



LSEC, 2020, Private & Confidential – Closed User Group Distribution – Do Not Distribute







www.cybersecurityforrobotics.com

f У 🞯 ท





RINITY







Source : Half A Roast Chicken, Eve De Haan, 2018



LSEC, 2020, Private & Confidential – Closed User Group Distribution – Do Not Distribute





This project has received funding from the European Union's Hortzon 2020



TRINITY DIH

A Network of Digital Innovation Hubs in Advanced Robotics

FUNDS UP TO	TAKES
€300K	0%
per team	equity



A network of Digital Innovation Hubs supporting manufacturing SMEs to become more competitive through robotics and digital technologies!

Why TRINITY?

There is a huge opportunity for manufacturers to adopt new robotics and IoT technologies





Agenda CyberSecurity for Robotics at ERF 2020

14.00 Relevance of CyberSecurity for Robotics : putting the Elephant in the Room

Introduction :

Current security threat landscape in robotics,

Detection anomalies in CPS environments: Results from the IoT4CPS project.

Robotics honeypots: Learning from robot hackers.

Attacking mobile robot bases

15.00 Discussion - Debate & Interactive Workshop

with Francesco Ferro, Pall Robotics

Víctor Mayoral, Alias Robotics

Endika Gil Uriarte, Alias Robotics

Arndt Bonitz, AIT

Francisco Lera, University of León

Bernhard Dieber, Joanneum Research















© 3IF.be, 2020, Private & Confidential, Closed User Group Distribution. p 6

Agenda CyberSecurity for Robotics at ERF 2020

16.15 CyberSecurity for Robotics Solutions : cutting the Elephant into Pieces

Security in ROS & ROS 2 robot setups

Access Control Models, with Applications to Robotics,

SecDevOps & Agile Development, Embedded and other Security Solutions,

17.15 Discussion - Debate & Interactive Workshop Robot Security Survey, Endika Gil Uriarte, Alias Robotics

© 3IF.be, 2020, Private & Confidential, Closed User Group Distribution. p 7

Víctor Mayoral Vilches, Alias Robotics

Stefan Rass, Uni of Klagenfurt (AAU)

Ulrich Seldeslachts, LSEC – Shift Left, SKUDO







CyberSecure Robot Development – Slicing the Elephant



Recent Events : nothing sophisticated

Asco closure after cyber-attack to last another week

Saturday, 22 June 2019





Asco, the Zaventem-based company that makes aircraft parts, will now remain closed at least until 28 June, following a cyber-attack two weeks ago.

WIM DE PRETER, MARIE VAN OOST | 14 januari 2020 00:16

Source : Stormshield, The Register, Brussels Times, , Tijd





BUT END USER

' MANUFACTURER

© Leaders in Security – LSEC, 2020, Private & Confidential – Closed User Group Distribution – Do Not Distribute

CyberSecure Robot Development – Slicing the Elephant

IOT: Value Chain Analysis





Whole Robotics Value Chain & Ecosystem

S

affected by

Ø

responsible

CyberSecure Robot Development – Masterplan Objectives WP

- 1. Safety of the user(s)
- 2. Consider users not trusting robots AI & automation, ethics & privacy
- 3. Align to existing CyberSecurity frameworks and guidance
- 4. Bringing ecosystem and all stakeholders together : policy makers, manufacturers, users, integrators, industry, developers, operators



- 5. Liaise, reaching out to partners, partner constituencies
- 6. Formalizing Collaborations
- 7. Develop and Maintain Industry Guidelines, SBOM / Design / RIM ..
- 8. Educate and Awareness
- 9. Innovate and Research

© 3IF.be, 2020, Private & Confidential, Closed User Group Distribution. p 11

10. Advocate & Promote CyberSecured Robotics

* Thanks to Oasis ...





To obtain CyberSecure Robots

We need to ...



Developers, Manufacturers, Integrators, End Users – Operators, ...

* Thanks to Oasis ...





- 1. Pre-market Guidance
- 2. Shared Responsibility Model
- 3. Cybersecurity Product Management
- 4. Software Bill of Materials
- 5. Reference Integrity Manifest
- 6. Secure Components
- 7. CyberSecurity by Design Reduce Regression testing time
- 8. Certification Re-certification
- 9. Train Developers, Manufacturing Design, Threat Modelling, Train the Trainer
- 10. Postmarket severity of harm CVSS Common Vulnerability Scoring System
- 11. Responsible and Coordinated Disclosure
- 12. Active ISAC
- 13. CyberSecurity Safety Analysis Board
- 14. Incentivize
- 15. Patching

THE PROGRAM

WINNING WAS IN HIS BLOOD



* Thanks to Studio Canal



CyberSecurity by Design – premarket guidance

Critical Manufacturing Sector Cybersecurity Framework Implementatio MANUFACT TO CYBERSI Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

For Small and Medium-Sized Manufacturers

Source : FDA 2020, NIST 2015, NIST 2018

CyberSecurity by Design – premarket guidance

- 1. Identify and Protect Device Assets and Functionality Management of Cybersecurity in
 - 1. Prevent unauthorized use : limit to trusted users and devices only
 - 2. Authenticate and check authorization of safety-critical commands
 - 3. Ensure trusted content by maintaining code, data, execution integrit
 - 4. Maintain Confidentiality of Data
- 2. Detect, Respond, Recover : Design Expectations
 - 1. Design the Device to detect cybersecurity events in a timely fashion
 - 2. Design the Device to Respond to and contain the impact of a potential cybersecurity incident
 - 3. Design the Device to Recover capabilities or services that were impaired due to a cybersecurity incident
- 3. Labeling Recommendations for Devices with Cybersecurity Risks
- 4. CyberSecurity Documentation
 - 1. Design Documentation
 - 2. Risk Management Documenation



Medical Devices

CyberSecurity by Design – Shared Responsibility – healthcare devices example

An official website of the United States government Here's how you know \sim	
	hcare Delivery Organization
DRUG	Contract & Requirements Management • Policy & Requirements Memt

← Home / Medical Devices / Digital Health / Cybersecurity

Medical device manufacturers (MDMs) and health care delivery organizations (HDOs) should take steps to ensure appropriate safeguards are in place.

- Medical device manufacturers (MDMs) are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity.
- Health care delivery organizations (HDOs) should evaluate their network security and protect their hospital systems.
- **Both MDMs and HDOs** are responsible for putting appropriate mitigations in place to address patient safety risks and ensure proper device performance.

Source : Symantec, 2016, FDA , 2020 https://www.researchgate.net/publication/325746918 CYBERSECURITY FOR HEALTHCARE MEDICAL DEVICES



CyberSecurity by Design – CyberSecurity Product Management



CyberSecurity Product Manager

- PM whose solution addresses information security needs of its customers.
- hands-on security practitioners, who've transitioned into product management
- built up their infosec prowess after becoming a PM by building upon their business, software engineering or other expertise
- empathize with risk-sensitive customers concerned about issues such as online threats, data safeguards, information security regulations, security incident handling, etc.
- answer questions related to your product's security domain, including: measures are your prospective customers employing today to address the risks that your product tackles? How will your product's capabilities handle the ever-evolving threat and/or regulatory landscape? security benefits? operational burdens compare to the product's security value proposition? Security, compliance, audit or other roles benefit?



CyberSecurity by Design – Supply Chain Risk



CyberSecurity by Design – Software Bill of Materials



CyberSecurity by Design – Software Bill of Materials



Limited visibility enables less awareness of risk

https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf

More complete visibility enables more complete awareness of risk

CyberSecurity by Design – Reduce Regression testing time







© 3IF.be, 2020, Private & Confidential, Closed User Group Distribution. p 21

CyberSecurity by Design – Software Bill of Materials



https://www.ntia.gov/files/ntia/publications/ntia sbom formats and standards whitepaper - version 20191025.pdf



Industrial and Connected Robots : categorizing according to operation

Controller operated	the robot functionalities are being controlled by a robot controller, either integrated or separated from the robot arm or robot itself. Mostly the instructions to the robot are being sent in clear text.	
PLC operated	the robot is being controlled through a PLC, typically connected to a central controlling environment, instructing directly the robots or sending instructions to the robot controller	Zuriti verbatent Ende des Schutzberickes
ROS (1-2)	the (ROS) Robot Operating System v1 and 2 can directly instruct a number of robotic systems, and v2 is improving cybersecurity; but both systems have seen adoption in research projects, but only few in production and operational environments,	
IoT	latest generation robots receive direct instructions from a series of microcontrollers integrated in the robot, running on an operating system utilizing internet technologies	
Cloud Operated	new developments are taking place to have the robot receiving direct instructions from the cloud, requiring a continuous and constant internet connection to the robot. Instructions can be transformed from IoT to a robot controller or via PLC.	



CyberSecure Robot Development Program – Responsible Disclosure

m.

stream.

Buffalo NAS - 335 days in the wild without a patch

Disclosure timeline:

- 18-06-22: E-mail security contact listed on website.
- 18-07-02: E-mail security contact again.
- 18-07-03: Sent v
- 18-08-22: Sent C
- 18-11-06: Public
- 18-11-08: Public
- 18-11-09: @Buf
- ??-??-??: @Buft
- 19-09-16: ISE re______shutterstock.com 228643177 _____per.
- 19-09-18: Buffalo reaches out, provides reliable email.

BAD PRACI

19-10-09: Buffalo releases firmware v4.02.







LIVESTREAM: How We Discovered New Vulnerabilities in the Buffalo TeraStati... blog.securityevaluators.com

†17



CS Robot Dev Program – Responsible Disclosure Manufacturers

- 1. Check your security inbox!
- 2. Social Media will hunt you down
- If you don't have a public security point of contact, create one!
- Bug bounty programs should not inhibit coordinated disclosure.
- 5. Audit your vulnerability disclosure resources.
- 6. Audit use of the X-Forwarded-For header.
- Custom protocols are not an answer researchers won't be intimidated by it
- 8. Remember that everyone makes mistakes.- Use them as opportunities to demonstrate integrity.





CyberSecurity by Design – Software Bill of Materials

Time to Remediation Case Studies



https://www.ntia.gov/files/ntia/publications/ntia sbom use cases roles benefits-nov2019.pdf

CyberSecure Robot Development Program – RIM

Reference Integrity Manifest



CyberSecurity by Design – Secure Components



CyberSecurity by Design – Reduce Regression testing time©





Source : LSEC Cloud 2019, Shift Left

CyberSecurity by Design – DevSecOps



CyberSecurity by Design – DevSecOps to AI Ons



CyberSecurity by Design – AI Challenges

Automation

- DevOps is everywhere
- Increase of using
 - Automation
 - Open Source libraries
 - Containerization
 - Re-use deployment / IaC scripts



Source : LSEC AI 2019, Shift Left

New attack vectors

- Taking advantage of automation.
- Open source libraries
- Fast build-deploy
- Containerization
- Complexity and dependencies







CyberSecurity by Design – AI Cybersecurity Risks

- 1. Data poisoning
- 2. Adversarial attacks

1. AI to create smarter 2. Robustness/Vulnerability of AI algorithms cybersecurity .g. more effective security controls E.g. adversarial machine learning (i.e. exploitation of weaknesses in Al tivirus, intrusion detection and algorithms to change their behavior), attacks against AI powered cyber- $+.007 \times$ physical systems, etc. = **RISK** 4. Use of AI to fight cyber 3. Misuse of AI attackers & criminals x + $sign(\nabla_{\boldsymbol{x}} J(\boldsymbol{\theta}, \boldsymbol{x}, y))$ E.g. creation of deep audio video $\epsilon sign(\nabla_{\boldsymbol{x}} J(\boldsymbol{\theta}, \boldsymbol{x}, \boldsymbol{y}))$ E.g. better biometrics, smarter fakes, AI powered malware, smarter forensics, fraud analysis, encryption "panda" "nematode" "gibbon" social engineering attacks, etc challenge, fight against fake news, 57.7% confidence 8.2% confidence 99.3 % confidence *IBM Research has recently released an open source library called Adversarial Robustness Toolbox ("ART Model stealing (model extraction attack) 3. Conceptual model depicting the logical links between the different components of the ML service cybersecurity risk in the context of the influence of AI and Digital Transformation Data owner Extraction adversar European Commission mode Source: CSSF, 2019 Video Forgery 4.

Cybersecurity and AI & DT: 4 angles of influence

Opportunities

Challenges

CyberSecurity by Design – use PLC's only if nothing else can be used

- Real-time digital computer used for automation
- Replaces electrical relays
- Lots of analogue or digital inputs & outputs
- Rugged devices (immune to vibration, electrical noise, temperature, dust, ...)



Siemens S7-1200





CyberSecurity by Design – Use PLC's only if there is no alternative

- SoMachineBasic is the software provided by Schneider Electric to program the entry-level PLCs.
- PLCs used in big plants are usually programmed using Unity Pro, for which there is no free demo version.
- Fortunately, the way this software work is very much the same

Arrison tables Methods Methods Methods Splaten abjects Protopics Methods Splaten abjects Protopics Splaten abjects Methods Splaten abjects Splaten abjects <th>rapertim</th> <th>Configuration</th> <th></th> <th>Programming</th> <th></th> <th></th> <th>Display</th> <th></th> <th></th> <th>Comments</th> <th>oning</th> <th></th>	rapertim	Configuration		Programming			Display			Comments	oning	
Memory visual lat System digets System digets Solution Cognets Solution Soluti	Nessages Animation tablea	1.2.2 B		4 9 49 99 99 1 - RAM POSITION	C +++ +) (/) (0) (x) (4) (40)				
PTO Openia Special Plan 9 Communication Objects Description with Sensor 9 Search and Replace Sensor 9 Search and Replace Sensor 9 Memory Resources/Sensor The Sensor	Memory objects System objects To objects Metrocrite objects Software Objects Software Objects	Range Ran	n pesition counter en in atu- post- post- post- pat	Adjustes 180 degree	e bit and parts fe	oler .	ж					
	PTO objects Communication Objects Search and Replace Symbol last	The second se		 Type: Dual Pha Sivit, Outlo S. T.C.UTL: Preset 8 	u_							
	a location frances				тне_							
				·	i i	1		•	×	×		- 1

PLC programming

- Create a project
- Define the hardware setup
- Create variables
- Define the program
- Test
- Debug
- Push to PLC
- START



CyberSecurity by Design – PLC's Modbus and OPC inherently insecure

At the beginning, specific protocols on specific **physical layer** (RS232, RS485, 4-20 current loop) Some protocols were **adapted to TCP/IP**, like Modbus, and other were developed to allow interoperability.

ICS devices often use **specific protocols**, some of them are **proprietary**, and some of them are **common standards** We will hereafter cover the most used ones.





CyberSecurity by Design – When using PLC's, mind security



- Standard protocol
- Used to exchange data between ICS and Windows devices
- Works on TCP/IP
- Several variants:
 - OPC-DA : Data access, used to gather data from the process control
 - OPC A&E : Alarm & Events
 - OPC HDA : Historical Data Access
 - OPC DX : Data Exchange, allow to exchange data between OPC servers
 - OPC Security
 - OPC XML-DA
 - OPC UA : Unified Architecture, aimed at replacing the others while using a more modern Servi Oriented Architecture.
- Provides authentication and encryption, probably the future of ICS protocols



- Defined in IEC 62541 in 2015
- Designed to replace « DCOM »
- Open and non-hardware specific protocol
- Probably the future of ICS communications

How it works

- Service-oriented architecture (client/server)
- A client can read and edit server nodes, as well as subscribe to them. It is then notified by the server when the node is modified.
- Thanks to the nodes hierarchy and names, it is possible to know what is controlled by the node.
- One server can handle several clients simultaneously.
- The protocol can use « binary/TCP » or « SOAP/HTTP »

Security

- Several security levels: none, signature, signature and encryption.
- Compatible with X.509 certificates and Kerberos.
- Login/password connection
- Fine grained access rights for each node (read/write).





CyberSecurity by Design – network traffic provides insight

- Analyze a Modbus communication with Wireshark
- Wireshark owns by default a Modbus dissector

Analyze an opc-ua communication with Wireshark

Protocol

OpcUa OpcUa OpcUa

OpcUa

OpcUa OpcUa OpcUa

0pcUa

OpcUa OpcUa

OpeUa

OpcUa OpcUa

Wireshark owns by default an opc-ua dissector

4	0.001595	127.0.0.1	127.0.0.1	Modbus/T(
5	0.001638	127.0.0.1	127.0.0.1	TCP
6	0.015000	127.0.0.1	127.0.0.1	Modbus/T(
7	0.015047	127.0.0.1	127.0.0.1	TCP
8	0.015225	127.0.0.1	127.0.0.1	TCP
9	0.019268	127.0.0.1	127.0.0.1	TCP
10	0.019310	127.0.0.1	127.0.0.1	TCP
11	15.592238	127.0.0.1	127.0.0.1	TCP
12	15,592255	127.0.0.1	127.0.0.1	TCP

- т папашізатон сонстос Рготосос, эго Рогс, зэрэч (эзрэч), рас Рогс, аза-аррс-
- Modbus/TCP
 - Transaction Identifier: 28737
 - Protocol Identifier: O
 - Length: 6
 - Unit Identifier: l
- Modbus
 - Function Code: Read Holding Registers (3)
 - Reference Number: 0
 - Word Count: 16

- Launch Wireshark
- Open « modbus1.pcap »
- Try to understand what's going on
 - Reading request
 - Writing request
 - PLC's answer
- What's the value of register #123 at the end?

No.	Time	Source	Destination
14	9 17.937435	192.168.0.15	10.0.2.15
15	0 17.940843	10.0.2.15	192.168.0.15
15	2 17.945418	192.168.0.15	10.0.2.15
15	4 23.039340	10.0.2.15	192.168.0.15
15	6 23.045154	192.168.0.15	10.0.2.15
15	8 23.053165	10.0.2.15	192.168.0.15
16	0 23.067247	192.168.0.15	10.0.2.15
16	2 23.344418	192.168.0.15	10.0.2.15
16	4 23.345797	10.0.2.15	192.168.0.15
16	6 26.128772	10.0.2.15	192.168.0.15
16	8 26.132215	192.168.0.15	10.0.2.15
16	9 26.134839	10.0.2.15	192.168.0.15
17	1 26.137928	192.168.0.15	10.0.2.15
17	3 26.854666	192.168.0.15	10.0.2.15
- OpcUa	Binary Protoco	1	
Mes	sage Type: MSG		
Chu	nk Type: F		
Mes	sage Size: 154		
Sec	ureChannelId: ()	
Sec	urity Token Id:	1	
Sec	urity Sequence	Number: 42	
Sec	urity RequestIo	1: 42	
- Opc	Ua Service : Er	codeable Object	
+ 1	<pre>'ypeId : Expand</pre>	edNodeId	
- 1	/riteRequest		
	RequestHeader	: RequestHeader	
	 NodesToWrite: 	Array of WriteValue	
	ArraySize:	1	
	- [8]: WriteV	alue	
	NodeId: N	lodeId	

- Launch Wireshark
- Open « opcua.pcap »
- Try to understand what's going on
 - Browse request
 - Read request
 - Write request
 - Create subscription request
 - Create monitored item request
 - Publish request
- Which node has been changed and what was the value?



CyberSecurity by Design – Training- (ROS2 Security covered by Viktor)

ightarrow C (i) Not Secure design.ros2.org/articles/ros2_dds_security.html

ROS 2 Design Contribute

ROS 2 DDS-Security integration

Robotics is full of experimentation: evaluating different hardware and software, pushing ahead with what works, and culling what doesn't. ROS was designed to be flexible to enable this experimentation; to allow existing components to easily be combined with new ones or swapped with others. In ROS 1, this flexibility was valued above all else, at the cost of security. By virtue of being designed on top of DDS, ROS 2 is able to retain that flexibility while obtaining the ability to be secured by properly utilizing the DDS-Security specification. This article describes how ROS 2 integrates with DDS-Security.

Original Author: Kyle Fazzari

DDS-Security overview

The DDS-Security specification expands upon the DDS specification, adding security enhancements by defining a Service Plugin Interface (SPI) architecture, a set of builtin implementations of the SPIs, and the security model enforced by the SPIs. Specifically, there are five SPIs defined:

- Authentication: Verify the identity of a given domain participant.
- Access control: Enforce restrictions on the DDS-related operations that can be performed by an authenticated domain participant.
- Cryptographic: Handle all required encryption, signing, and hashing operations.
- Logging: Provide the ability to audit DDS-Security-related events.
- Data tagging: Provide the ability to add tags to data samples.



CyberSecurity by Design – Training



DF



CyberSecurity by Design – Postmarket severity of harm - CVSS – Common Vulnerability



© 3IF.be, 2020, Private & Confidential, Closed User Group Distribution. p 41

CyberSecurity by Design – Detection of Flaws & Remediation



CyberSecurity by Design – Detection of Flaws – Automated Firmware Analysis





CyberSecure Robot Development Program – CS by Design CyberSecurity by Design – Postmarket severity of harm - CVSS – Common Vulnerability Robot Vulnerability Database (RVD)



Robot vulnerabilities by robot component

Last updated Mon, 02 Mar 2020 14:37:10 GMT

- Robot vulnerabilities by robot
- Robot vulnerabilities by vendor





CyberSecurity by Design – Postmarket severity of harm - Founding Robotics ISAC

SECTORS

PRIVATE SECTOR REASONS TO PARTICIPATE IN AN ISAC

- sh Universal Robots Robot Controllers | CISA
- ItI www.us-cert.gov/ics/advisories/ICSA-18-191-01
- Do not connect the **robot** to a network unless it is required by the application. Do not connect the **robot** directly to the internet. Use a secure ...

TYPES OF ORGANIZATIONS

Vecna VGo **Robot** (Update A) | CISA

- to www.us-cert.gov/ics/advisories/ICSA-18-114-01
- ^{or} 2 UPDATE INFORMATION. This updated advisory is a follow-up to the original advisory titled ICSA-18-114-01
- Vecna VGo Robot that was published April 24 ...
- Ac

Source : ENISA

- Fo ABB **Robot** Communications Runtime Buffer Overflow | CISA
- kn www.us-cert.gov/ics/advisories/ICSA-12-059-01

Overview. ICS-CERT received a report from ABB and the Zero Day Initiative (ZDI) concerning a buffer overflow

Ne vulnerability in the **Robot** Communication ...

meeting people from different organizations. In the presence of an incident and need to gather information, there is always a know-how way to network with the respective team.



Industrial Control System Information Sharing and Anal

Bringing together infrastructure stakeholders to improve cybersecurity knowledge sharing.

COLLABORATION

STYLES AND TOOLS

ne Resources Current Members Member Benefits C-CIP Member Portal Contact Us





21110 22



Key Learnings

- 1. Need for a CyberSecurity for Robotics Masterplan
- 2. All actors in the ecosystem need to be involved and collaborating
- 3. Other vertical industries and technology domains can provide insights
- 4. Guidance and materials are available
- 5. CyberSecurity by Design requires a Program for Manufacturers and Users

6. Join the CSfR community of researchers, industry and users





© 3if.eu, 2020, Private & Confidential – Closed User Group Distribution – Do Not Distribute



DIGITAL SECURITY CATALYST









© Leaders in Security – LSEC, 2020, Private & Confidential – Closed User Group Distribution – Do Not Distribute

MarketIntelligence.Leadersinsecurity.org

DIRECTORY (plore actors by clicking the top right fil	lter button and enter keywords or use the d	rop downs to filter the directory of actors.	~	COMPANIES 🗹 PEOPLE	₹ FILTER 1865 ACT
Search on keyword, locations, ta	gs,				Z L
Category 🗸 Memberships	✓ Activities ✓ Indus	stries 🗸 Domains 🗸	Technology 🗸		More fi
SSHTEAM S	SENTINELONE	SAMOBY Samoby protects your	SODENA S	SECURITYPORT (8)	SCORECHAIN S AML Compliance for Bitcoin.
	that defends every endpoint against every type of attack, at every stage in the threat lifecycle	company from mobile security threats while improving employees' mobile IT experience and controlling the cost of own	instrument of the Government of Navarre for the business development of the region. SODENA carries out its activities	marketplace where companies that face a cybersecurity skills gap can find verified freelance experts to so	Ethereum and cryptocurrencies
And Mark		Cannoby Extend your security perimeter to mobile devices Sunobly protects your company from mobile security theats while improving employees' mobile if experience and controlling the cost of ownership. See how Samoby can help your business			Control (Control (Contro) (Control (Control (Contro) (Control (Contro) (Control (Contro)
skudo 🔇	SECCOURIEL S	SWANSEA UNIV 🗊	<u>s</u> ecrutiny lim \mathbb{Q}	<u>silensec</u>	SENSATIVE 8
Hardware encryption based on a custom-built chip (HSM on a chip)		Swansea University is a public research university located in Swansea, Wales, United Kingdom.	Secrutiny are Incident Response specialists who spend 95% of our time making sure our clients don't need to respond to incidents from our	Silensec is an Information Security Management Consulting and Training company. Silensec was initially created to utilise the skills of r	Sensative develops practical IoT products and platforms for everyday use. Strips by Sensative is our first product. It's a wireless magne
	Use deliver the gold standard	cherishice ? and mar there, there is a colorate and and the sole is allowed and the sole is allowed	nanda Malangu angananana	SilonSec" h à l ≠ 5 Internet de la sector	

© Leaders in Security – LSEC, 2020, Private & Confidential – Closed User Group Distribution – Do Not Distribute



© Leaders in Security – LSEC, 2019, Private & Confidential – Closed User Group Distribution – Do Not Distribute





www.trinityrobotics.eu



© Leaders in Security – LSEC, 2020, Private & Confidential – Closed User Group Distribution – Do Not Distribute

under grant agreement No 825196

DIH TRINITY



Digital Technologies, Advanced Robotics and increased Cyber-security for Agile Production in Future European Manufacturing Ecosystems

DT-ICT-02-2018 - Robotics -Digital Innovation Hubs (DIH)



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



Overall budget: ~ € 16 400 000



48 months- January 2019 to December 2022



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



- At least 30 company demonstrators to be funded
- Proof-of-Concepts in industrial environments
- All thematic areas covered
- Calls open for 3 months
- Up to EUR 300,000 funding per demonstrator (70%)
- Total budget 8m€, target budget for 1st Open Call is 4m€

6th 3IF.be international conference

www.3if.be **3IF.be – iotconvention.be** 10.06.2020 Industrie 4.0 – Proof International Conference 2019

- Trends & Developments in Industrie 4.0 & IIoT
- From Use Case to Business Case to Industrial Roll Out and Operations
- Edges and Cloud, Mastering End to End Security
- Flanders Industrie 4.0 Field Lab experiences from the trenches.





NOT THE END

More information, slides and follow-up **WWW.ISEC.EU** www.3if.be - .eu



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



