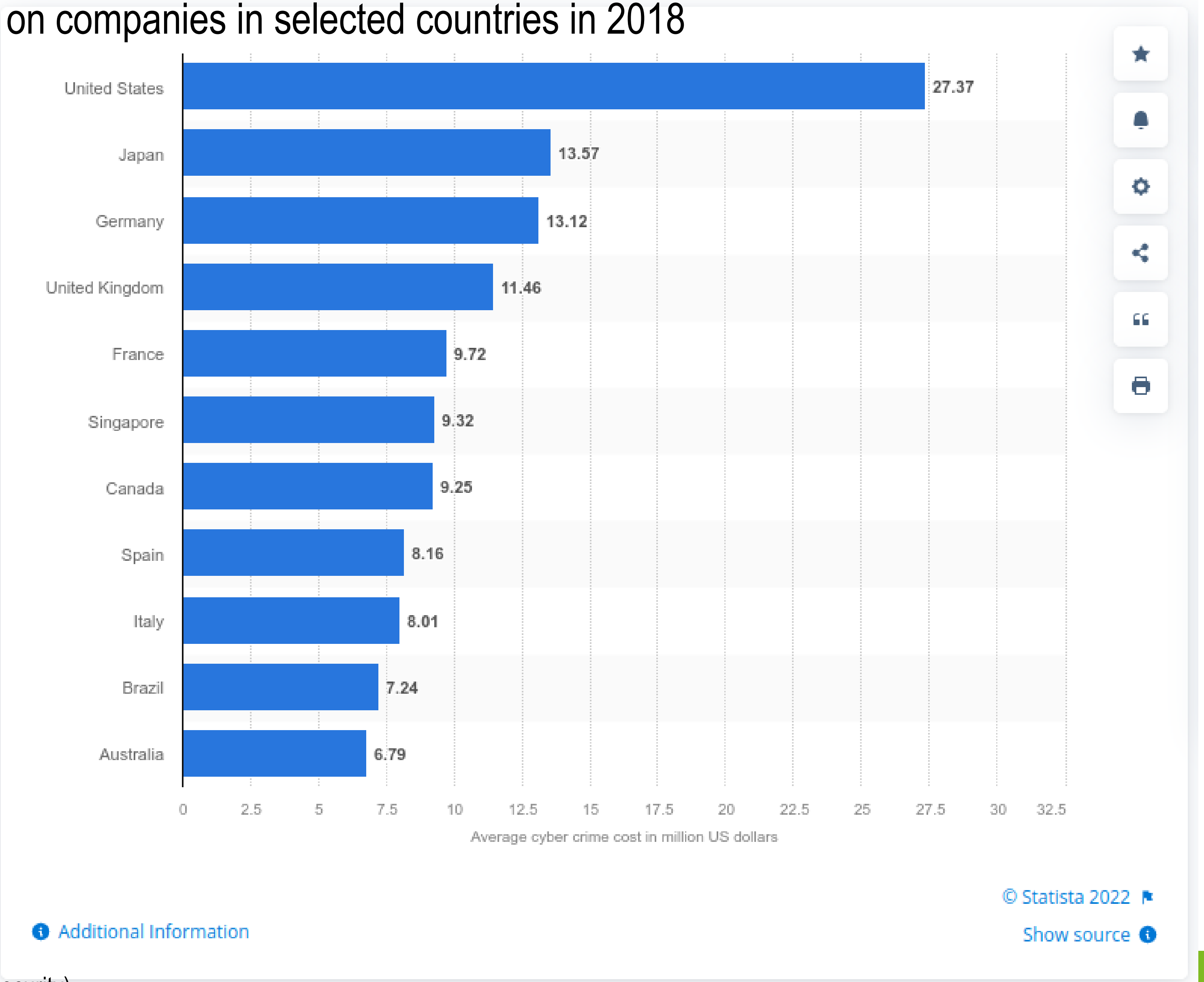
Need for IT Security



Need for IT Security

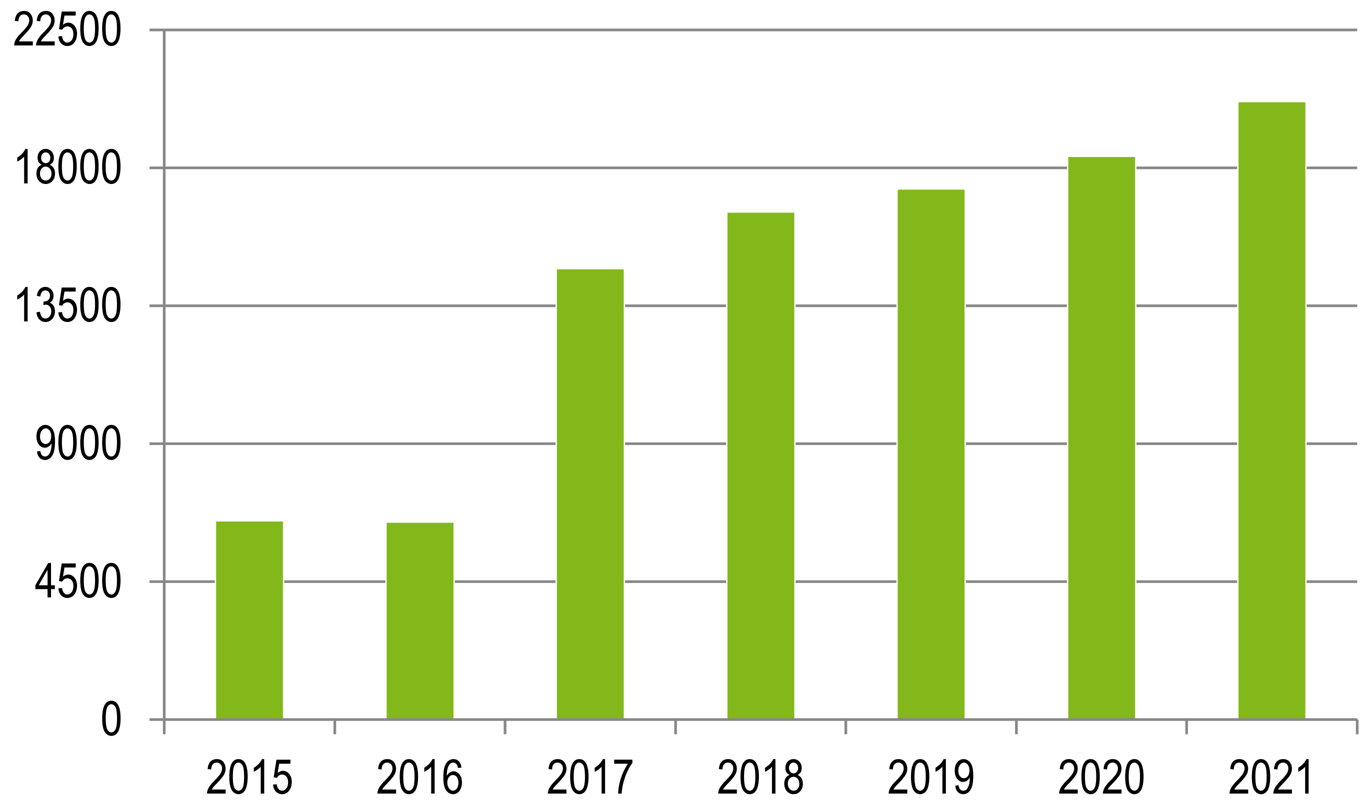
Average annualized cost of cyber attacks on companies in selected countries in 2018

(in million U.S. dollars)



Need for IT Security

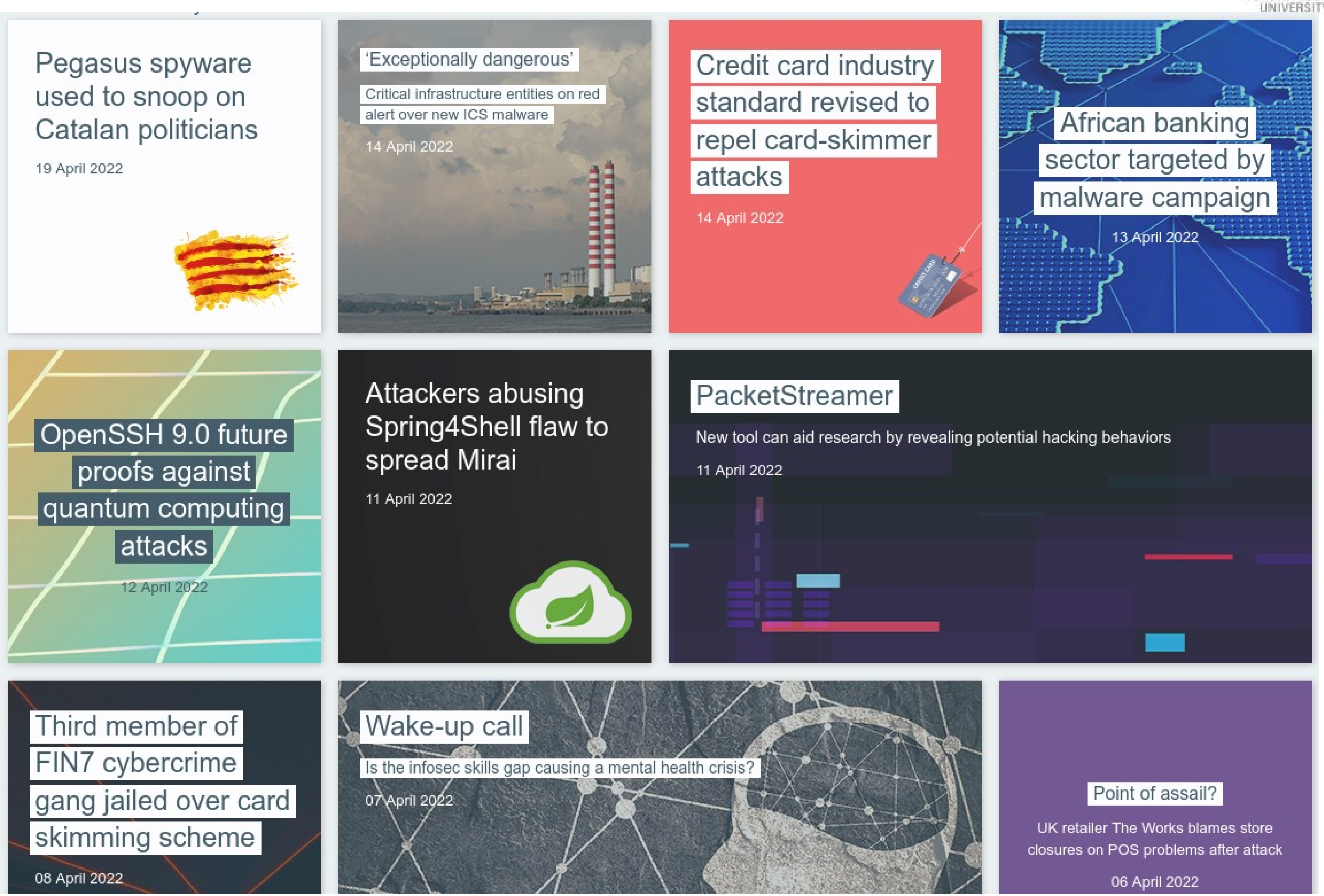
CVE entry of the last years (CVE: security vulnerabilities and Exposures)



https://www.cve.org/About/Metrics#PublishedCVERecords

CVE entry of the last 4 years

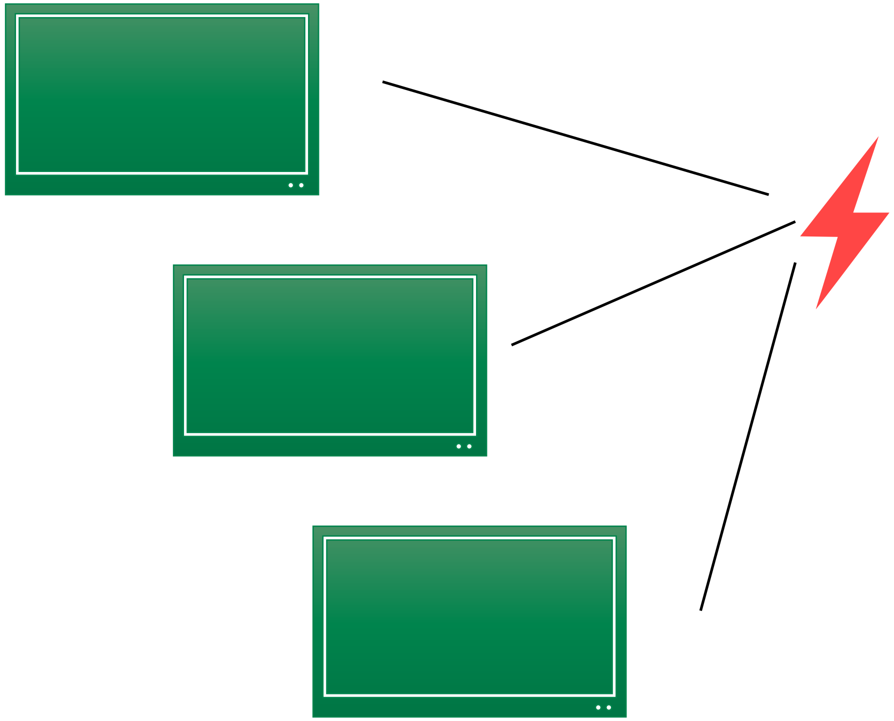
Cyber-attack



https://portswigger.net/daily-swig/cyber-attacks

Known Attacks - Mirai Botnet (Malware)

- Created botnets with everyday objects
  Router, Digital Video Recorder, TVs, etc.
- Standard Passwords have been used
- Goal: DDoS
- 2016: 500.000 IoTs corruped
- It is expected more then 3.000.000 IoTs.



<u>Countermeasures:</u>
No standard password

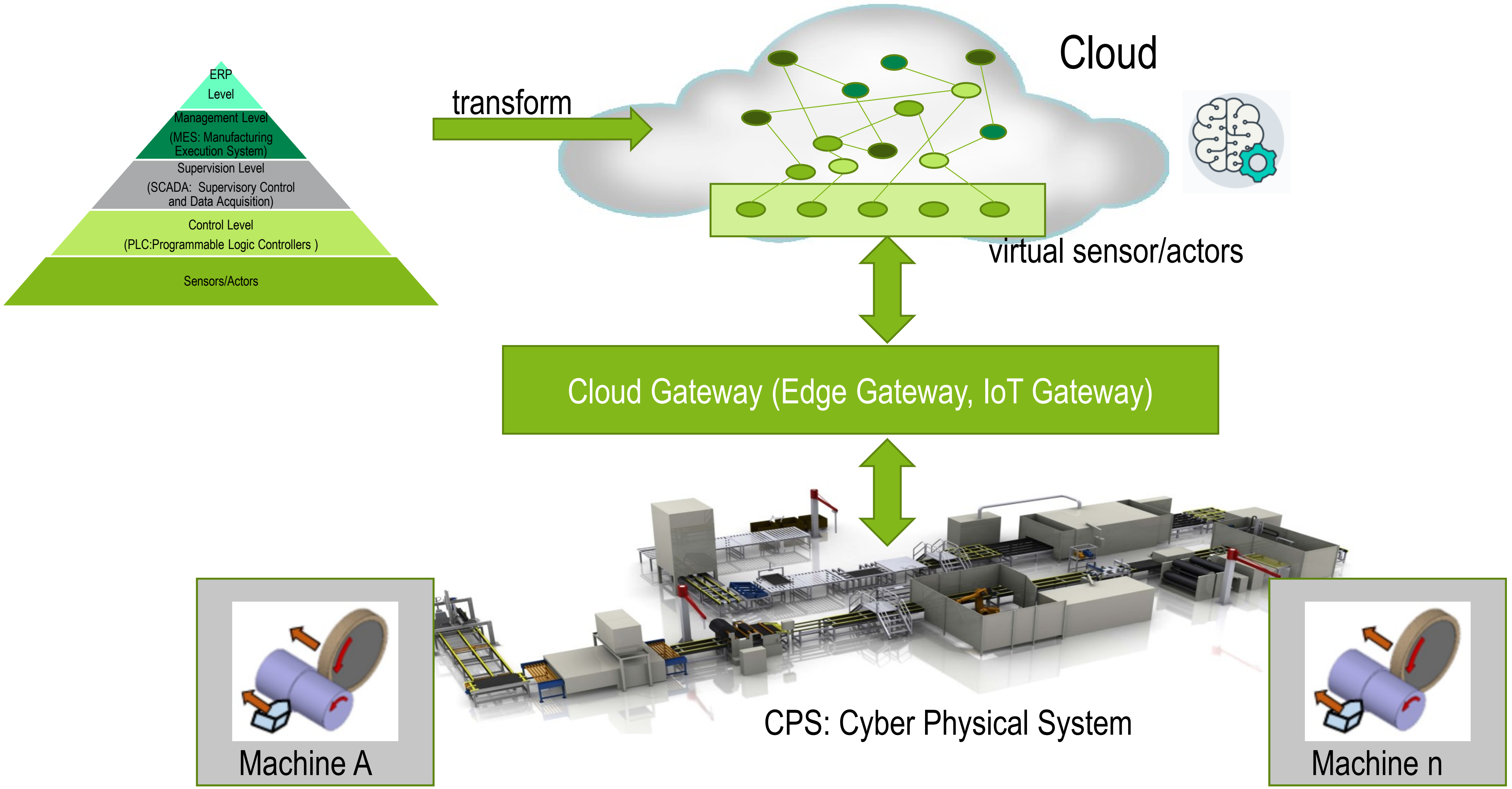
Known Attacks - WannaCry (Ransomware)

- May 2017 - 3 days 300.000 Windows computer in 150 nations
- Crypt data and tried to get ransam money
- <u>Countermeasures:</u>
- 8 weeks before the outbreak, there have been provided a Windows
- Periodical data backup
- Do not open unkown appendix
- Limit or block access to data and systems

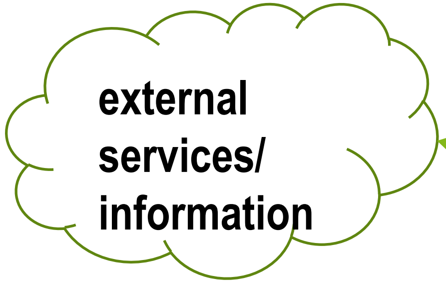
estimated damage billions of dollars

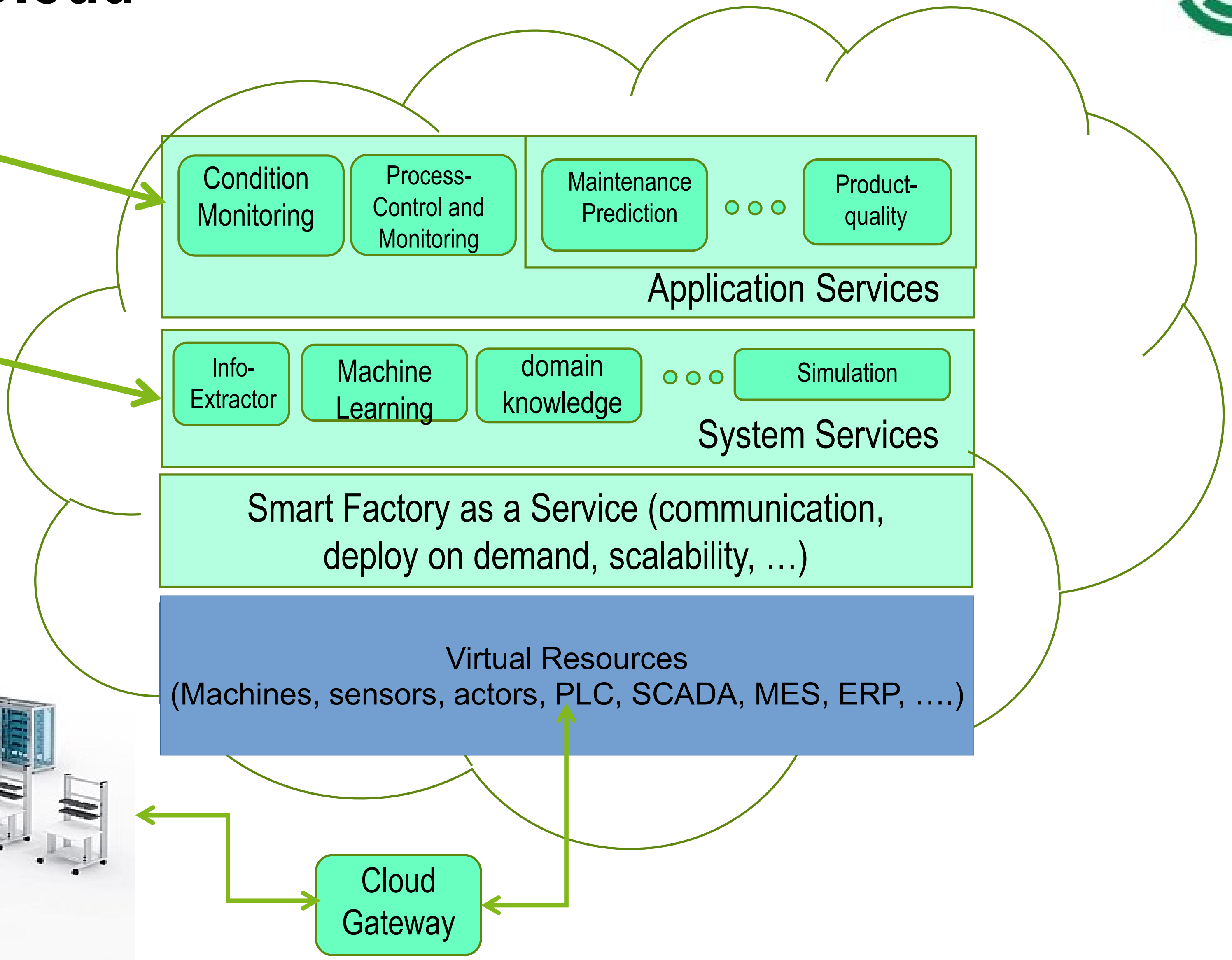
Industry 4.0 Infrastructure Cyber Attacks

Industry 4.0 and Cloud and ML



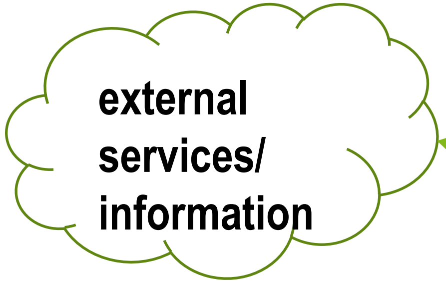
Architecture of Industry Cloud



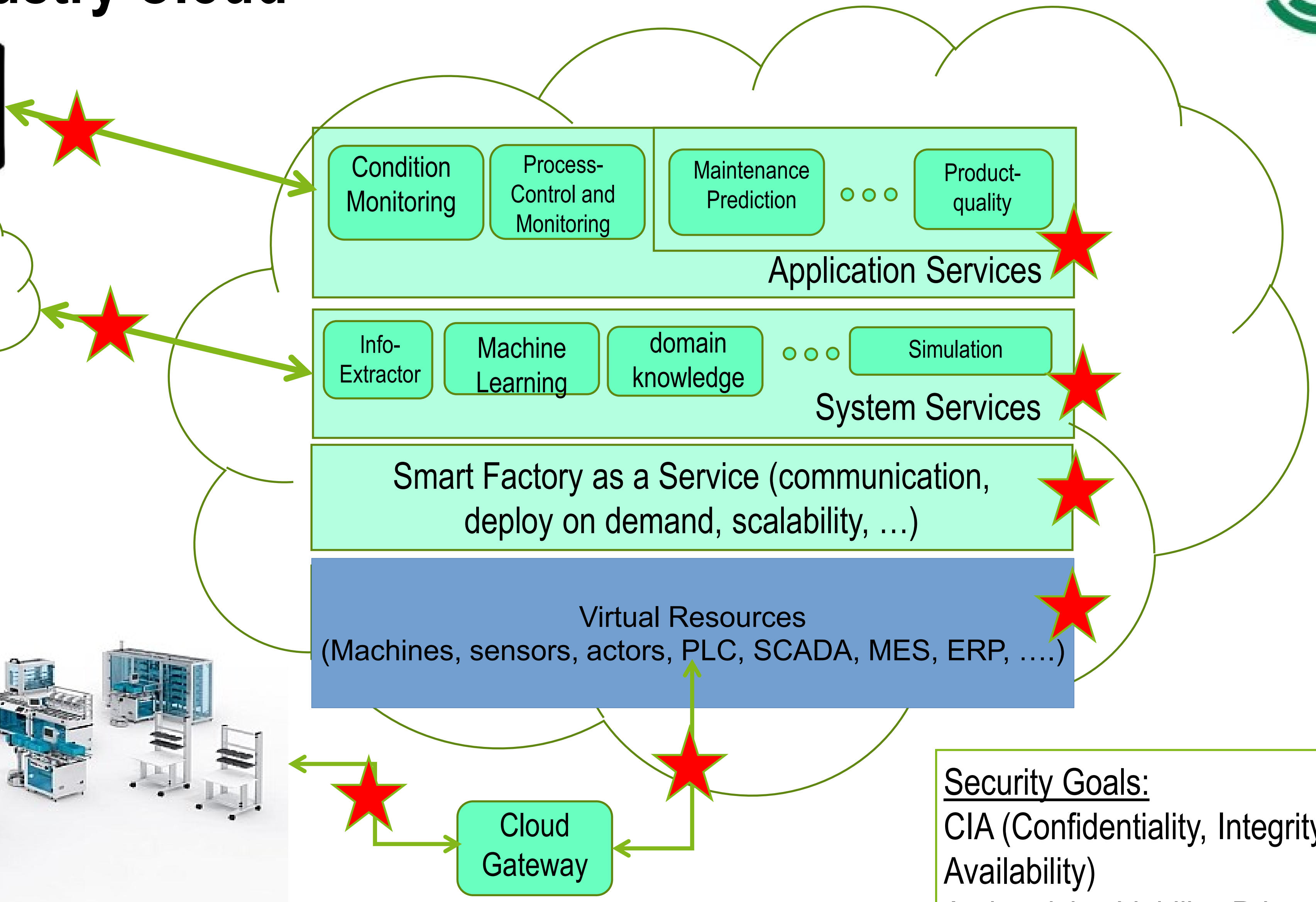


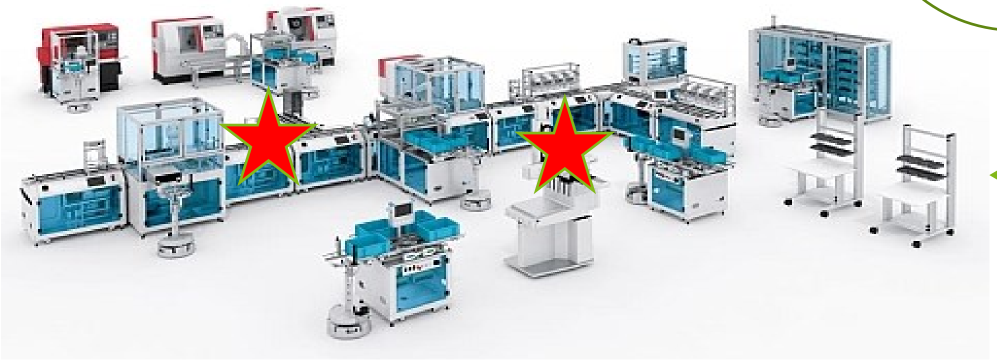
- Attack on a machine
- Attack on communication
- Attack on Cloud infrastructure

Architecture of Industry Cloud



- Attack on a machine
- Attack on communication
- Attack on Cloud infrastructure





<u>Security Goals:</u>
CIA (Confidentiality, Integrity, Availability)
Authenticity, Liability, Privacy

Security Threats of Industry Ecosystems in the Cloud

Exposure	Threat	Impact	Risk	Vulnerability	Mitigation
Infrastructure	Cloud Infrastructure Information Discovery	Low	Middle	Low	User account management, least privilege, periodic audits
	Public Facing Applications	Critical	Low	Low	Firewall, access policies configured carefully
	Patch Deficit	Critical	Middle	Probable	Continuous patch management
	Denial of Service	Middle	Middle	-	Firewall, DDoS protection services
	Malware	Critical	Middle	Probable	Malware detection, awareness training
	SCADA System Attack	Critical	Middle	Probable	Least privilege, periodic audits, network segmentation
Human	Social Engineering	Critical	Critical	Probable	Awareness training, behavior anomaly detection, least privilege
	Identity Spoofing	Critical	Critical	Low	2 factor authentication, identity fraud detection, physical key cards
	Misconfiguration	Critical	Critical	Low	4-eyes configuration, periodic audits, config file validation
Business	Faulty Defined KOSMoS Contract Tempate	Critical	Low	Low	Carefully defined templates by experts
	Service Provider Manipulates Data	Critical	Low	Low	Audit data collector securely connected to blockchain
	Error in Data Collection	Probable	Low	-	Monitoring, anomaly detection
	Contract Manipulation	Critical	Low	-	Blockchain nodes must have consensus for contract changes
Use Case (Infrastructure Specific)	Denial of Service	Low	Low	-	Data caching on premise
	Malware	Middle	Middle	Probable	Male detection, awareness training
	Application Disguising	Critical	Low	Low	Audit container image before publishing
	Man in the Middle	Critical	Low	Probable	Message encryption and authentication (certification)
	Non Compliance	Critical	Low	Low	Anonymization
	Edge Misconfiguration	Critical	Middle	-	4-eyes configuration, periodic audits, config file validation
Use Case (Human Specific)	Social Engineering	Critical	Low	Probable	Awareness training, behaviour anomaly detection, least privilege
	Identity Spoofing	Critical	Low	Low	2 factor authentication, identity fraud detection, physical key cards
	Inside Attacker	Critical	Middle	-	Intrusion detection system, network segmentation, least privilege
Use Case (Business Specific)	Sensor Data Manipulation	Middle	Low	-	Monitoring, anomaly detection
	Smart Contract Manipulation	Critical	Low	Low	Blockchain nodes must have consensus for contract changes
	Machine Usage Data Manipulation	Middle	Middle	-	Periodic audit, data caching, anomaly detection
Smart Contract	Non-Determinism	Middle	Middle	Low	Smart contract scanner, programming specific linting tools, Hyperledger Fabric architecture
	External Stateful Services	Critical	Middle	Low	Blockchain oracle that acts as intermediary / caching
	Input Validation / Error Handling	Critical	Middle	Probable	Input validation, strict error handling / safe error behaviour

Security Threats of a Blockchain-Based Platform for Industry Ecosystems in the Cloud

Philipp Ruf*, Jan Stodt*, Christoph Reich*
*Institute for Data Science, Cloud Computing and IT-Security (IDACUS) –
Furtwangen University of Applied Science, Furwangen, Germany
Email: {philipp.ruf, jan.stodt, christoph.reich}@hs-furtwangen.de

***Abstract*—In modern industrial production lines, the integration and interconnection of various different manufacturing components, like robots, laser cutting machines, milling machines,**

and executions implemented as smart contracts. While the BC itself must be generally secure, the security requirements for the broad KOSMoS ecosystem which feeds the BC and

False Data by Accident/Purpose?

Uber's Self-Driving Car

Problem:

- Sensor has been replaced
  ⇨ protect identity
- Sensor is highjacked and delivers wrong data
  ⇨ check data plausibility
- Data integrity violation during transport
  ⇨ secure data transport

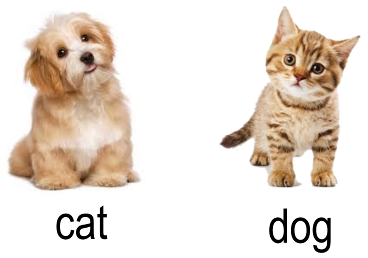
What is detected?

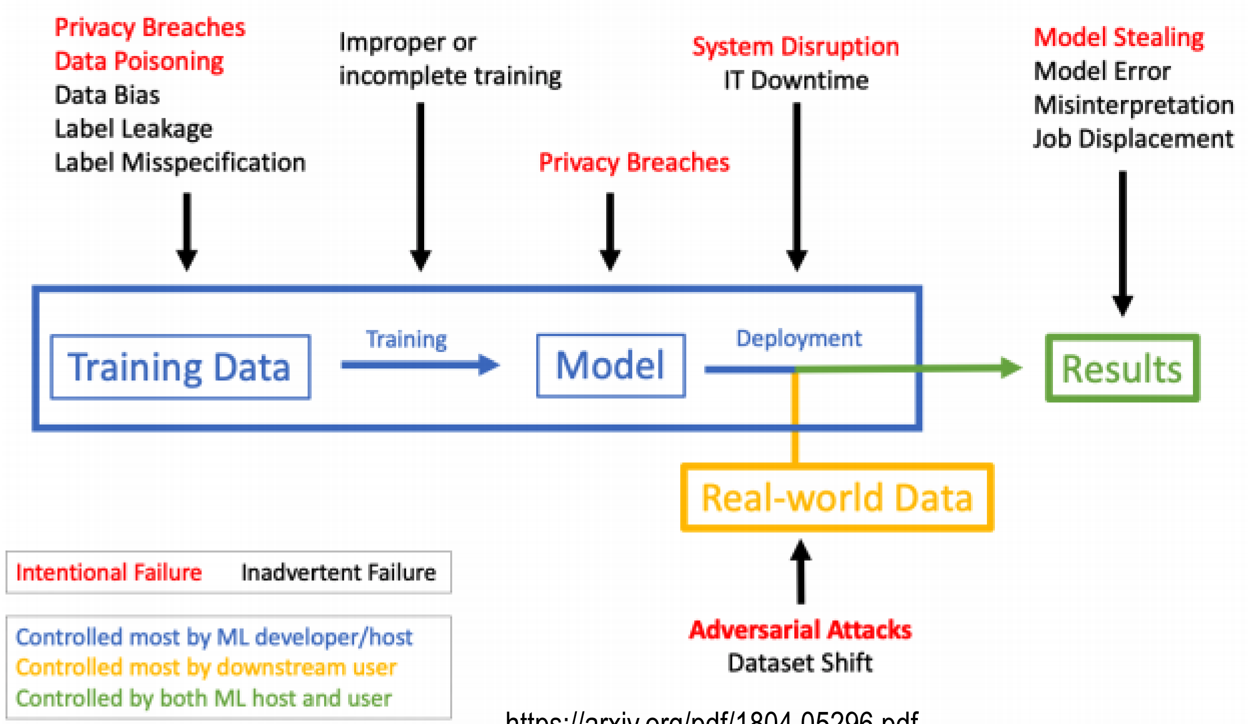
Scene A:

Scene B:

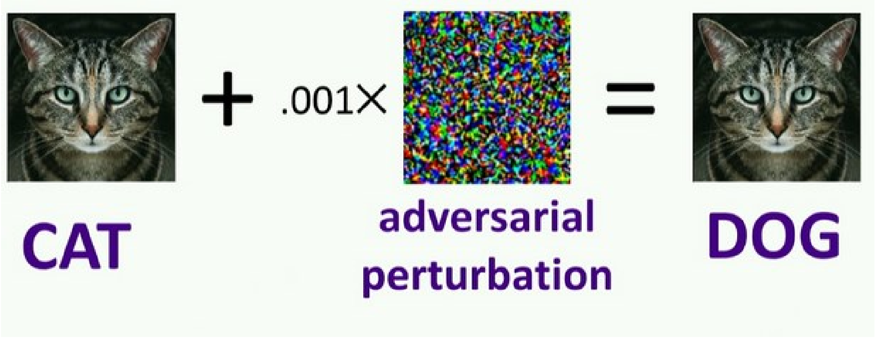
Adversarial Attacks Against Machine Learning

- Label Manipulation (e.g. Flipping Label)
- Backdoor Poisoning (e.g. hidden trigger)





https://arxiv.org/pdf/1804.05296.pdf



Counter Measurement: Distributed Data Validation Networks

Context-Aware Anomaly Detection for the Distributed Data Validation Network in Industry 4.0 Environments

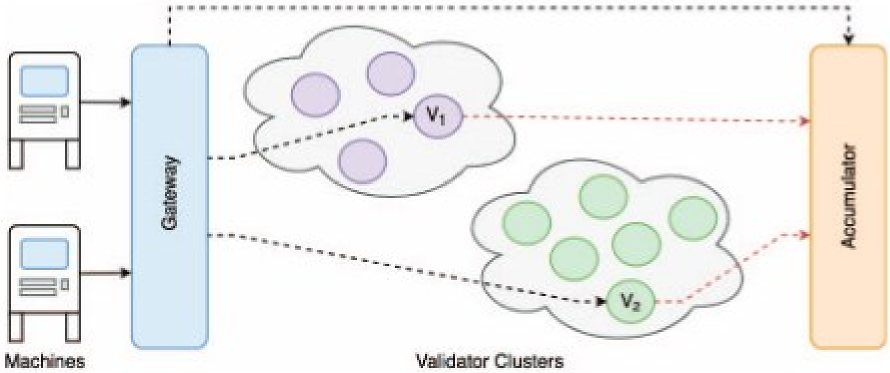
Kevin Wallis, Fabian Schillinger, Elias Backmund, Christoph Reich and Christian Schindelhauer
University of Applied Sciences Furtwangen
Email:{kevin.wallis, elias.backmund, christoph.reich}@hs-furtwangen.de
University of Freiburg
Email:{schillfa, schindel}@tf.uni-freiburg.de

***Abstract*—In the Industry 4.0 context, especially when considering large factories producing costly goods, monitoring sensor values is important to ensure high quality. This reduces large costs for mending faulty products or recall of those. Different approaches are used to ensure efficient monitoring and validation of sensor values. The Distributed Data Validation Network (DDVN) can remove single points of failure. Still, not every anomaly in the validation procedure means that errors or attacks have occurred. Other reasons like maintenance procedures, updates of firmware, or changed materials can lead to False-Positive (FP) or False-Negative (FN) detection of errors. To reduce these, we incorporate context information in the validation procedure. Further, we show how the appropriate context information is selected and used on a real machine data set.**

***Keywords*-Anomaly Detection, Context-Awareness, Distributed Data Validation Network, Industry 4.0**

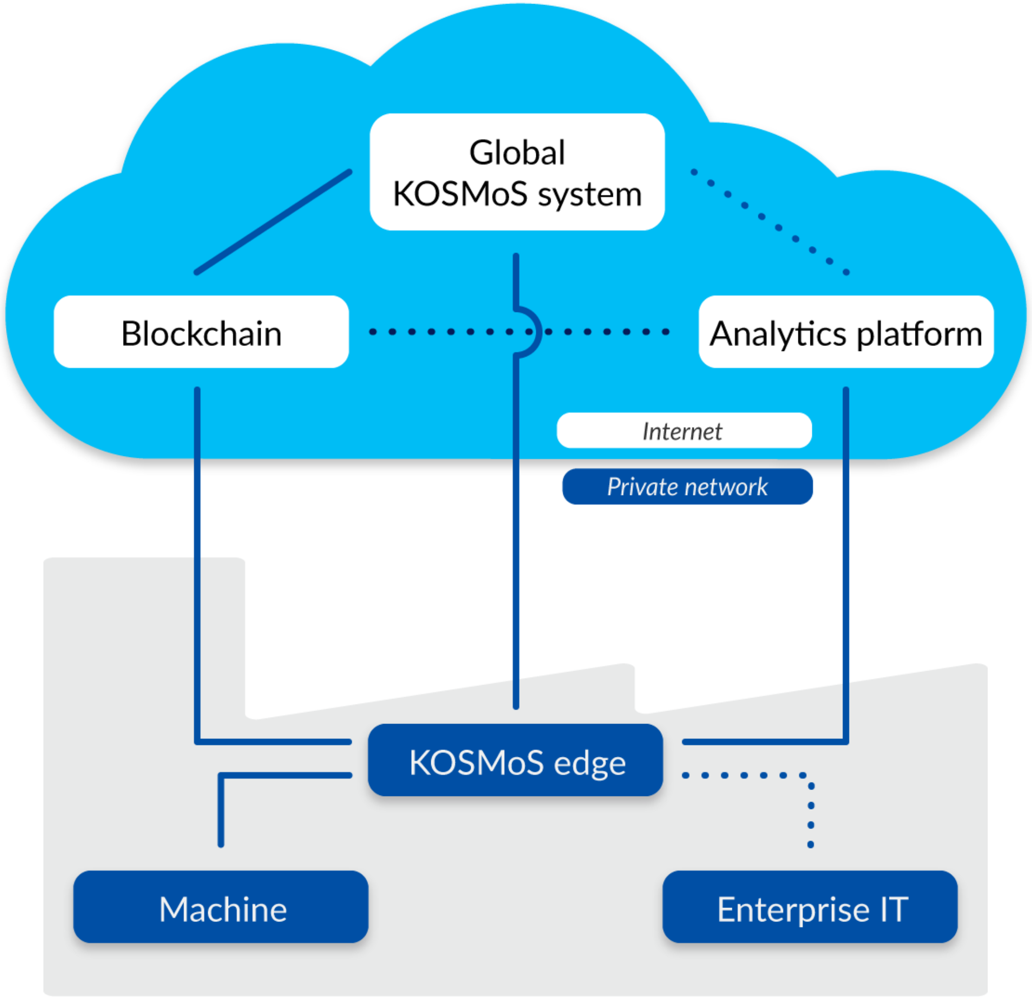
system is applied to consider and evaluate the listed dimensions. Individual solutions are used because most production systems are custom-made. Besides using an external data validation system, there are also production systems that perform the validation on the machine or on the server itself. If the machine does not have a network connection, this will make updating the validation logic, exchanging telemetry data and merging sensor values (sensor fusion) for more accurate and complete data even harder.

Using a single data validation system has the disadvantage of a single point of failure. If the validation system is successfully attacked correct data can be marked as incorrect and, conversely, incorrect data can be evaluated as valid. Furthermore, if a validation system is used for data evaluation as well as data reconstruction [3], incorrect data can be injected

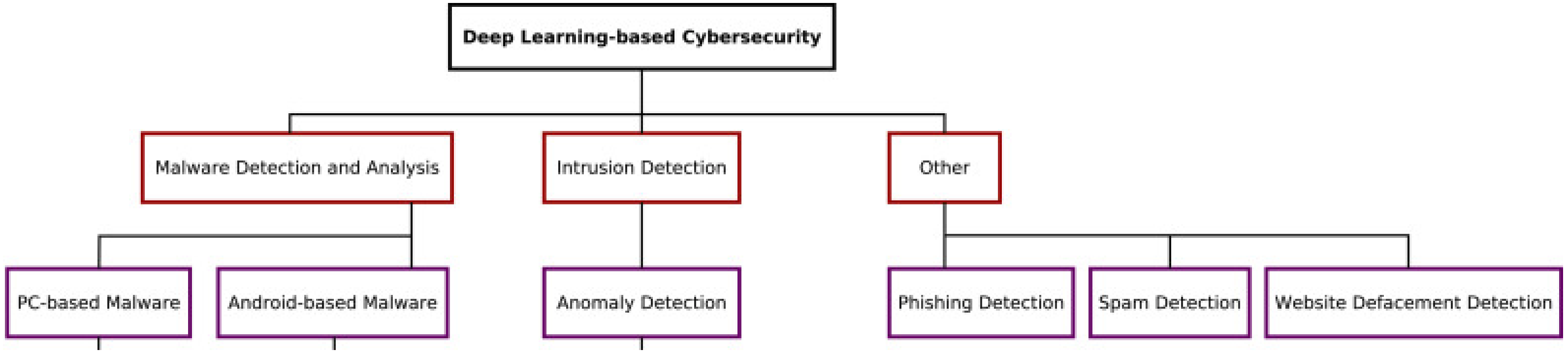


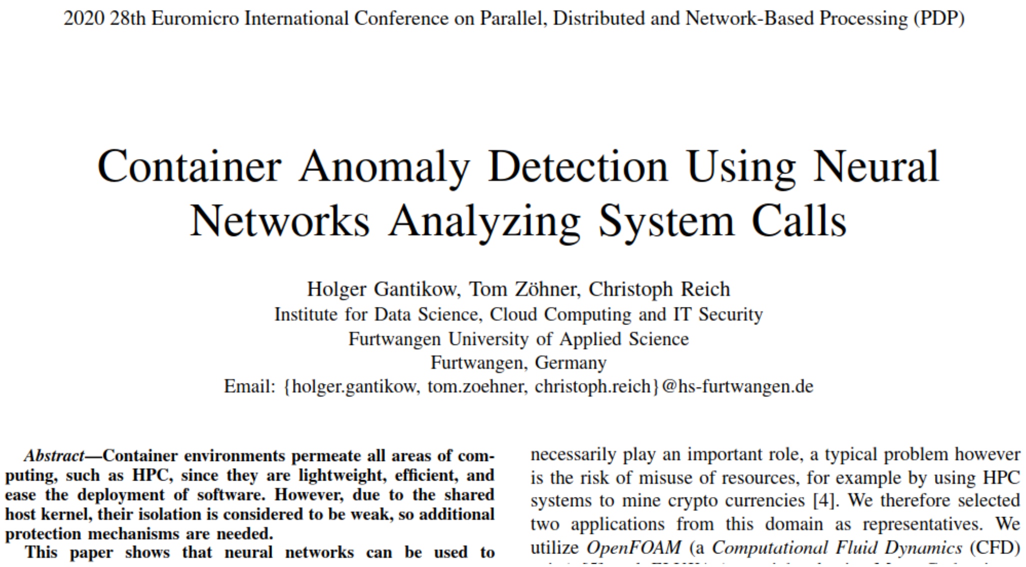
Counter Measurement: Blockchain Audit Trails

- KOSMOS research project: https://www.kosmos-bmbf.de/
- enables cross-company data-driven business models
- Consens of all participants
- Smart contracts implement rules of communication
- Blockchain provides data integrity and audit trails



Machine Learning for Cyber Security





2020 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)

Container Anomaly Detection Using Neural Networks Analyzing System Calls

Holger Gantikow, Tom Zöhner, Christoph Reich
Institute for Data Science, Cloud Computing and IT Security
Furtwangen University of Applied Science
Furtwangen, Germany
Email: {holger.gantikow, tom.zoehner, christoph.reich}@hs-furtwangen.de

***Abstract*—Container environments permeate all areas of computing, such as HPC, since they are lightweight, efficient, and ease the deployment of software. However, due to the shared host kernel, their isolation is considered to be weak, so additional protection mechanisms are needed.**

This paper shows that neural networks can be used to

necessarily play an important role, a typical problem however is the risk of misuse of resources, for example by using HPC systems to mine crypto currencies [4]. We therefore selected two applications from this domain as representatives. We utilize *OpenFOAM* (a *Computational Fluid Dynamics* (CFD)

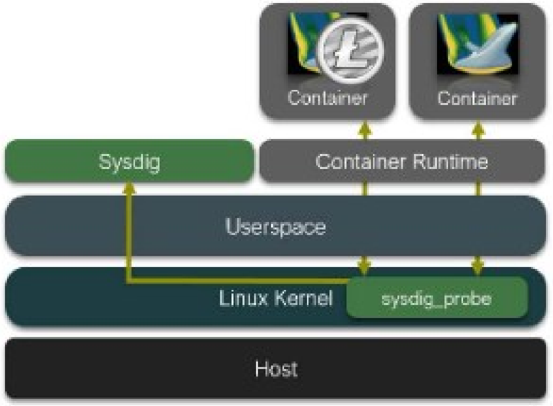


Fig. 1: Sysdig Architecture

ML Generates new Attack Vectors

- ML generates more realistic phising mails
- Robots espionage for hackers
- GANs generate flow to overcome IDS

Summary

Threat	Desired property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

- Traditional
    - Risk analysis (STRIDE)
    - Device analysis (e.g. Common Criteria)
    - Crypto capability of devices
    - RFID tags will not do crypto for some years
    - Security objectives must be risk based
    - Privacy protection must be risk based
    - Identity protection must be risk based
    - Traffic analysis protection
- Machine Learning-specific
    - ML has new risks
    - ML can assist in information security
    - ML generates new risks

Thank you very much for your attention!

THANK YOU

Christoph Reich

christoph.reich@hs-furtwangen.de
University of Applied Science Furtwangen
Institute for Data Science, Cloud Computing and IT Security

idacus.hs-furtwangen.de