Digital Twin Cybersecurity

Luigi Romano

Università degli Studi di Napoli «Parthenope»

luigi.romano@uniparthenope.it

La Cybersecurity e le PMI

28 Giugno 2022 - MediTech

Organization of the talk

- Setting up the scene
- Digital Twins: what they are
- Digital Twins: threats and attacks
- Securing a Digital Twin
- Wrap Up

Setting Up The Scene

Business Drivers

- ➢ While volumes have increased, **margins have dropped**

  The Airbus example:

  Airbus has an average of about 100 billion euros throughput in cash flow going out of their factories

  Their margin on sales is **below five percent**

→ It is key that production plants be managed efficiently:

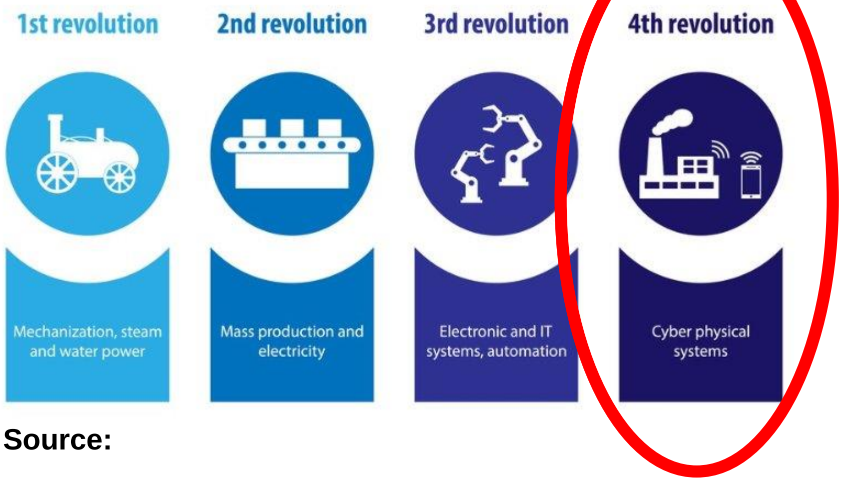
- ○ Quickly apply changes in product design
- ○ Handle increasingly smaller lot sizes
- ○ Ensure that distribution meets challenging reliability and timeliness requirements

This is not possible if we do not make the transition from traditional manufacturing models to Flexible Manufacturing Systems (FMS), aka Digital Manufacturing Platforms (DMPs)*

***The terms FMS and DMP will be used interchangeably throughout this talk**

Hyperconnected Manufacturing

- Manufacturing as we knew it is a memory from the past **that will never come back**


1st revolution
Mechanization, steam and water power
2nd revolution
Mass production and electricity
3rd revolution
Electronic and IT systems, automation
4th revolution
Cyber physical systems

Source:

https://www.iotcentral.io/blog/the-evolution-of-industry-4-0

- The current (and the future) scenario is a global competition arena
- Companies must react quickly and in an economically feasible fashion to market requirements that change continuously, and at an amazingly fast pace

Claims

- FMS are a great opportunity, and – at the end of the day – the only option we have

  (meaning: **even if we don’t like them, we will have to live with them**)

- Unfortunately, we are witnessing a dramatic escalation in cyber attacks to FMS:

  - By 2019, **the manufacturing sector reached the top 10 status** as the 8th most targeted industry by cyber attackers
  - The problem exploded in 2020, when many companies were forced to depend almost entirely on remote workers due to pandemic restrictions

  - In 2020, **the manufacturing industry moved from the 8th most targeted industry** by cyber attackers **to number 2** (falling behind only finance and insurance)
  - According to the 2021 Global Threat Intelligence Report (GTIR), **this represents a 300% increase in a single year!**

Source: https://www.bitlyft.com/resources/cyber-threats-manufacturing-companies

Claims

- Effective protection of a DMP is a multifaceted problem (and a moving target)

- It requires a number of security-enhancing features/tools

Detection

Monitoring

Reaction

Awareness

Remediation

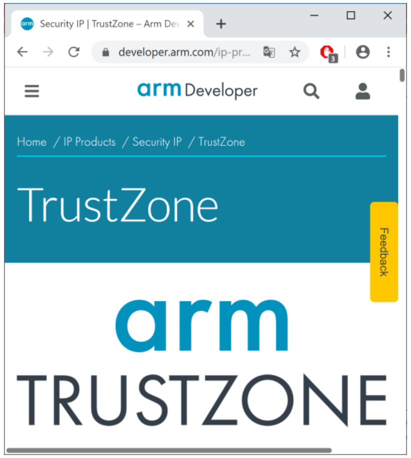
Preparedness

Information Exchange

- Cannot be solved without a rigorous methodological approach, to be rolled out in a continuous process

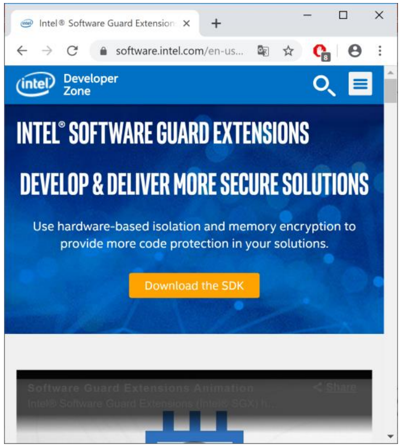
Claims

- A handful of technologies is already available, which can be used to build such features/tools


Security IP | TrustZone – Arm Dev
developer.arm.com/ip-pr...
arm Developer
Home / IP Products / Security IP / TrustZone
Feedback

TrustZone

arm TRUSTZONE

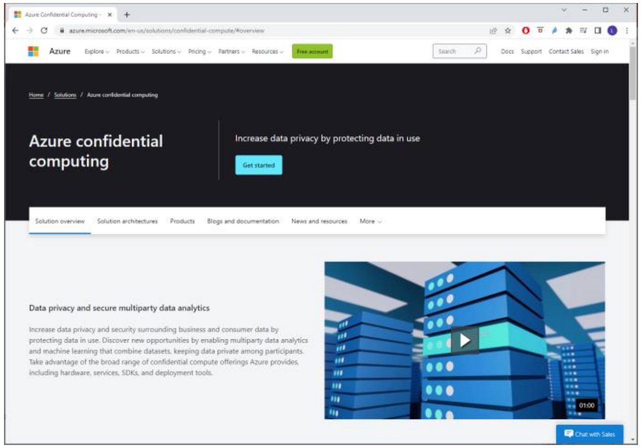

Intel® Software Guard Extension
software.intel.com/en-us...
intel Developer Zone
Download the SDK
Software Guard Extensions Animation
Share

INTEL® SOFTWARE GUARD EXTENSIONS

DEVELOP & DELIVER MORE SECURE SOLUTIONS

Use hardware-based isolation and memory encryption to provide more code protection in your solutions.

Intel® Software Guard Extensions (Intel® SGX) h...



Azure confidential computing

Increase data privacy by protecting data in use

Data privacy and secure multiparty data analytics

Increase data privacy and security surrounding business and consumer data by protecting data in use. Discover new opportunities by enabling multiparty data analytics and machine learning that combine datasets, keeping data private among participants. Take advantage of the broad range of confidential compute offerings Azure provides, including hardware, services, SDKs, and deployment tools.

- Regrettably, the potential of these technologies is not exploited at all, or it is exploited to a limited extent

Rationale for this talk here today

- We must be **creative** in inventing methods/techniques for fully unleashing the power of such technologies, while ensuring that ultimate control stays with the human (Human In the Loop principle)

- This is where SMEs* can play a key role

*SME stands for «Small and Medium Enterprise» → PMI in Italian

- Of course, this is none of an easy task, but …

“When the going gets tough,

the tough get going”

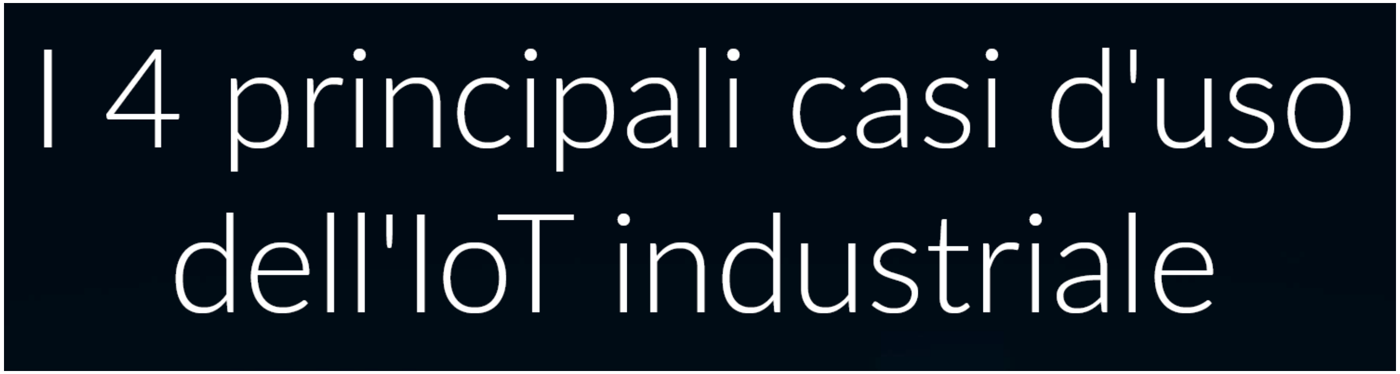
Focus of this talk

- How to protect a key enabling technology of DMPs, namely: Digital Twins

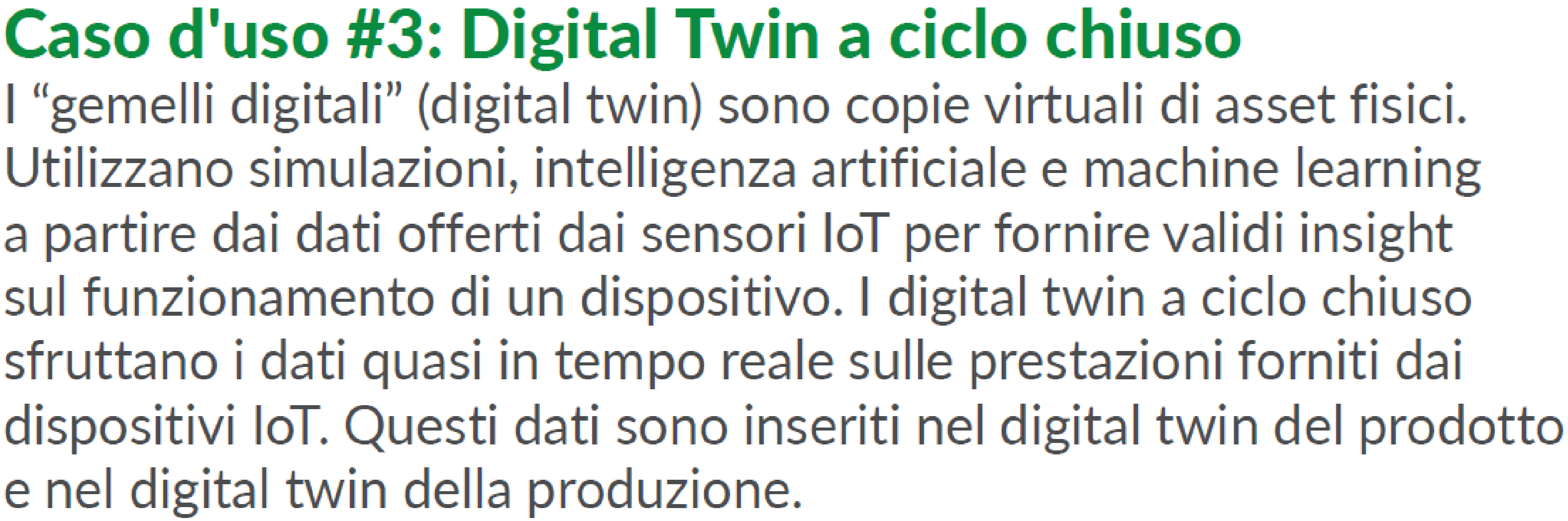
Digital Twins are the next big thing in Fourth Industrial Revolution for the development of new products and processes.

An introduction to the wider topic of protection of DMPs is given here: «Cybersecurity for Manufacturing:challenges and R&I avenues», Luigi Romano - https://cloud.effra.eu/index.php/s/LatomDjFrY8s3lX#pdfviewer

Digital Twins according to Siemens



I 4 principali casi d'uso dell'IoT industriale



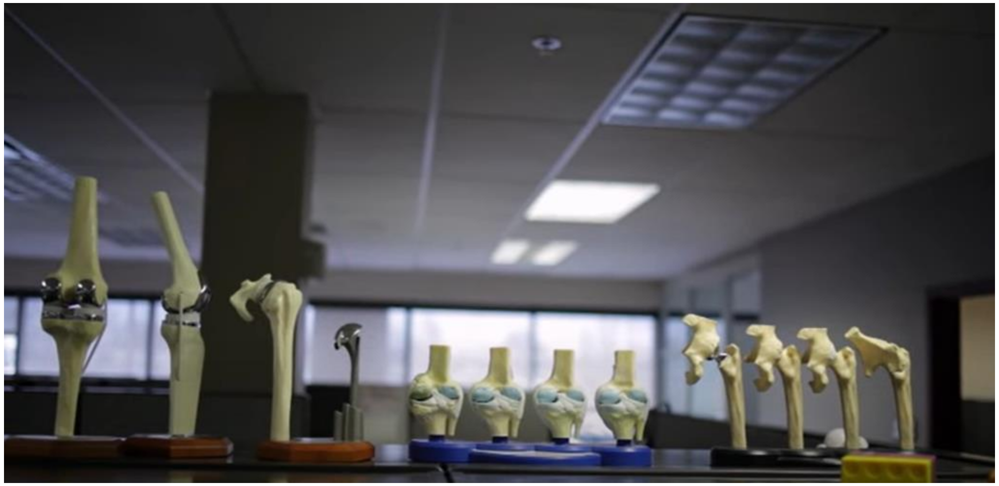
Caso d'uso #3: Digital Twin a ciclo chiuso

I “gemelli digitali” (digital twin) sono copie virtuali di asset fisici. Utilizzano simulazioni, intelligenza artificiale e machine learning a partire dai dati offerti dai sensori IoT per fornire validi insight sul funzionamento di un dispositivo. I digital twin a ciclo chiuso sfruttano i dati quasi in tempo reale sulle prestazioni forniti dai dispositivi IoT. Questi dati sono inseriti nel digital twin del prodotto e nel digital twin della produzione.

A major challenge (and an opportunity): re-using legacy systems

- In Septemer 2018 DePuy was recognized as one of the nine Industry 4.0 Lighthouse projects/companies

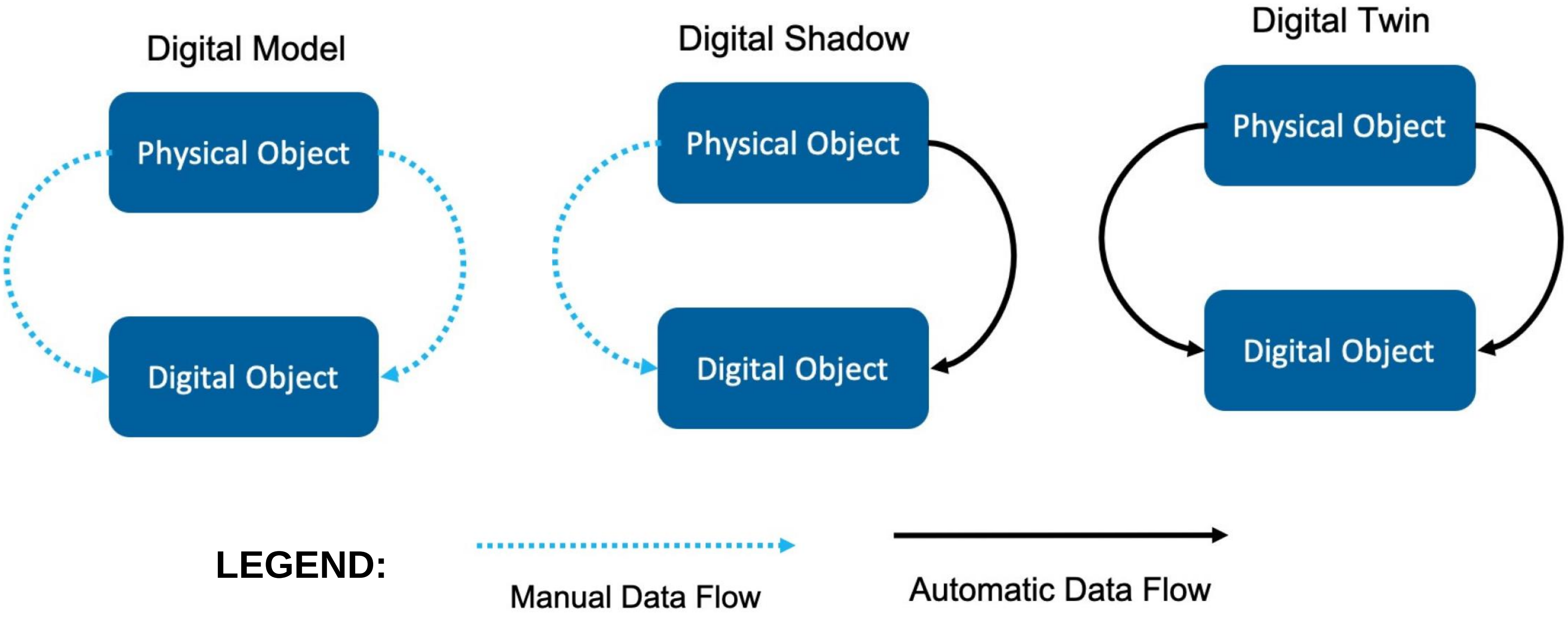
THE ORTHOPAEDICS COMPANY OF Johnson&Johnson



- A major motivation behind this decision was that **they use legacy technology to build Digital Twins**

Digital Twins: what they are

Digital Model, Shadow and Twin



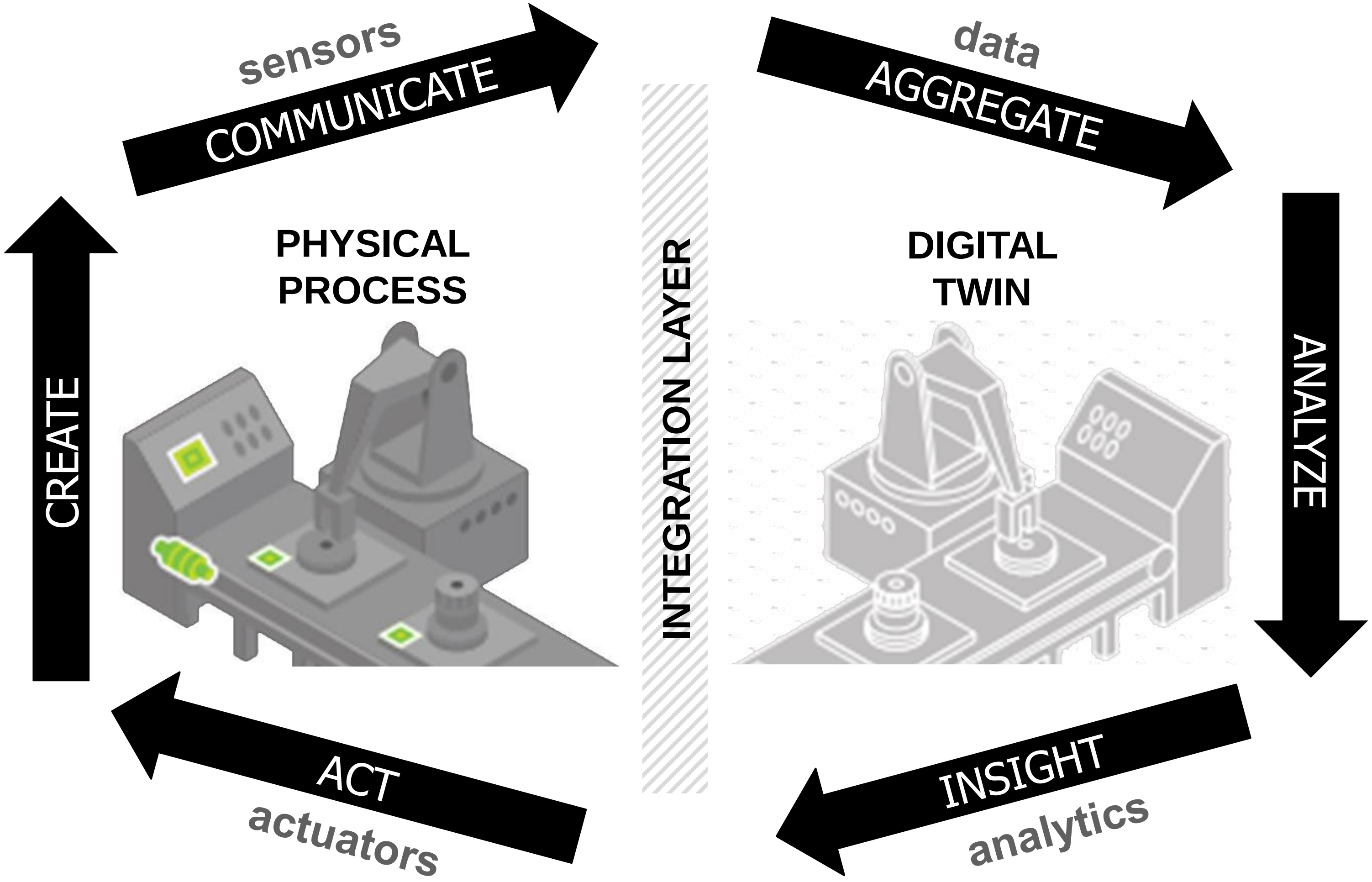
Source:

“Digital Twin: Enabling Technologies,Challenges and Open Research”

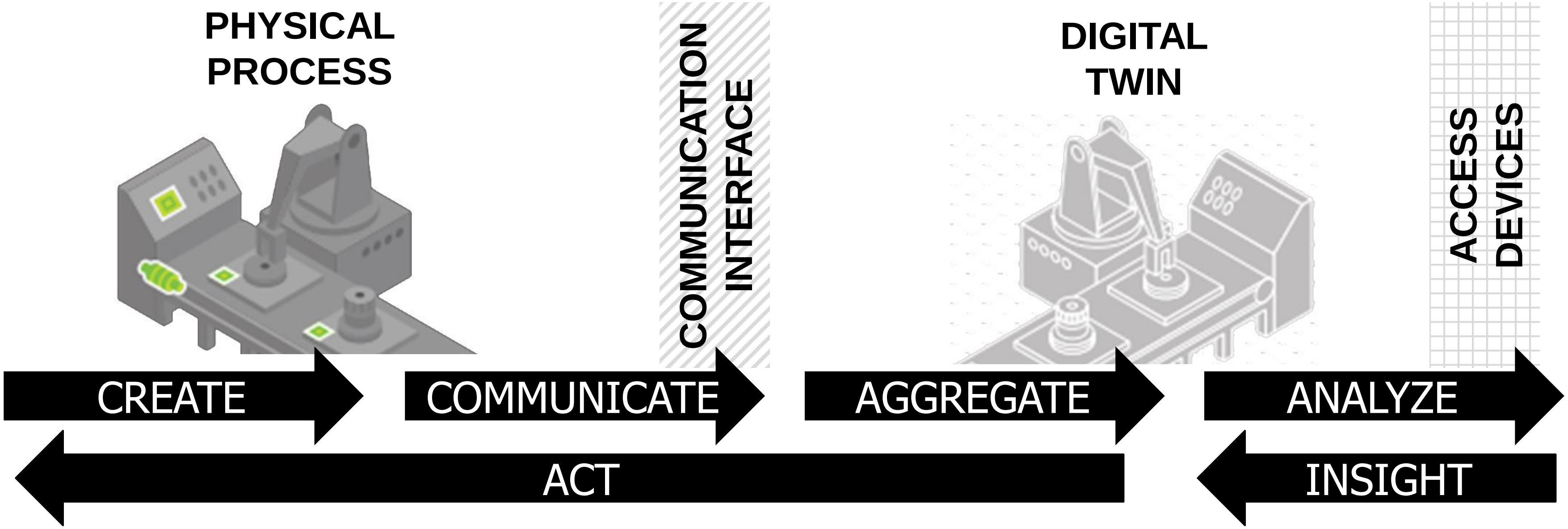
AIDAN FULLER et al. – IEEE Access VOLUME 8, 2020

Digital Twins: threats and attacks

Conceptual Process and Architecture



Attack Surface

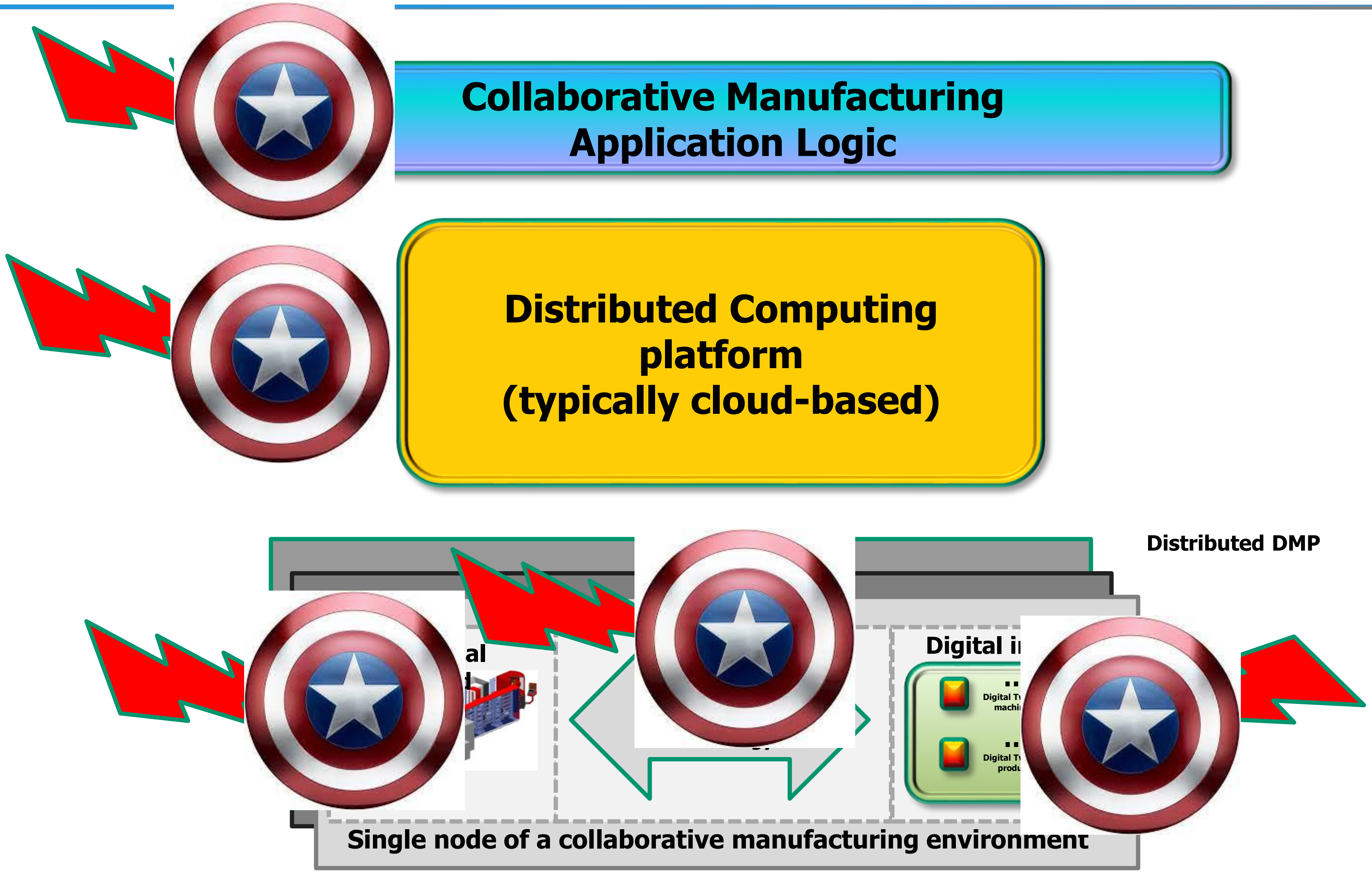


Contextual information (social, weather, etc.)	ERP systems	Sensors	Edge processing	Integration middleware	Data ingestion	Artificial Intelligence	Notifications
	MES software			BAM software	Data lake	Cognitive engines	Visualizations
	CAD models	Actuators	Edge security	Service bus	Legacy data	Hybrid models	Dashboardas

Attack Surface

Securing a Digital Twin

Conceptual architecture of a protection infrastructure



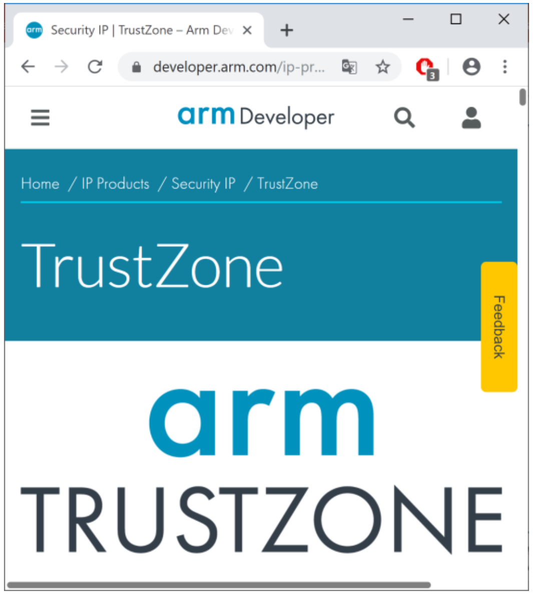
Collaborative Manufacturing Application Logic

Distributed Computing platform (typically cloud-based)

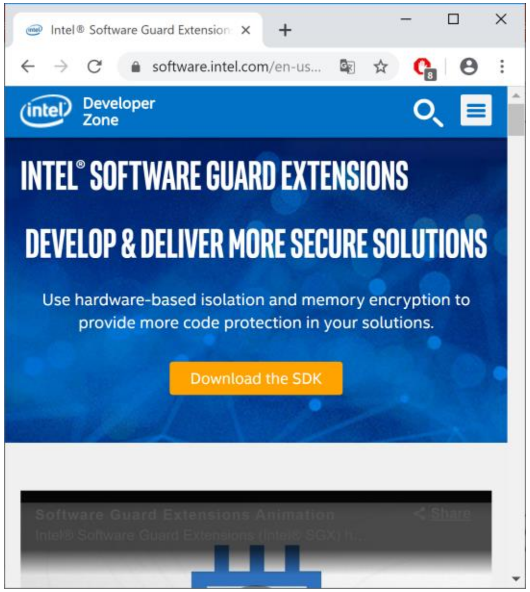
Distributed DMP

Single node of a collaborative manufacturing environment

Enabling Technologies


Security IP | TrustZone – Arm Dev
developer.arm.com/ip-pr...
arm Developer
Home / IP Products / Security IP / TrustZone
Feedback
arm
TRUSTZONE

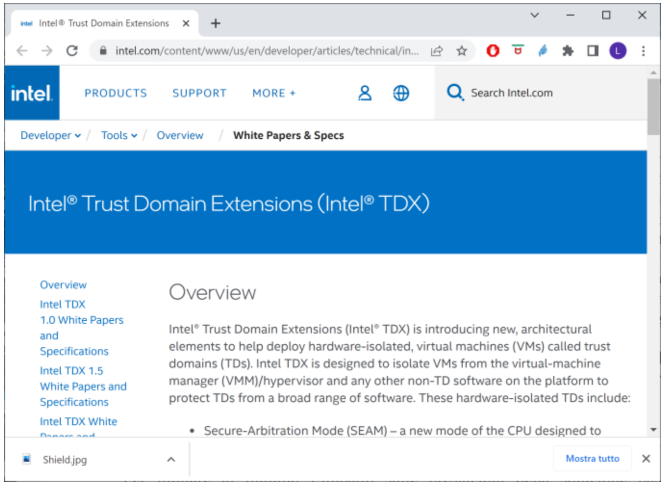
TrustZone


Intel® Software Guard Extension
software.intel.com/en-us...
intel Developer Zone
Download the SDK
Software Guard Extensions Animation
Share
Intel® Software Guard Extensions (Intel® SGX) h...

INTEL® SOFTWARE GUARD EXTENSIONS

DEVELOP & DELIVER MORE SECURE SOLUTIONS

Use hardware-based isolation and memory encryption to provide more code protection in your solutions.

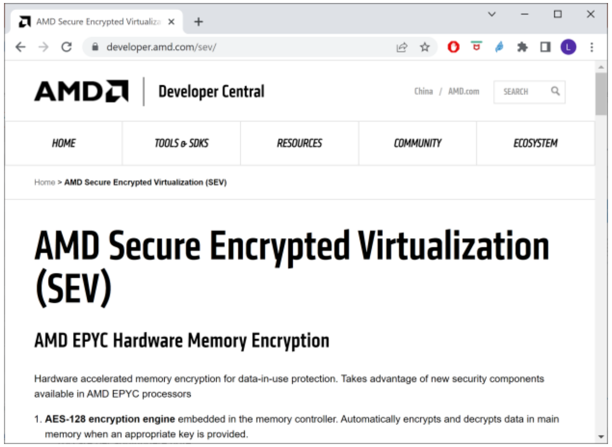

Intel® Trust Domain Extensions
intel.com/content/www/us/en/developer/articles/technical/in...
intel
PRODUCTS
SUPPORT
MORE +
Search Intel.com
Developer
Tools
Overview
White Papers & Specs
Overview
Intel TDX 1.0 White Papers and Specifications
Intel TDX 1.5 White Papers and Specifications
Intel TDX White Papers and
Shield.jpg
Mostra tutto

Intel® Trust Domain Extensions (Intel® TDX)

Overview

Intel® Trust Domain Extensions (Intel® TDX) is introducing new, architectural elements to help deploy hardware-isolated, virtual machines (VMs) called trust domains (TDs). Intel TDX is designed to isolate VMs from the virtual-machine manager (VMM)/hypervisor and any other non-TD software on the platform to protect TDs from a broad range of software. These hardware-isolated TDs include:

- Secure-Arbitration Mode (SEAM) – a new mode of the CPU designed to

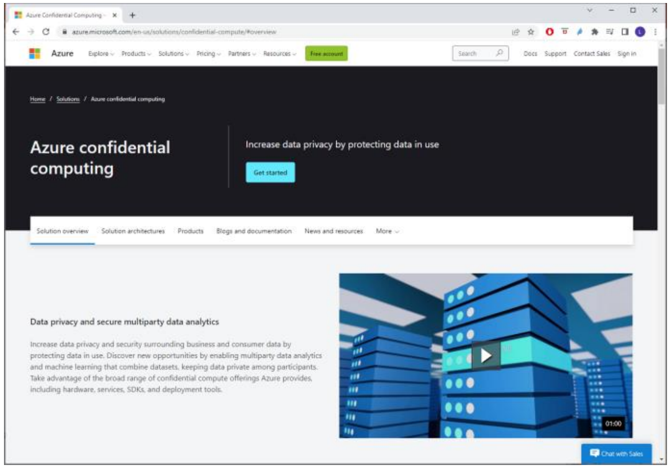


AMD Secure Encrypted Virtualization (SEV)

AMD EPYC Hardware Memory Encryption

Hardware accelerated memory encryption for data-in-use protection. Takes advantage of new security components available in AMD EPYC processors

1. **AES-128 encryption engine** embedded in the memory controller. Automatically encrypts and decrypts data in main memory when an appropriate key is provided.



Azure confidential computing

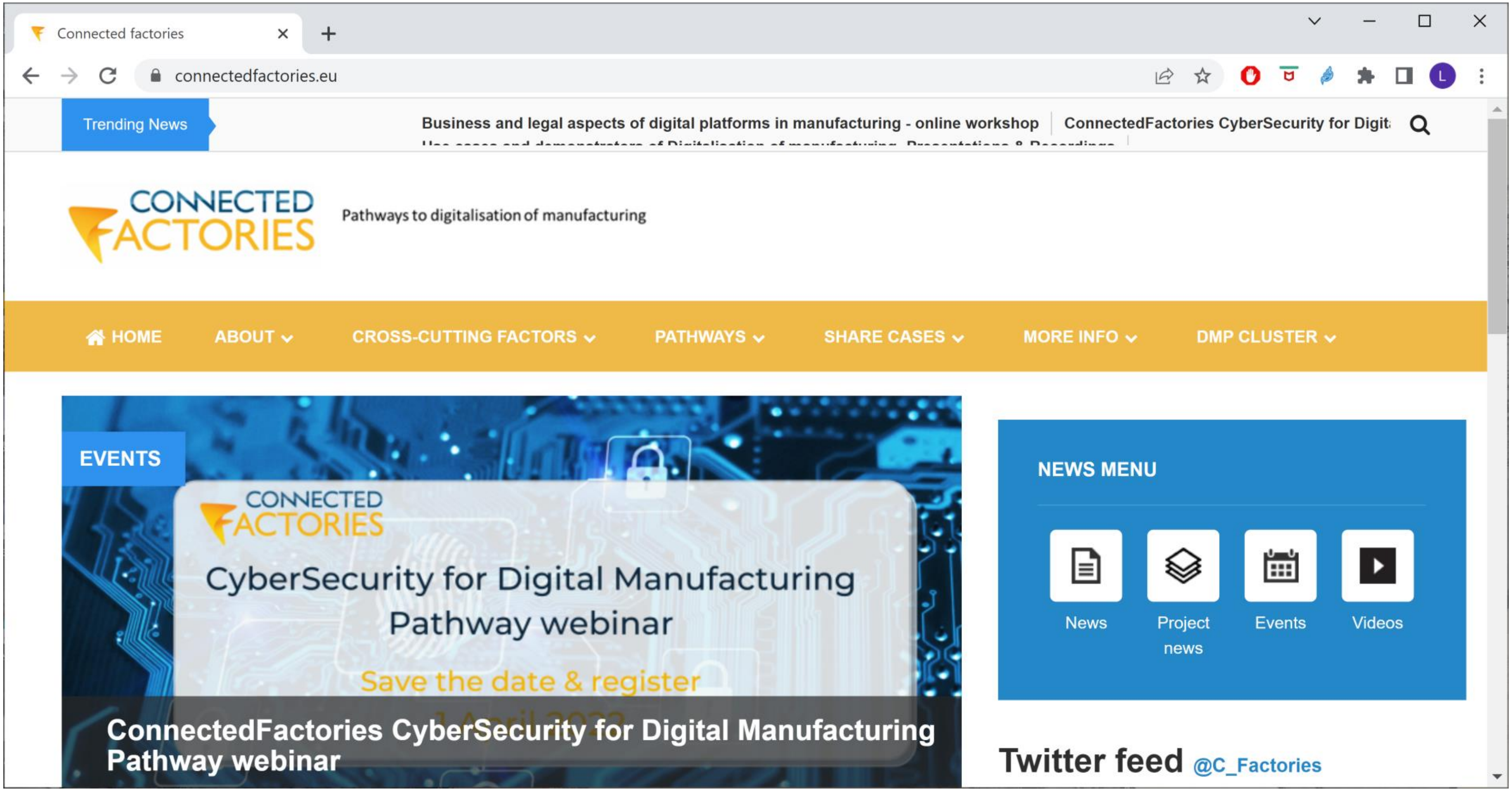
Increase data privacy by protecting data in use

Data privacy and secure multiparty data analytics

Increase data privacy and security surrounding business and consumer data by protecting data in use. Discover new opportunities by enabling multiparty data analytics and machine learning that combine datasets, keeping data private among participants. Take advantage of the broad range of confidential compute offerings Azure provides, including hardware, services, SDKs, and deployment tools.

Related initiatives

Connected Factories 2



Business and legal aspects of digital platforms in manufacturing - online workshop | ConnectedFactories CyberSecurity for Digit

Use cases and demonstrators of Digitalisation of manufacturing - Presentations & Recordings

CONNECTED FACTORIES

Pathways to digitalisation of manufacturing

CONNECTED FACTORIES

CyberSecurity for Digital Manufacturing Pathway webinar

Save the date & register

ConnectedFactories CyberSecurity for Digital Manufacturing Pathway webinar

Twitter feed @C_Factories

Wrap Up

FITNESS

FAULT AND INTRUSION TOLERANT NETWORKED SYSTEMS

Concluding Remarks

- DMPs are the future, but they are exposed to high-impact attacks, which are increasing at an amazingly fast pace
- If future is at risk, you must make an effort to protect it
- Protection is possible, but it requires that:
  - Tools/technologies are carefully selected and their potential is fully exploited
  - A sound methodological approach is used, to drive a continuous improvement process which is rolled out iteratively
- At each iteration, results must be measured based on widely accepted standards
- Automation is a nice to have, but Human In the Loop (HIL) is a must
- Important results have already been achieved, but there is still a long way to go
- Synergies can be found at the European level

Contact Info

Luigi Romano

e-mail: luigi.romano@uniparthenope.it
Cell: +39-333-3016817

The **F**ault and **I**ntrusion **T**olerant **NE**tworked **S**ystem**S**
(FITNESS)
Research Group
http://www.fitnesslab.eu/