This database contains a list of all results generated by partners within the scope of IoT4CPS. It is intended as a source for external partners to utilize the project outcomes. The latest version of this document can be found on http://iot4cps.at
If you have any general questions concerning the project IoT4CPS, please contact the project lead Mario Drobics (mario.drobics@ait.ac.at). For specific questions concerning the mentioned deliverables, kindly approach the specific contact person directly.

Titel	Description	Source	Type	Licence	Deliverable	Demonstrator	Contact Person (Name)	Contact Person (eMail)	Partners involved	Comments
Bloom Filter Encryption from Boneh-Franklin IBE	Library implementing BFE based on "Bloom Filter Encryption and Applications to Efficient Forward-Secret 0-RTT Key Exchange" by Derler, Jager, Slamanig, and Striecks (EC'2018)	https://github.com/sebastinas/bfe-bf	Software	Free-to-use			Sebastian Ramacher	sebastian.ramacher@ait.ac.at	AIT Austrian Institute of Technology	
OpenSSL with fs-0RTT key exchange	Integration of BFE library in OpenSSL to provide an efficient Forward-secret zero round-trip time key exchange in TLS 1.3.	https://github.com/sebastinas/openssl-bfe	Software	Free-to-use			Sebastian Ramacher	sebastian.ramacher@ait.ac.at	AIT Austrian Institute of Technology	
Online Anomaly Detection	Analytical Toolbox for Online Anomaly Detection. This includes: (1) Classical and Deep Neuronal Network based models for anomaly detection, and (2) a software platform to perform online anomaly detection and learning.		Software	Protected	D4.3.2;#26		Christian Lettner	christian.lettner@scch.at	SCCH Software Competence Center Hagenberg	
Concept for secure distance estimation using coupled fields.	This paper describes a concept for secure distance estimation using coupled fields. Differently from time-of-flight-based methods, this method is resilient to the distance enlargement fraud.	We've Got the Power: Overcoming the Distance Enlargement Fraud with Wireless Power Transfer	Document	Free-to-use	D3.3;#17		Leo Botler	leo.happbotler@tugraz.at	TU Graz - ITI	Paper
Single-Anchor Localization Approach: E-SALDAT	This paper describes an efficient and collaborative single-anchor localization approach called E-SALDAT. This approach relies on nodes using two spaced antennas and a magnetometer. We evaluated its effectiveness via simulations.	E-SALDAT: Efficient Single-Anchor Localization of Dual-Antenna Tags	Document	Free-to-use	D3.4;#18		Leo Botler	leo.happbotler@tugraz.at	TU Graz - ITI	Paper
Evaluation of BLE and UWB-based AoA for accurate indoor localization	This paper presents a comparison between the angle-of-arrival performances of two ubiquitous technologies in the field of indoor localization, namely Bluetooth Low Energy (BLE) and Ultra-Wideband (UWB). Our experiments show that UWB is, in general, more accurate and precise than BLE.		Document	Free-to-use	D5.4.2;#35		Leo Botler	leo.happbotler@tugraz.at	TU Graz - ITI	Paper.A URL will be provided once the paper is available on IEEExplore.
JiT: Method to increase availability in embedded redundant systems	This papers describes a method to increase availability in COTS redundant systems. The basic approach consists in verifying errors in memory which were overwritten before causing a failure.		Document	Free-to-use			Leo Botler	leo.happbotler@tugraz.at	TU Graz - ITI	Paper. A link will be provided once the paper is available on IEEExplore.
Simulator - E-SALDAT	This simulator implements the localization method E-SALDAT, as well as two existing competitors. It was coded in Python and enables the user to easily configure simulation parameters and error models for specific devices.		Software	Protected	D3.4;#18		Leo Botler	leo.happbotler@tugraz.at	TU Graz - ITI	Internal prototype.
JiT parser	This parser modifies a Cortex-M3 Assembly code introducing JiT. It is suitable for availability-critical applications. The code can be easily ported to different CPU architectures and/or compilers.		Software	Protected			Leo Botler	leo.happbotler@tugraz.at	TU Graz - ITI	Internal prototype.
Simulator - UWB RSS-based distance fraud detection	This simulator aims to verify whether a distance fraud is taking place in a UWB-based distance estimation using signal strength instead of time-of-flight measurements. It accounts for measurements imperfections in the distance estimation using existing models.		Software	Protected	D7.3;#48		Leo Botler	leo.happbotler@tugraz.at	TU Graz - ITI	Internal prototype.
More Efficient Bloom Filter Encryption	A more efficient Bloom-Filter Encryption (BFE) scheme with shorter ciphertexts building on the work by Derler, Jager, Slamanig, and Striecks, for more efficient low-latency key exchange.	https://eprint.iacr.org/2018/199	Document	Free-to-use	D3.6.2;#21		Christoph Striecks	Christoph.Striecks@ait.ac.at	AIT Austrian Institute of Technology	To be published in Journal of Cryptotology.
Dual-Form Puncturable Encryption	An identity-based Puncturable Encryption scheme, dubbed Dual-Form Puncturable Encryption (DFPE) scheme, to have a more scalable encryption scheme with fine-grained access control and strong security guarantees such as forward secrecy.	https://eprint.iacr.org/2019/912	Document	Free-to-use	D3.6.2;#21		Christoph Striecks	Christoph.Striecks@ait.ac.at	AIT Austrian Institute of Technology	Currently in submission.
Post-Quantum Secure Bloom Filter Encryption	A post-quantum secure BFE instantiation from identity-based cryptography techniques. Furthermore, we are able to reduce the decryption error generically present in many only weakly secure post-quantum key encapsulation mechanisms from the literature and show strongly secure variants thereof.		Document	Free-to-use	D3.6.2;#21		Christoph Striecks	Christoph.Striecks@ait.ac.at	_Unknown	Accepted at ASIACRYPT 2020.
Guidelines and recommendations for the use of cryptography to build trustworthy IoT applications	This document gives a short overview of cryptographic schemes that ensure confidentiality, authenticity and integrity for secure communication in IoT applications. This overview also includes a discussion of the typical APIs that cryptographic libraries offer users and are used during the National Institute of Standards and Technology (NIST) competitions to standardize the post-quantum secure digital signature, public-key encryption and key exchange schemes as well as lightweight authenticated encryption schemes. For secure implementations on both on the software as well as the hardware side, this deliverable introduces guidelines and recommendations for implementing cryptographic schemes. For the software side, those guidelines focus on the design of the APIs of cryptographic libraries to make them easily accessible to application developers, but also to ensure their correct usage. On the hardware side, the deliverable introduces guidelines for the secure implementation of lightweight symmetric encryption algorithms on Field Programmable Gate Arrays (FPGAs), so that protocols for secure communication can also be deployed on resource-constrained devices and legacy hardware.		Document	_Unknown	D3.5;#19		Sebastian Ramacher	sebastian.ramacher@ait.ac.at	AIT Austrian Institute of Technology;#SBA Research;#TU Graz - IAIK	
industrial sensor and control networks: Challenges and issues in a real implementation for a smart production use-case	Conference Paper 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)	https://ieeexplore.ieee.org/document/9211995	Document	Free-to-use			Franz Dielacher	Franz.Dielacher@infineon.com	Infineon	
Report on the applicability of tools, methods and models related to connectivity issues in I4.0	related to connectivity issues in Industry 4.0. It discusses challenges and limitation on the application of wired and wireless communication technologies for secure connectivity in smart manufacturing environments. The main IoT4CPS connectivity demonstrators that include AVL´s Device Connect, X-Net Virtual Factory and Infineon´s Device Application for Wireless Industrial Connectivity are presented.	http://iot4cps.at	Document	Free-to-use	D7.2;#47		Franz Dielacher	Franz.Dielacher@infineon.com	AVL;#Infineon;#X-Net	To be published

Applicability of solutions for secure and reliable V2X communications	This deliverable describes all ongoing activities in the context of solutions for secure and reliable V2X communications. Beyond of that examples of hardware for implementation are included. In detail, D6.2 includes the IoT4CPS V2X connectivity use-case and connectivity requirements and challenges for autonomous & connected vehicles. State-of-the-art V2X connectivity technologies and the evolution of 3GPP Standardization for V2X connectivity are discussed in this report. Finally, 5G NR Radio Access Networking and Wireless Infrastructure HW models specifications, recommendations and guidelines for secure and reliable V2X communications are presented.		Document	Protected	D6.2;#42	Franz Dielacher	Franz.Dielacher@infineon.com	Infineon;#NOKIA	confidential
Wireless Connectivity Requirements and Challenges in Industrial IoT Applications	Master Thesis Adeel Ahmed		Document	Protected		Franz Dielacher	Franz.Dielacher@infineon.com	Infineon	not published
Connectivity Requirements and Challenges for mission critical Industrial IoT Applications	Master Thesis Muhammad Arslan Ali		Document	Protected		Franz Dielacher	Franz.Dielacher@infineon.com	Infineon	not published
ThreatGet	subjective expert judgment. ThreatGet helps you innovate this expensive and subjective process by automating the analysis and formalizing threat information. Its analysis results are reusable and all mitigations and design decisions are traceable through the development process. ThreatGet helps saving cost and due to the updatable threat catalogue the analysis stays up-to-date automatically.	https://www.threatget.com/	Software	Protected	D3.7;#22	Cristoph Schmittner	Christoph.Schmittner@ait.ac.at	AIT Austrian Institute of Technology	
MORETO	The Model-based Security Requirement Management Tool (MORETO) serves a tool for security requirements analysis, allocation, and management using modelling languages such as SysML/UML. MORETO is an Enterprise Architect (EA) plugin for managing the IEC 62443 security standard.		Software	Protected	D3.7;#22	Cristoph Schmittner	Christoph.Schmittner@ait.ac.at	AIT Austrian Institute of Technology	
Crypto API Guidelines	The complexity, insecure defaults, and poor documentation of cryptographic APIs are among reasons for frequent developer-induced errors in applications that subsequently lead to security incidents..We address this problem by extensively examining cryptographic APIs with regards to their usability and extract guidelines for improvement.		Document	Free-to-use	D3.5;#19	Katharina Pfeffer	KPfeffer@sba-research.org	SBA Research	
SBI connected virtual factory	The SBI-connected virtual factory consists of a database (SBI-Core) at the machine manufacturer, several VPN hubs (SBI-HUB) also from the machine manufacturer and the gateways (SBI-Box) for the machine user. The SBI-Core ist the central database that manages the SBI-System. Among other things, it manages and provides the SBI-Hubs, SBI-Boxes, connected machines, technicians, audit logs, firewall templates and rules for the SBI-Boxes. The task of the SBI-Hubs is to coordinate the operation of a connection between the service technician, the machine manufacturer or the manufacturer of machine components and the machines. The SBI-Boxes set up at the end user take over several functions. They are primarily used as a gateway to the connected machines. In addition, they can act as a firewall with additional functions and		Hardware	Limited-use	D7.4;#49	Security by Isolation proof of concept;#5	Nikolaus Dürk	nd@x-net.at	X-Net;#Salzburg Research	
SBI flash recording demonstrator	The demonstrator is designed to transfer digital content from de-centrally located data sources into IoT products in a secure and customised way. It makes use of secure communication protocols, single encryption and quality control mechanism to take the recording of data carrier to a completely new level. Quality control mechanism avoid errors during production or in the matching of data to the products. With the combination of different tools and methods like authentication, encryption, access control, remote access, validation and matching processes,		Hardware	Limited-use	D7.4;#49	Security by Isolation proof of concept;#5	Nikolaus Dürk	nd@x-net.at	X-Net
Digital Twin Stack	An open source platform for IoT lifecycle data streaming and metadata management for Digital Twins	https://github.com/iot-salzburg/panta_rhei	Software	Free-to-use	D5.5.1;#36;#D5.5.2;#37;#D5.5.3;#38	WP5-Digital Twin Software Demonstrator;#2	Felix Strohmeier	felix.strohmeier@salzburgresearch.at	Salzburg Research
IoT Discovery Tool	Tool for a safe and reliable detection and classification of IoT devices and network topologies. The IoT Discovery Tool supports setups with Ethernet (IPv4 and IPv6), LoRa, and Bluetooth based communication by default, but due to its flexible architecture additional scanner and analyzer modules can be added very easily.		Software	Protected	D4.5;#29		Heribert Vallant		Joanneum Research
Laboratory demonstrator of reliable IoT discovery and classification	Demonstrates the application range of the IoT Discovery Tool and that automated network mapping of a production site can contribute to obtain an authentic view of the actual network structure and connected equipment at any time		_Unknown	_Unknown	D4.5;#29		Heribert Vallant		Joanneum Research
Functional and formal checks	Novel approaches for formally analyzing hardware, protocols, system architecture as well as test case generation to ensure a secure connection and cooperation of IoT in cyber physical systems.		Document	_Unknown	D4.2;#24		Heribert Vallant		Joanneum Research;#SBA Research;#Siemens;#TU Graz - IAIK;#TU Wien
Report on the applicability of tools, methods and models related to traceability of components and systems throughout lifetime	This deliverable looks into two aspects of IIoT usecases. First, integrity and authenticity checks of complex systems via RoT architectures to achieve traceability through efficient and trustworthy identification and authentication of pre-provisioned devices are investigated. Second, modern localization techniques leveraging new UWB technology are highlighted.		Document	Protected	D7.3;#48		Mario Lamberger	mario.lamberger@nxp.com	TU Graz - ITI
Automated Security Testing for MQTT	Framework for automated security testing using random test case generation guided by attack patterns. The framework includes a demonstrator for security testing of MQTT-based IoT applications (MqttRazzer). Running the demonstrator on popular MQTT broker implementations (Mosquitto, ActiveMQ, etc.) revealed more than 20 security bugs! Contact rudolf.ramler@scch.at for details on how to apply MqttRazzer to your application.		Software	Protected	D4.4.1;#27	Laboratory demonstrator of automated testing final release;#7	Rudolf Ramler	rudolf.ramler@scch.at	SCCH Software Competence Center Hagenberg
A recommender system for dependable IOT applications	The recommender system is intended to suggest a feasible combination of wireless communication technologies (or services) based on the user's specifications.		Software	Protected	D3.1;#15;#D3.2;#16		Lukas Krammer	lukas.krammer@siemens.com	Siemens	Internal prototype.

Guidelines for Implementing Cryptographic Algorithms in Hardware	A short collection of best practices to consider when implementing cryptography in programmable logic.		Document	Free-to-use	D3.5;#19	Martin Matschnig	martin.matschnig@siemens.com	Siemens	
Dynamically Exchangeable Runtime Checkers in HW	Framework to enable a set of hardware-based security checks within a resource-constrained FPGA device. Here the Dynamic Partial Reconfiguration feature of modern FPGAs is used to implement exchangable checkers for random numbers as an example.		Software	Protected	D4.2;#24	Martin Matschnig	martin.matschnig@siemens.com	_Unknown	Internal prototype.
Side-Channel Watermarking for LoRaWAN Using Robust Inter-Packet Timing	Conference Publication about research results on watermarking for protection of low level sensors Abstract: Low-data rate networks typically cannot afford the overhead entailed with security measures because of lack of bandwidth. In this paper we propose a method for embedding digital watermarks in LoRaWAN based sensor systems. With the presented approach, the transmitted messages themselves do not need to be modified. Rather, the inter-packet interval between individual packets is used as a side-channel to carry the security-relevant information. We first examine the specific characteristics of LoRaWAN which are typical also for similar low-data rate wireless networks and then present a feasible, lightweight approach for the generation of the digital watermarks. Subsequently, we analyze first simulation results of two different differential methods for the watermark implementation. Published in:	https://doi.org/10.1109/ETFA46521.2020.9211875	Document	Limited-use	D9.4;#58	Albert Treytl	albert.treytl@donau-uni.ac.at	Donau-University Krems	Published via IEEE. Terms and conditions of use according to IEEE explore
Simulation environment and LoRa testbed for watermark-based security for sensor connection	This test-bed for industrial application of watermark-based security measures contains: a) A Phyton-based simulation environment to evaluate properties of watermarks embedded both in sensor data as well as in side-channels. This environment allows investigations of watermark-based security measures in sensor networks. b) A proof-of-concept implementation using LoRa and side-channel-based watermarks for measurements in LP/WAN technologies to interconnect remote sensors in highly distributed industrial environments but also other applications		Software	Protected	D3.6.2;#21	Albert Treytl	albert.treytl@donau-uni.ac.at	_Unknown;#Donau-University Krems	