Security Matters and How It Is Now So Easy

A Leading Provider of Smart, Connected and Secure Embedded Control Solutions

Presenter: Chris Kim – Senior Embedded Solutions Engineer

Date: March 15, 2022

IoT Made Easy

Security is a Duty for Every Professional to Implement

SMART | CONNECTED | SECURE

MICROCHIP

Why Security for IoT?

Save Costs, Reduce Risk, Increase Revenue

Brand Reputation

Privacy and Safety

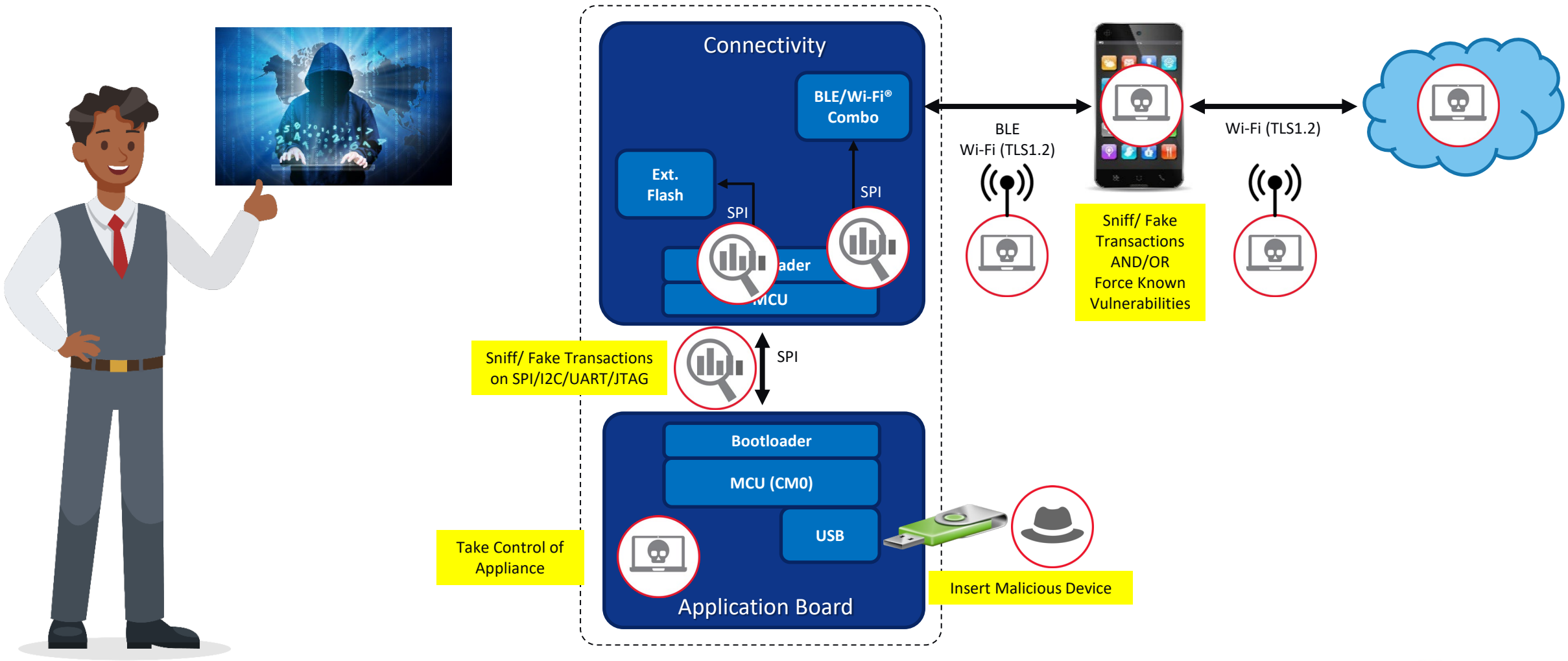
Revenue Stream Protection

Liability and Regulation

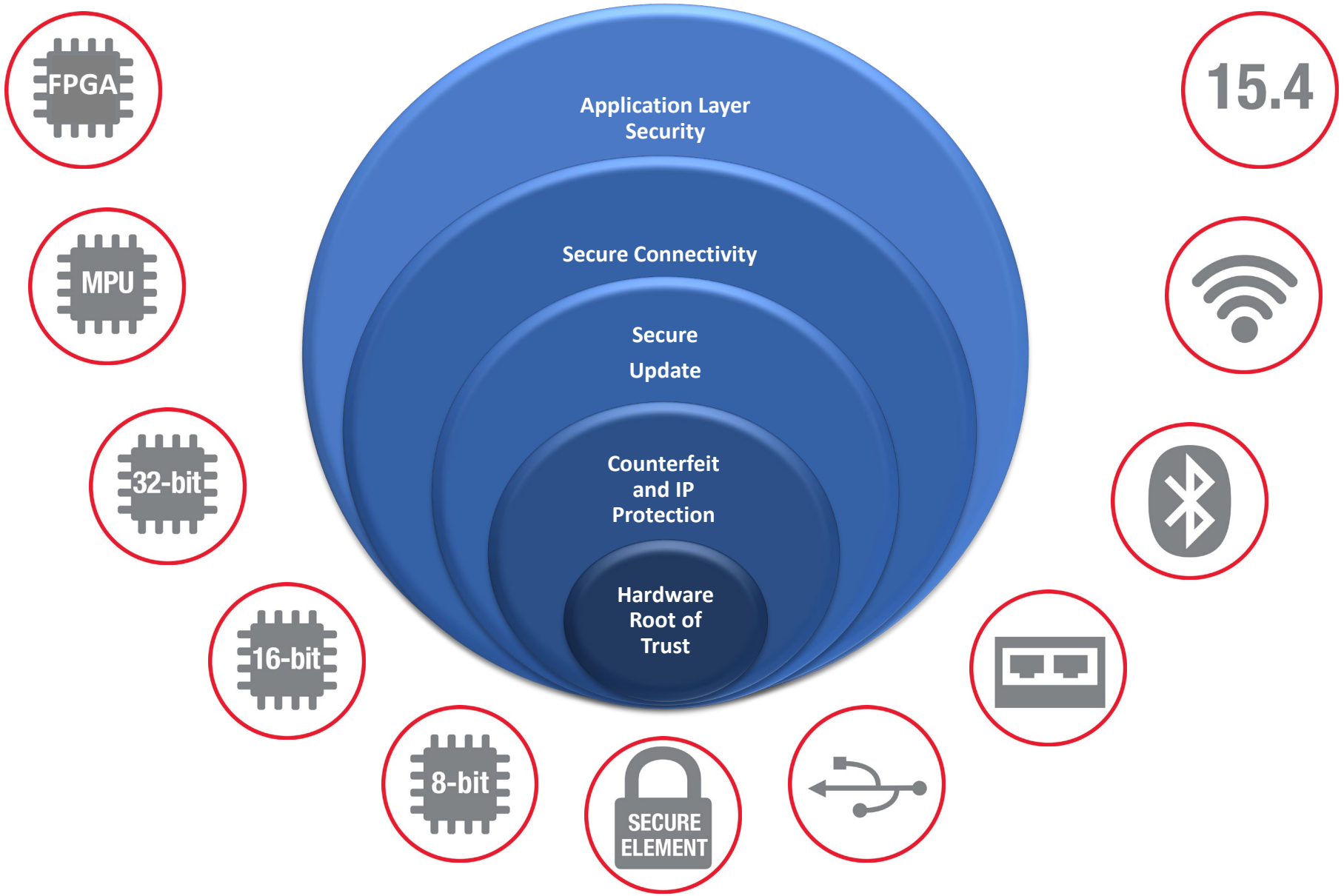
MICROCHIP

Start with a Threat Model

Example: Building Access Authorization



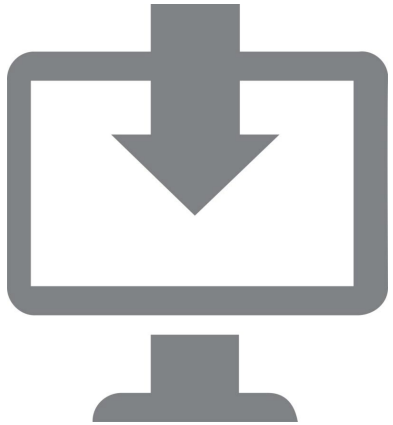
Anatomy of a Secure Embedded System



MICROCHIP

Hardware Root of Trust for An IoT Device

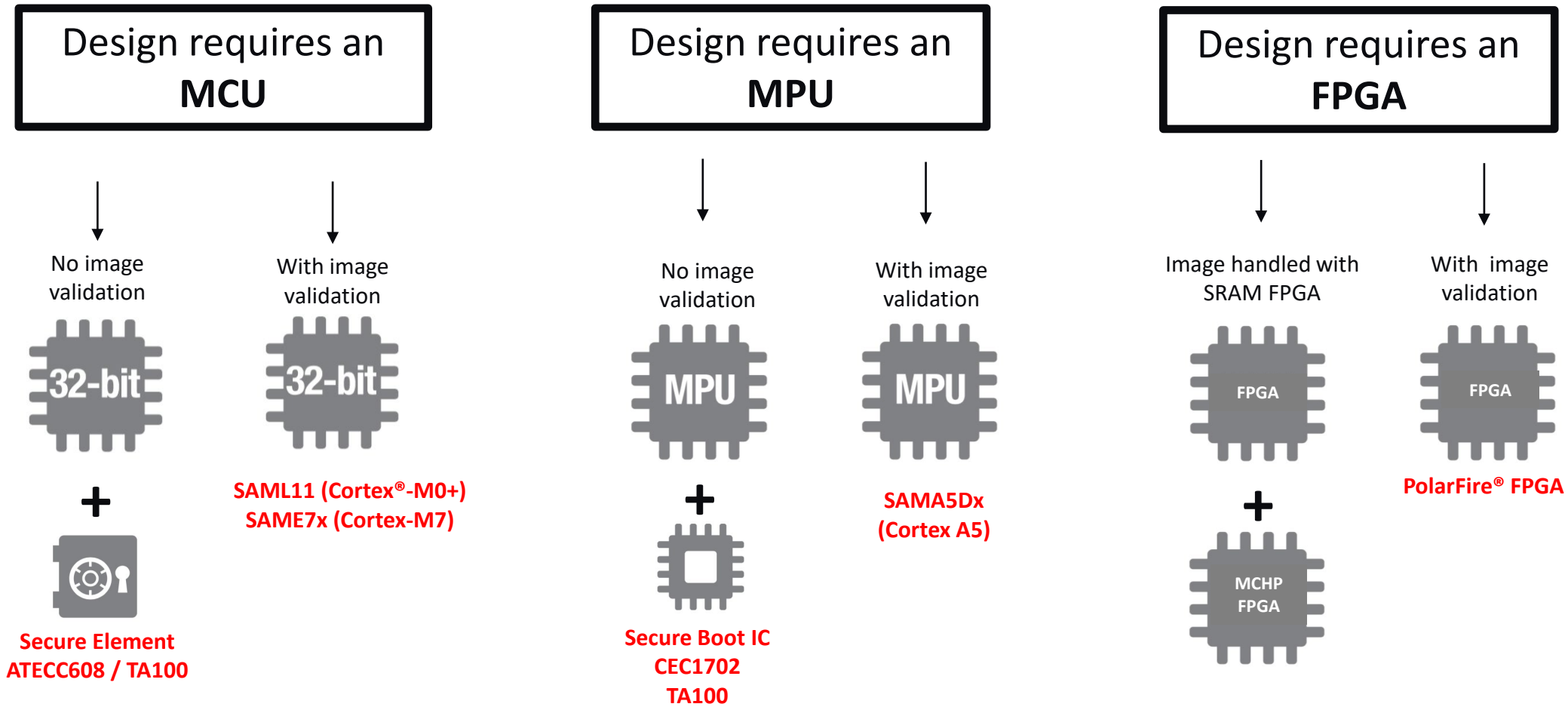
A hardware root of trust consists of **2 attributes**



Secure
Boot

Unique Trusted
Protected Identity

Implementing Secure Boot



MICROCHIP

Adding Unique, Trusted, Protected Identity

X509 CERTIFICATES

SELF SIGNED CERTIFICATES

JSON WEB TOKEN

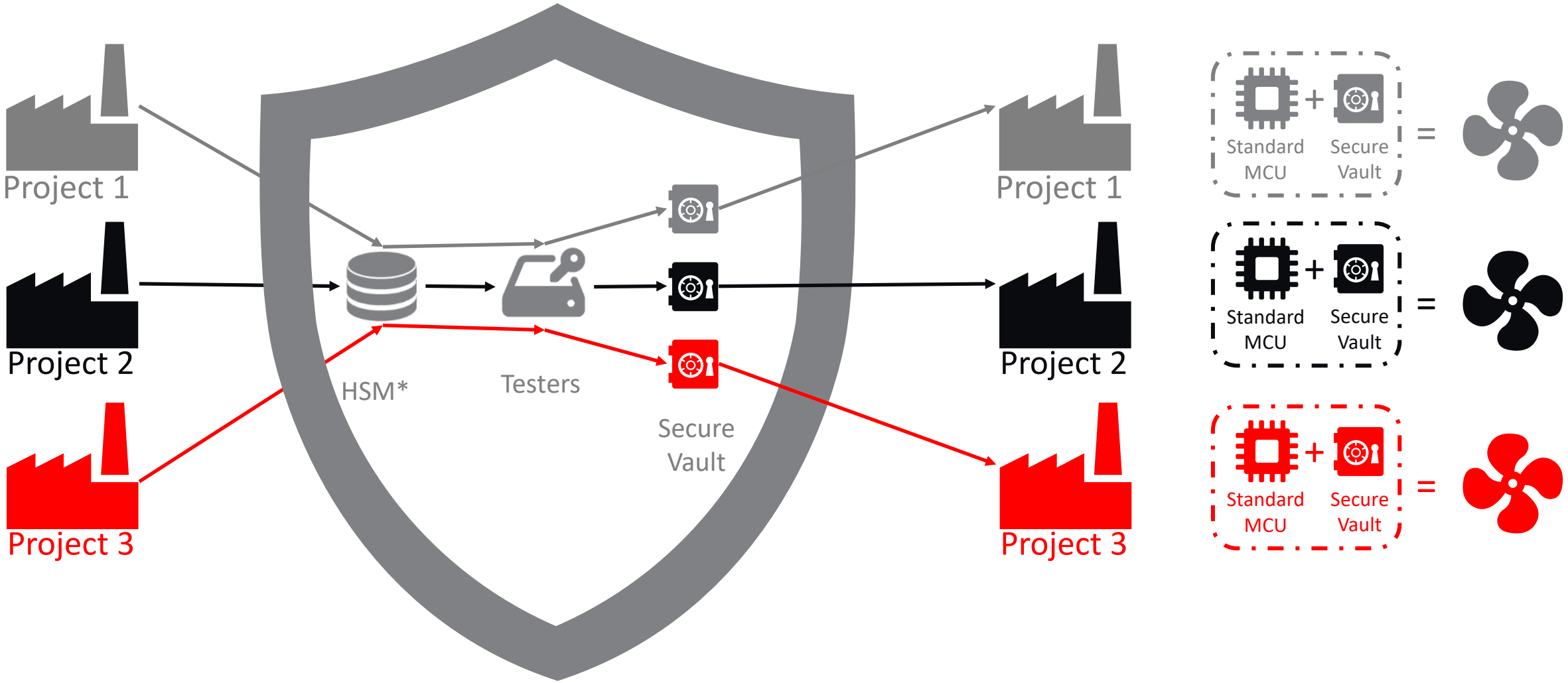
SYMETRIC KEYS

PUF

Remember if **I have the key, I AM YOU**

How to provision the key inside your secure silicon?

Secure Key Provisioning: Trust Platform



*HSM: hardware security module in isolated network and dedicated secure rooms

MICROCHIP

Trust Platform: Pre-configuration

	TRUST&GO	TRUST FLEX	TRUST CUSTOM
Pre-configured	YES	YES	NO
Development Time	Lowest	Lower	Custom
Complexity	Lowest	Lower	Custom
Low Volume MOQ (<100 ku EAU)	10 units	2,000 units	4,000 units
High Volume MOQ (>100 ku EAU)	Starting 30,000 units	Starting 30,000 units	Starting 30,000 units
Secure Key Storage	JIL High	JIL High	JIL High
Use Cases	TLS authentication LoRaWan® authentication	TLS authentication LoRaWan authentication Token authentication Key rotation Firmware verification (OTA, Secure boot) IP protection Public key attestation (A-)symmetric Accessories authentication (A-)symmetric Disposable authentication	Fully customizable
Devices	ATECC608	ATECC608	ATECC608 ATSHA204A (w/o RBH)

MICROCHIP

Counterfeit / IP Protection

Gaming Accessories

Drone

Hair Dryer

HW Maintenance (Recurring Service)

Missile

Medical Accessories

Cosmetic Solutions

Medical Disposable

MICROCHIP

Counterfeit / IP Protection

Host has **low** value

8-bit

HOST

CLIENT

Shared Key

Value in cartridge

Secure Element ATSHA204A

Host has value

32-bit

Secure Element ATSHA204A

HOST

CLIENT

Shared Key

Value in replacement part

Secure Element ATSHA204A

Host has value

MPU

HOST

CLIENT

PKI

Value in accessory

Secure element ATECC608

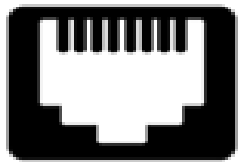
MICROCHIP

Secure Update

- **Secure remote Over-the-air** (OTA) update
- **Local update** (example: USB stick) assuming the SW or FW to be updated is securely stored in the source
- Code/ software/ image **signing and verification**
- **Secure loader** (SW that does the update) needs to authenticate the target device, file or system

Secure and Private Communication

Secure communication is ensured with **authentication** capabilities between a host and a client.


Ethernet

Privacy** is ensured by **encryption/ decryption

Application Layer Security

- Security is applied to the application layer specifically to **protect against unauthorized access**
  - Disable keys or firmware operation upon tamper detection
  - Code Integrity monitoring
  - User permission/ access authorization
  - Kernel separation
  - Multizone security
  - Key zeroization
  - Secure code provisioning
  - Image signing/ verification

Conclusion

Microchip is here to support you during your journey

- **Security is a necessity for all stakeholders including end users**
- **Secure your designs NOW, as IoT regulation is already in place**
- **Microchip offers a comprehensive variety of solutions for IoT security**

MICROCHIP

And for Even More...

Shields UP! webinars

Microchip.com/**ShieldsUP**

Quick Start with No Compromise in IoT Designs

A Leading Provider of Smart, Connected and Secure Embedded Control Solutions

Presented by: Chris Kim – Senior Embedded Solutions Engineer

March 15, 2022

The Challenge – IoT designs are complex

Solutions for Rapid Prototyping and Reduced Time to Production

- **Design complexity and risk management**
- **Flexibility and innovation**
- **Fast time-to-production**

MICROCHIP

Development Tool Ecosystem

Discover

Feature
Application
Software

MPLAB DISCOVER

Configure

System init
Device init
Peripheral init

MPLAB CODE CONFIGURATOR
MPLAB HARMONY

Develop

IDEs, Compilers
Example code
Software Stacks

MPLAB X IDE
MPLAB XPRESS IDE
MICROCHIP STUDIO FOR AVR® AND SAM DEVICES
MPLAB XC COMPILER
GCC

Debug

Eval boards
Debuggers
Data Visualizer

MPLAB SNAP IN-CIRCUIT DEBUGGER
MPLAB DATA VISUALIZER
MPLAB PICKIT 4 IN-CIRCUIT DEBUGGER
MPLAB ICD4

Qualify

Code coverage
Code profiling
Functional safety

TÜV SÜD
MPLAB CODE COVERAGE

Production

Programmers
Prog Center
3rd Party

MPLAB IPE
Softlog Systems
XELTEK HOME OF AUTOMATED PROGRAMMERS

Support clients from product concept through release

MICROCHIP

Development Tool Ecosystem

Discover

Feature
Application
Software

MPLAB DISCOVER

Configure

System init
Device init
Peripheral init

MPLAB CODE CONFIGURATOR
MPLAB HARMONY

Develop

IDEs, Compilers
Example code
Software Stacks

MPLAB X IDE
MPLAB XPRESS IDE
MICROCHIP STUDIO FOR AVR® AND SAM DEVICES
MPLAB XC COMPILER
GCC

Debug

Eval boards
Debuggers
Data Visualizer

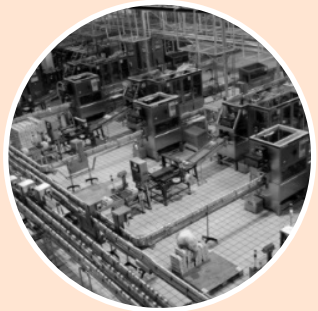
MPLAB SNAP IN-CIRCUIT DEBUGGER
MPLAB DATA VISUALIZER
MPLAB PICKIT 4 IN-CIRCUIT DEBUGGER
MPLAB ICD4

Qualify

Code coverage
Code profiling
Functional safety

TÜV SÜD
MPLAB CODE COVERAGE

Production



Programmers
Prog Center
3rd Party

MPLAB IPE
Softlog Systems
XELTEK HOME OF AUTOMATED PROGRAMMERS

Support clients from product concept through release

MICROCHIP

Discover

MPLAB Discover

- **Search and discover everything you need for your project**
- **Find information from multiple repositories**
- **Easy sorting with multiple categories and filtering**
- **Import code into MPLAB Code Configurator for the next step of your design**
- **Includes:**
  - Code Examples
  - Libraries
  - Data Sheets
  - Application Notes

MICROCHIP

Configure

Discover

Feature
Application
Software

MPLAB DISCOVER

Configure

System init
Device init
Peripheral init

MPLAB CODE CONFIGURATOR

MPLAB HARMONY

Develop

IDEs, Compilers
Example code
Software Stacks

MPLAB X IDE

MPLAB XPRESS IDE

MICROCHIP STUDIO FOR AVR® AND SAM DEVICES

MPLAB XC COMPILER

GCC

Debug

Eval boards
Debuggers
Data Visualizer

MPLAB SNAP IN-CIRCUIT DEBUGGER

MPLAB DATA VISUALIZER

MPLAB PICkit 4 IN-CIRCUIT DEBUGGER

MPLAB ICD4

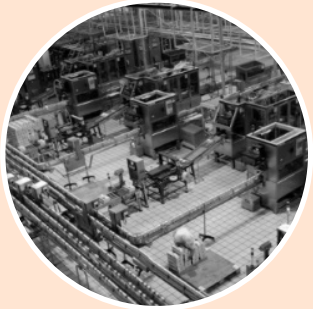
Qualify

Code coverage
Code profiling
Functional safety

TÜV SÜD

MPLAB CODE COVERAGE

Production



Programmers
Prog Center
3rd Party

MPLAB IPE

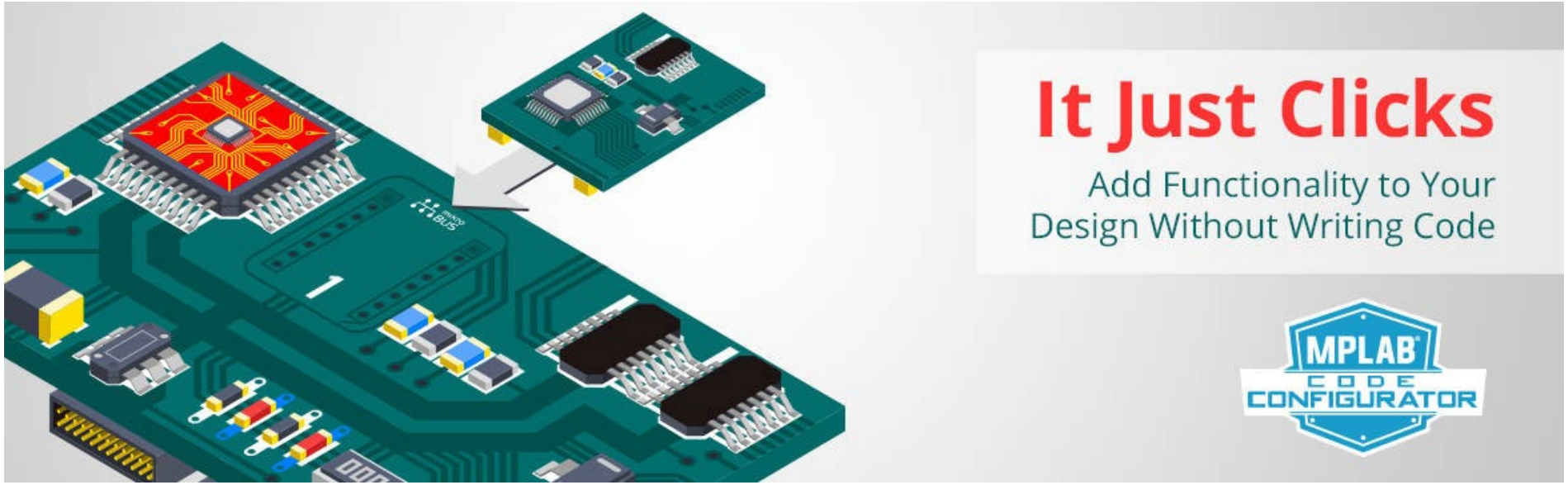
Softlog Systems

XELTEK
HOME OF AUTOMATED PROGRAMMERS

Support clients from product concept through release

MICROCHIP

Configure



- **Free graphical programming environment**
- **Intuitive interface to quick start development**
- **Automated configuration of peripherals**
- **Accelerates generation of production-ready code**

MICROCHIP

Configure

- Free development environment
- Easy to use graphical configuration features
- Point-and-click options selections
- Optimized peripheral libraries to simplify device setup
- Modular downloads and updates through GitHub
- Easy integration with FreeRTOS

MICROCHIP

Development Tool Ecosystem

Discover

Feature
Application
Software

MPLAB DISCOVER

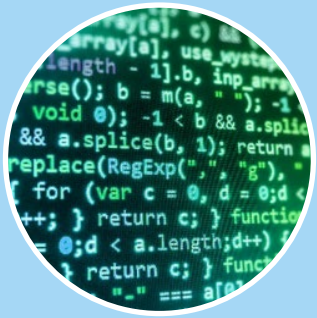
Configure

System init
Device init
Peripheral init

MPLAB CODE CONFIGURATOR

MPLAB HARMONY

Develop



IDEs, Compilers
Example code
Software Stacks

MPLAB X IDE

MPLAB XPRESS IDE

MICROCHIP STUDIO FOR AVR® AND SAM DEVICES

MPLAB XC COMPILER

GCC

Debug

Eval boards
Debuggers
Data Visualizer

MPLAB SNAP IN-CIRCUIT DEBUGGER

MPLAB DATA VISUALIZER

MPLAB PICKIT 4 IN-CIRCUIT DEBUGGER

MPLAB ICD4

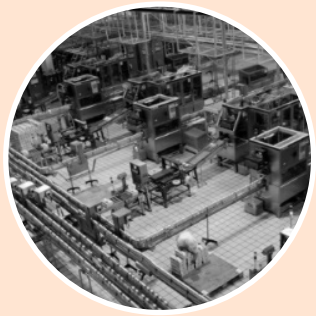
Qualify

Code coverage
Code profiling
Functional safety

TÜV SÜD

MPLAB CODE COVERAGE

Production



Programmers
Prog Center
3rd Party

MPLAB IPE

Softlog Systems

XELTEK HOME OF AUTOMATED PROGRAMMERS

Support clients from product concept through release

MICROCHIP

Develop

- **All Microchip devices are supported**
- **Pick a compiler by device:**
  - MPLAB® XC8 for 8-bit PIC® and AVR® devices
  - MPLAB XC16 for 16-bit PIC and dsPIC® devices
  - MPLAB XC32 for 32-bit PIC, SAM and MPU devices
- **Code optimizations provide smaller and more efficient code**
- **Pick your optimization level:**
  - 70% of optimizations available with free download
  - Additional optimizations maximize your code savings with PRO licenses
- **Pick a license type: workstation, network server, site, subscription or dongle**

Develop

- **GCC Toolchain**
  - Includes compiler, assembler, linker and Standard C and math libraries
- **Device-specific optimizations included**
  - Provides smaller, more efficient code than open source version
- **Pick your toolchain based on device:**
  - AVR GCC for AVR® devices
  - ARM GCC for SAM devices

MICROCHIP

Develop

Power Up with MPLAB® X IDE

The MPLAB Ecosystem Now Supports MPUs

- **Pick your operating system: Windows®, Linux® and macOS®**
- **Pick your compiler: MPLAB® XC, GCC or third party**
- **Pick your programmer/debugger:**
  - MPLAB ICD 4, MPLAB PICkit™ 4, MPLAB Snap
  - J-32 Debug Probe
  - Atmel-ICE
  - Third-party
- **Extensions let you do even more!**

MPLAB® X IDE

MICROCHIP

Develop

- **Now supported by MPLAB XC Compilers**
  - Includes MPLAB Functional Safety licenses
- **Develop and debug all AVR® and SAM MCU applications**
- **Connect seamlessly to debuggers, programmers and Xplained kits**
- **Extend functionality with plug-ins**
- **Seamless import of Arduino sketches as C++ projects**
  - Easy transition from makerspace to marketplace
- **Seamless import of projects from Atmel START**

Development Tool Ecosystem

Discover

Feature
Application
Software

MPLAB DISCOVER

Configure

System init
Device init
Peripheral init

MPLAB CODE CONFIGURATOR
MPLAB HARMONY

Develop

IDEs, Compilers
Example code
Software Stacks

MPLAB X IDE
MPLAB XPRESS IDE
MICROCHIP STUDIO FOR AVR® AND SAM DEVICES
MPLAB XC COMPILER
GCC

Debug

Eval boards
Debuggers
Data Visualizer

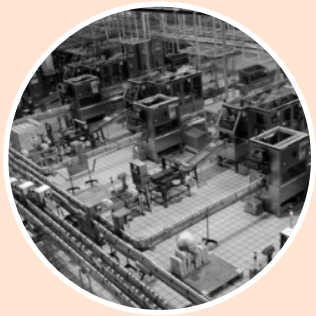
MPLAB SNAP IN-CIRCUIT DEBUGGER
MPLAB DATA VISUALIZER
MPLAB PICKIT 4 IN-CIRCUIT DEBUGGER
MPLAB ICD4

Qualify

Code coverage
Code profiling
Functional safety

TÜV SÜD
MPLAB CODE COVERAGE

Production



Programmers
Prog Center
3rd Party

MPLAB IPE
Softlog Systems
XELTEK HOME OF AUTOMATED PROGRAMMERS

Support clients from product concept through release

MICROCHIP

Debug

MPLAB SNAP IN-CIRCUIT DEBUGGER

MPLAB PICkit 4 IN-CIRCUIT DEBUGGER

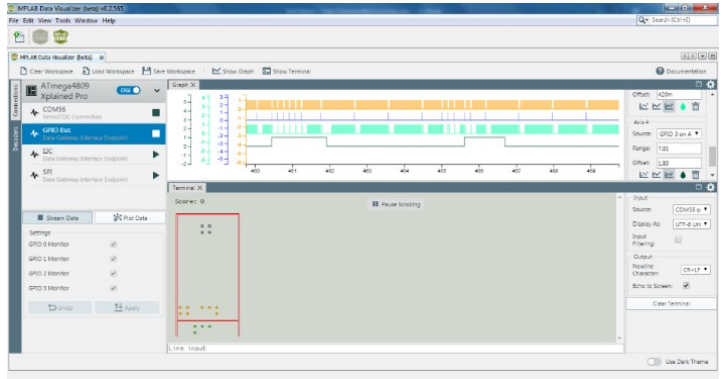
J-32 Debug Probe
MICROCHIP
Developed by SEGGER
www.segger.com

MPLAB ICD 4

MICROCHIP

Debug

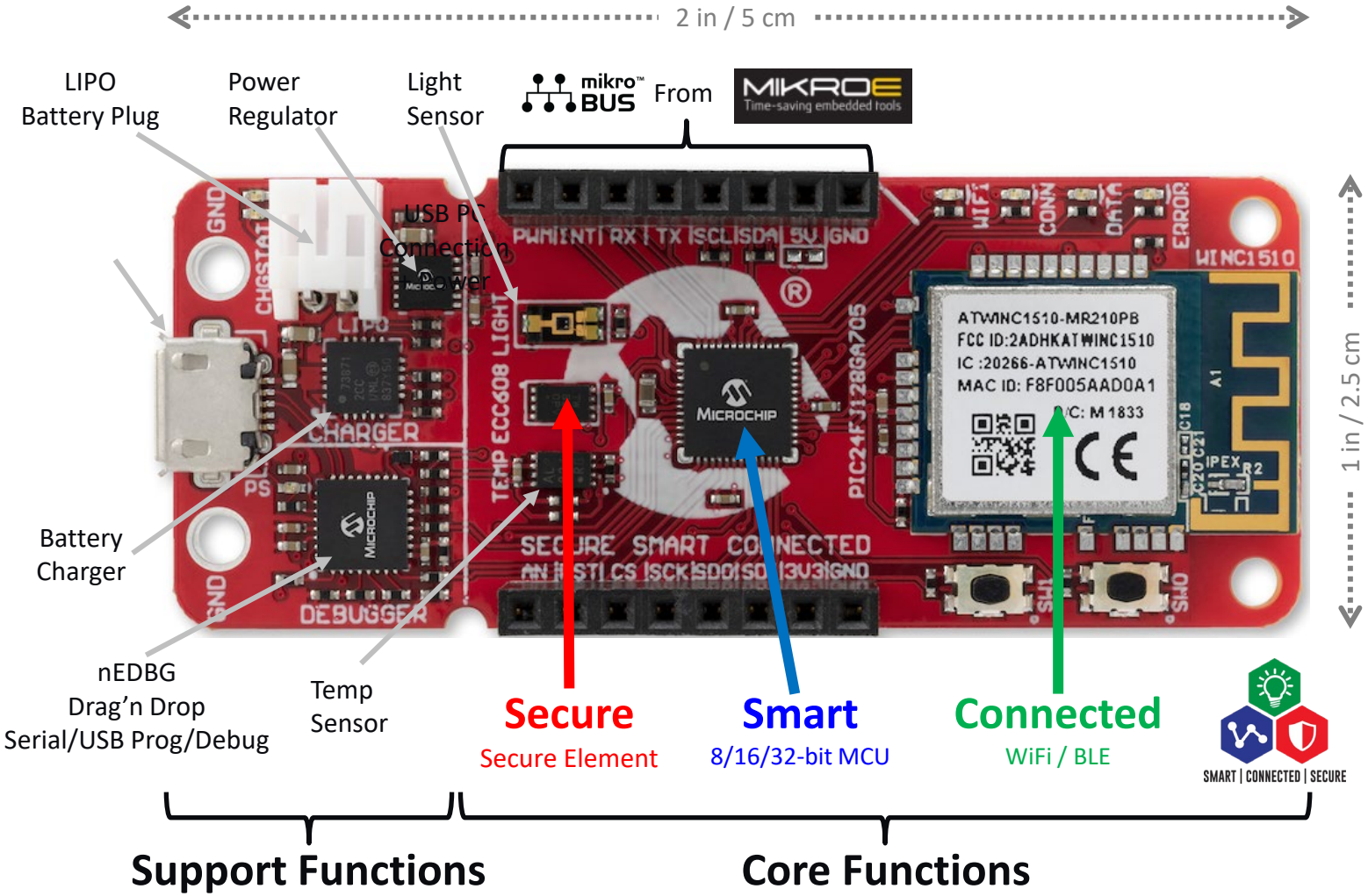
MPLAB ® Data Visualizer



- Free MPLAB X IDE extension or stand-alone application
- Debug data in near real-time
- Graph in single or multiple plots
- Stream via serial port (CDC) or Data Gateway Interface (DGI)
  - Xplained and Curiosity boards supported out of the box!

Debug

Flexible and Rapid Prototyping with IoT Development Boards



Development Tool Ecosystem

Discover

Feature
Application
Software

MPLAB DISCOVER

Configure

System init
Device init
Peripheral init

MPLAB CODE CONFIGURATOR
MPLAB HARMONY

Develop

IDEs, Compilers
Example code
Software Stacks

MPLAB X IDE
MPLAB XPRESS IDE
MICROCHIP STUDIO FOR AVR® AND SAM DEVICES
MPLAB XC COMPILER
GCC

Debug

Eval boards
Debuggers
Data Visualizer

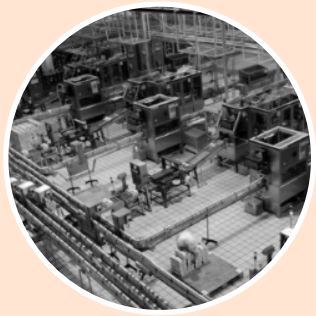
MPLAB SNAP IN-CIRCUIT DEBUGGER
MPLAB DATA VISUALIZER
MPLAB PICKIT 4 IN-CIRCUIT DEBUGGER
MPLAB ICD4

Qualify

Code coverage
Code profiling
Functional safety

TÜV SÜD
MPLAB CODE COVERAGE

Production



Programmers
Prog Center
3rd Party

MPLAB IPE
Softlog Systems
XELTEK HOME OF AUTOMATED PROGRAMMERS

Support clients from product concept through release

MICROCHIP

Qualify

MPLAB® Code Coverage

- Easily see which code has been executed
  - Run tests untethered
  - Minimal impact to program memory and execution speed
    - Typical addition to code size is <1%
- Create custom reports and configurable summary views
- Works with any MPLAB XC C Compiler
  - No PRO license required!

MICROCHIP

Qualify

- **Certified by TÜV SÜD for standards: ISO 26262, IEC 61505, IEC 62304, IEC 60730**
- **Installer package includes:**
  - TÜV SÜD Certificate
  - Functional Safety Manual
  - Safety Plan
  - Tools classification and Qualification report for MPLAB® XC compilers, MPLAB X IDE, MPLAB debuggers/programmers
- **License is perpetual – unlocks any version of Functional Safety compiler**
- **Any version of documentation is purchasable separately**

Development Tool Ecosystem

Discover

Feature
Application
Software

MPLAB DISCOVER

Configure

System init
Device init
Peripheral init

MPLAB CODE CONFIGURATOR
MPLAB HARMONY

Develop

IDEs, Compilers
Example code
Software Stacks

MPLAB X IDE
MPLAB XPRESS IDE
MICROCHIP STUDIO FOR AVR® AND SAM DEVICES
MPLAB XC COMPILER
GCC

Debug

Eval boards
Debuggers
Data Visualizer

MPLAB SNAP IN-CIRCUIT DEBUGGER
MPLAB DATA VISUALIZER
MPLAB PICKIT 4 IN-CIRCUIT DEBUGGER
MPLAB ICD4

Qualify

Code coverage
Code profiling
Functional safety

TÜV SÜD
MPLAB CODE COVERAGE

Production

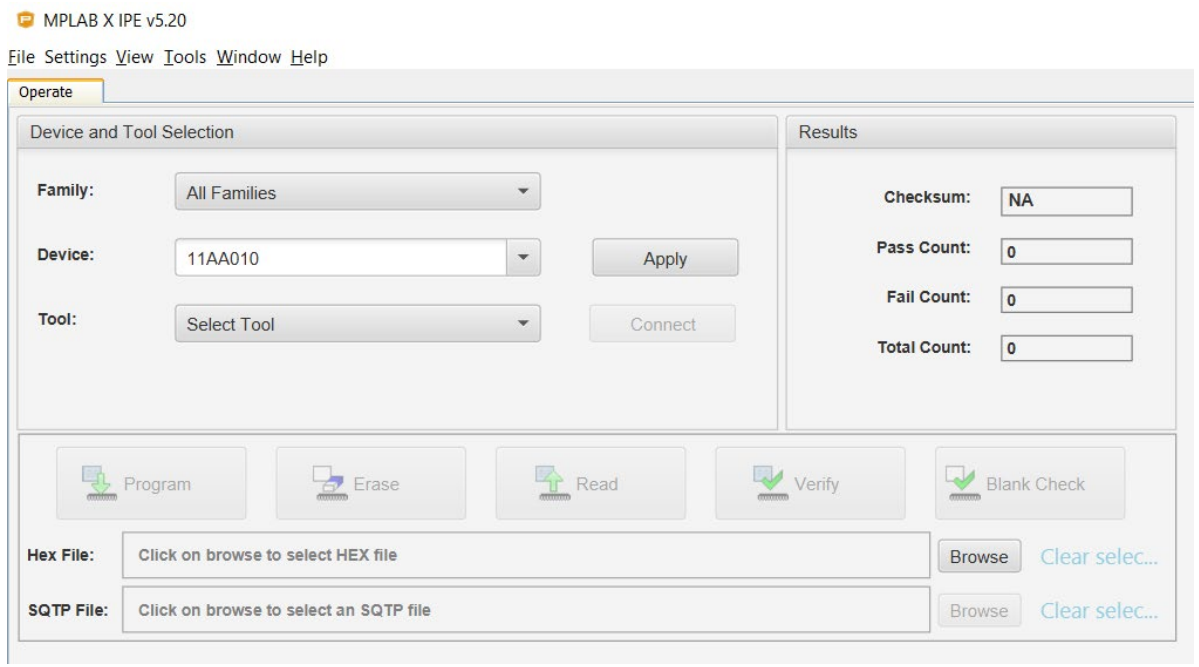
Programmers
Prog Center
3rd Party

MPLAB IPE
Softlog Systems
XELTEK HOME OF AUTOMATED PROGRAMMERS

Support clients from product concept through release

MICROCHIP

Production



- **MPLAB® IPE**
  - Programming-only environment
    - Easy technician views
    - Loadable configurations for quick set-up
    - Use with your favorite MPLAB programmer or third-party programmers
      - SEGGER J-Link Programmer
      - Softlog gang programmers
- **Pick your device: PIC®, dsPIC®, AVR® and SAM**
- **Pick your operating system: Windows®, Linux®, and macOS®**

MICROCHIP

Conclusion

IoT Design is Complex… Microchip simplifies the journey

- **Wide range of tools supporting any cloud and any core**
- **Support and experience for your design at all phases.**
- **Reduce design risk without limiting innovation in your IoT designs**

MICROCHIP

Learn more

Resources

- **Microchip IoT Landing Page**
  - www.microchip.com/iot
- **Microchip Security Landing Page**
  - www.microchip.com/security
- **Github**
  - https://github.com/MicrochipTech
- **Microchip YouTube Channel**
  - www.youtube.com/user/MicrochipTechnology
- **Microchip University**
  - https://secure.microchip.com/mu
- **Design Partner:**
  - https://get.microchipdirect.com/design-partner-ecosystem/

Thank You