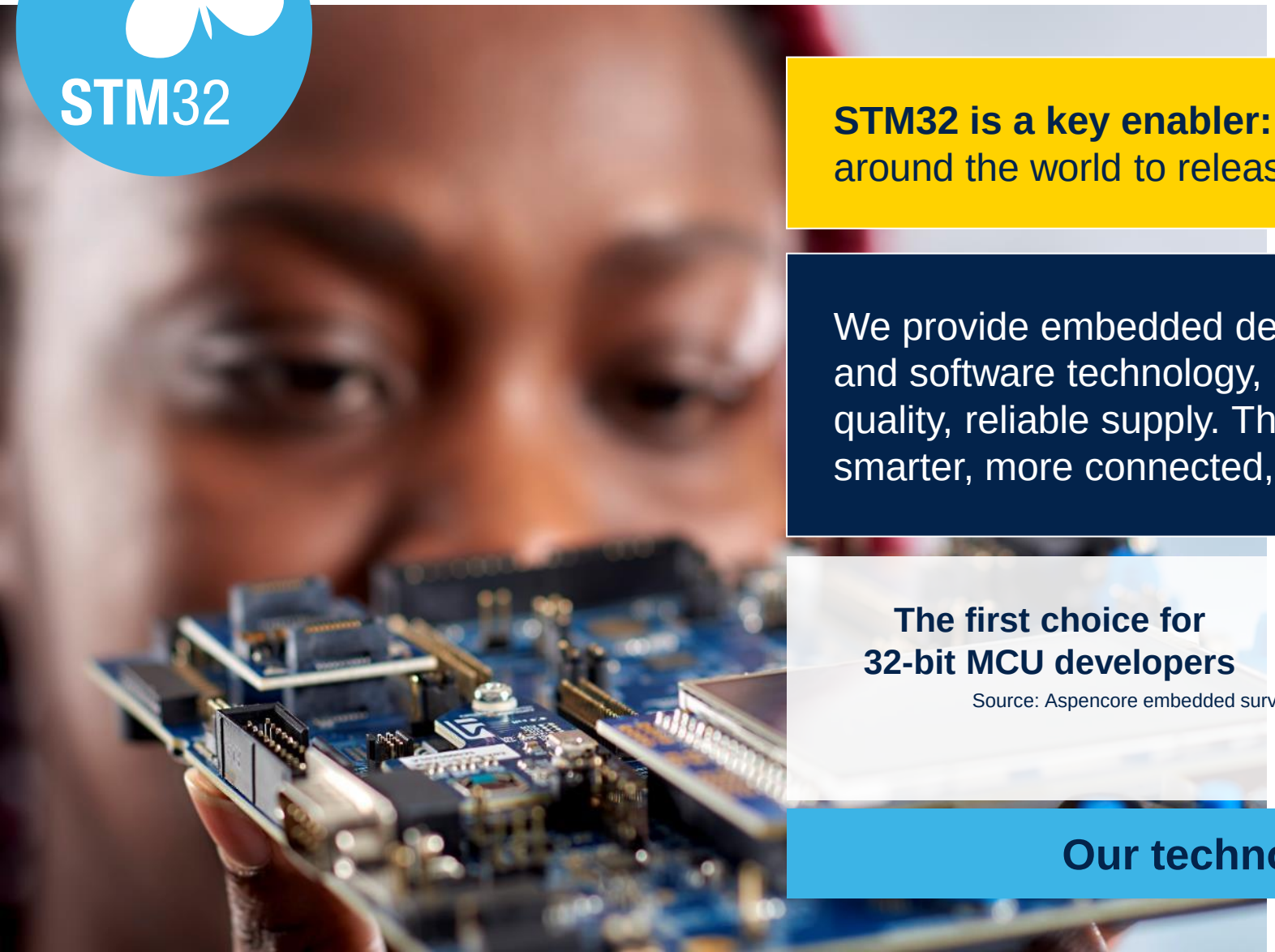
STM32
Digital Power Solutions

STMicroelectronics

Kevin Liang

STM32: a developer-first strategy since 2007



STM32 is a key enabler: empowering embedded developers around the world to release their creativity.

We provide embedded developers with cutting-edge hardware and software technology, comprehensive support, and high-quality, reliable supply. This helps them build designs that are smarter, more connected, and more secure.

The first choice for 32-bit MCU developers

Source: Aspencore embedded survey, 2022

#1 GP MCU Worldwide

Source: OMDIA CLT, 2022, 2023

100,000+ customers

Our technology starts with You

STM32 portfolio

LONGEVITY 10 YEARS COMMITMENT

MPU

- **STM32MP1** — 1 GHz Cortex-A7, 209 MHz Cortex-M4
- **STM32MP2** — Dual 1.5 GHz Cortex-A35, 400 MHz Cortex-M33

High-performance MCUs

- **STM32F7** — 1,082 CoreMark, 216 MHz Cortex-M7
- **STM32H7** — 3347 CoreMark, Up to 600 MHz Cortex -M7, 240 MHz Cortex -M4
- **STM32N6** — 3,360 CoreMark, 800 MHz Cortex -M55, Neural processing unit
- **STM32F2** — 398 CoreMark, 120 MHz Cortex-M3
- **STM32F4** — 608 CoreMark, 180 MHz Cortex-M4
- **STM32H5** — 1,023 CoreMark, 250 MHz Cortex-M33

Mainstream MCUs

Mixed-signal MCUs

- **STM32F3** — 245 CoreMark, 72 MHz Cortex-M4
- **STM32G4** — 569 CoreMark, 170 MHz Cortex-M4
- **STM32C0** — 114 CoreMark, 48 MHz Cortex M0+
- **STM32F0** — 106 CoreMark, 48 MHz Cortex-M0
- **STM32G0** — 142 CoreMark, 64 MHz Cortex-M0+
- **STM32F1** — 177 CoreMark, 72 MHz Cortex-M3

Ultra-low-power MCUs

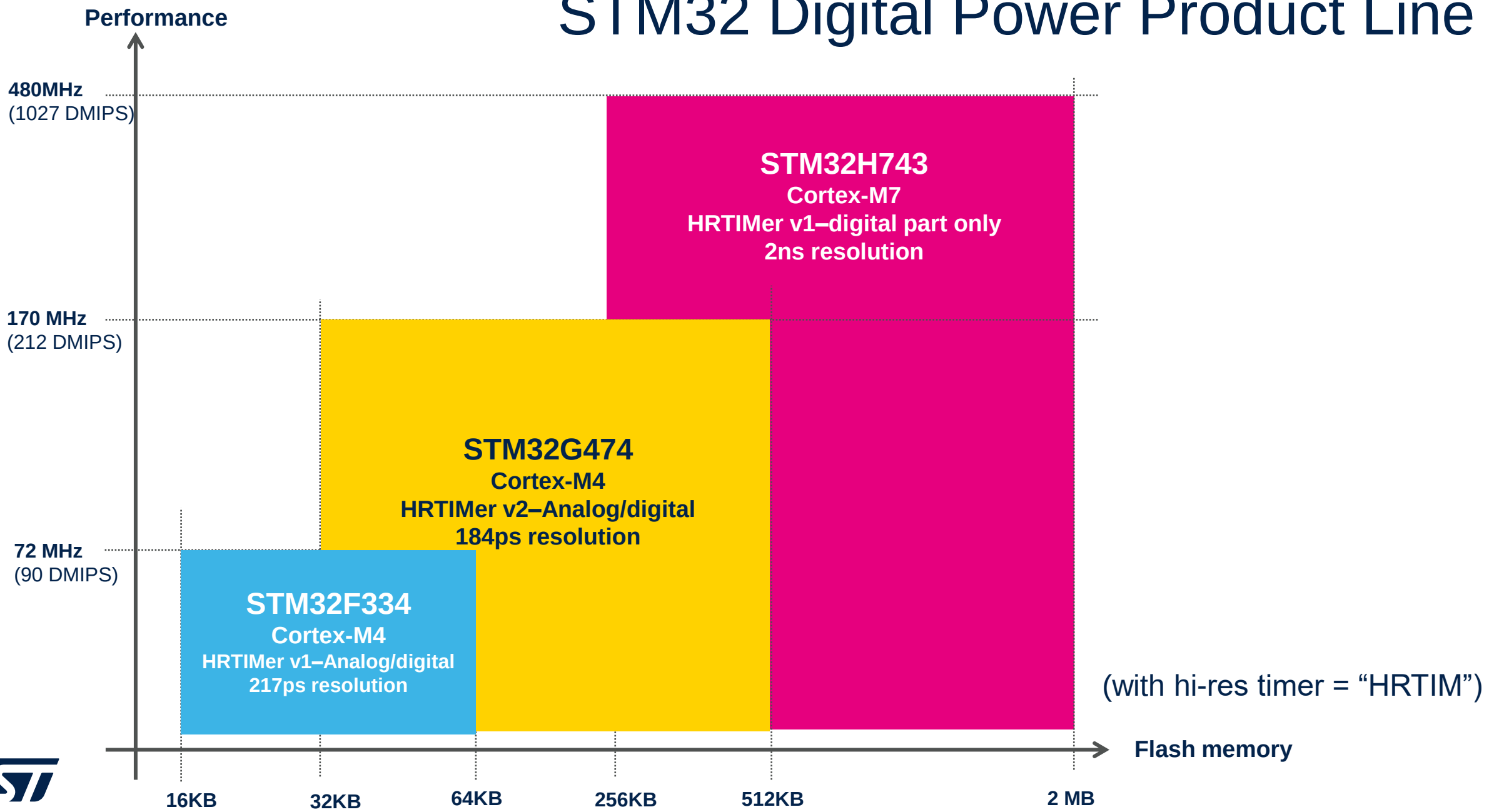
- **STM32L0** — 75 CoreMark, 32 MHz Cortex-M0+
- **STM32U0** — 140 CoreMark, 56 MHz Cortex-M0+
- **STM32L4** — 273 CoreMark, 80 MHz Cortex-M4
- **STM32U3** — 393 CoreMark, 96 MHz Cortex-M33
- **STM32L4+** — 409 CoreMark, 120 MHz Cortex-M4
- **STM32L5** — 443 CoreMark, 110 MHz Cortex-M33
- **STM32U5** — 651 CoreMark, 160 MHz Cortex-M33

Wireless MCUs

- **STM32WL** — 162 CoreMark, 48 MHz Cortex-M4, 48 MHz Cortex-M0+
- **STM32WB0** — 156 CoreMark, 64 MHz Cortex-M0+
- **STM32WB** — 216 CoreMark, 64 MHz Cortex-M4, 32 MHz Cortex-M0+ ●
- **STM32WBA** — 407 CoreMark, 100 MHz Cortex-M33

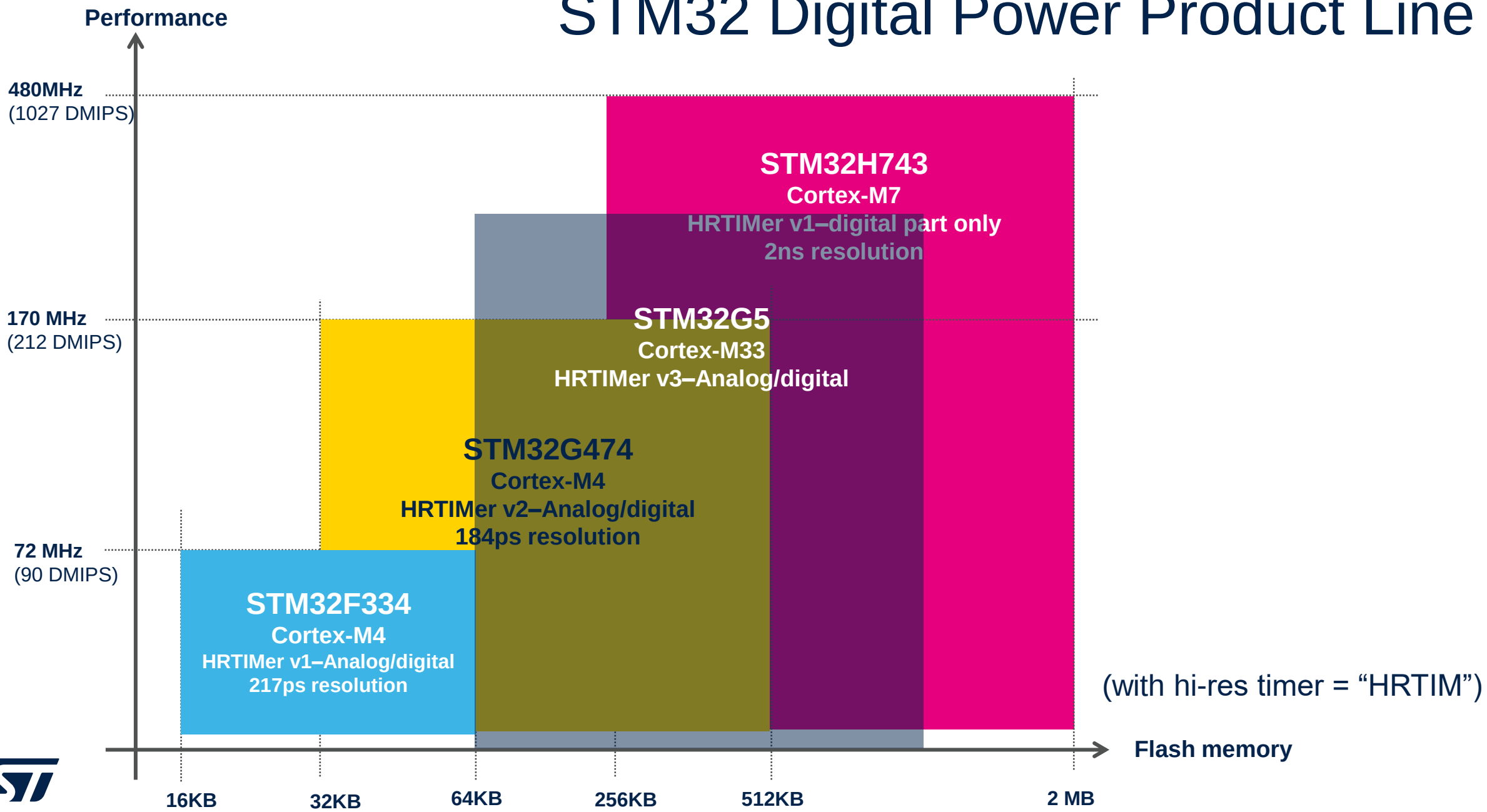
Latest product generation ● Radio coprocessor only ▭ New series or lines introduced in 2025

STM32 Digital Power Product Line



(with hi-res timer = “HRTIM”)

STM32 Digital Power Product Line



(with hi-res timer = “HRTIM”)

STM32G4 Series for Digital Power

High performance

Arm® Cortex®-M4 + FPU running @ 170MHz
+ 3x accelerators: ART, routine booster (CCM),
Math. accelerator (Cordic and FMAC)

7x comparators

Down to 19 ns propagation delay

5 x ADC

5x12-bit, 16-bit oversampling
4 MSPS (0.25µs)

7 x DAC

12-bit DAC 15 Msps

Motor control timer & high-resolution Timer (D-Power)

12 channels up to 184 ps resolution

STM32G4

Security

Arm PSA Level 1 logical security certification

STM32 Trust

USB Type-C® Power Delivery

High robustness

Highly immune to fast transients
Robust IOs against negative injections

Functional Safety

SIL and CLASSB Safety Packages, including
Self-Test Library

FD CAN

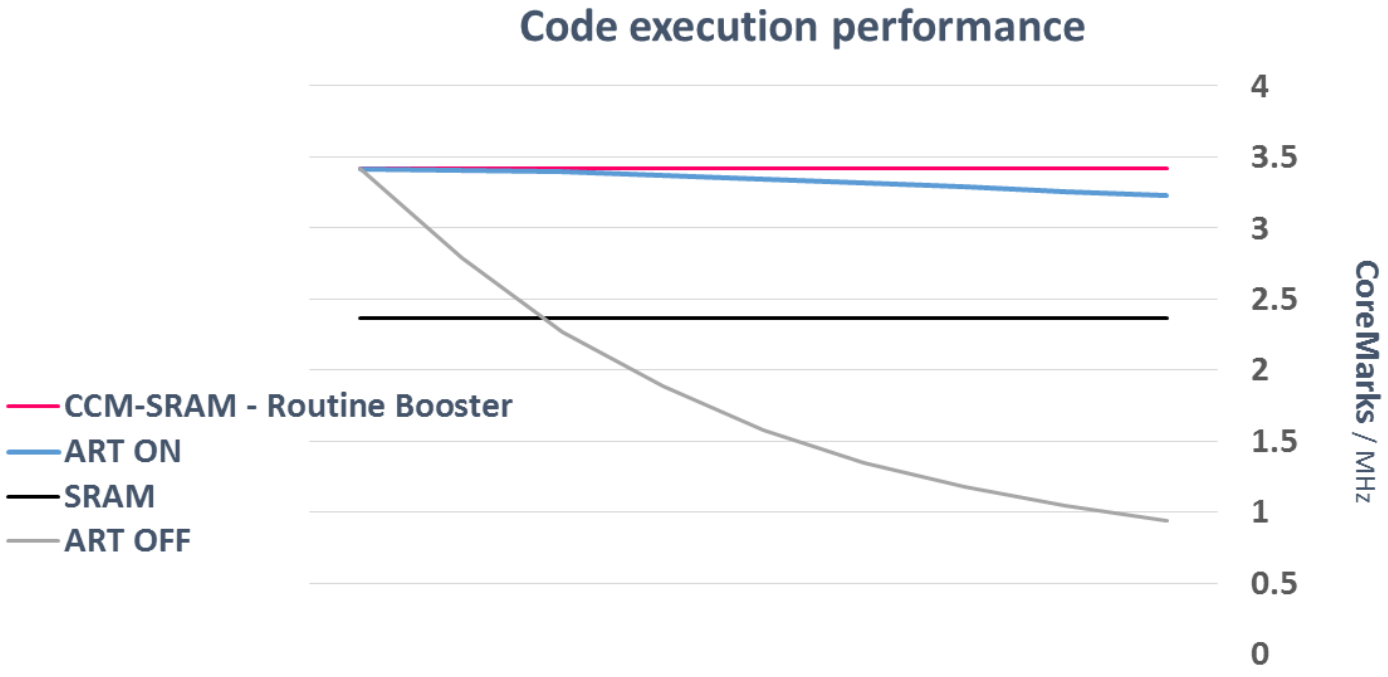
Up to 3 instances
Payload bit rate 8 times bigger than standard CAN

High temperature

from -40°C up to + **125°C**

Greater performance

170 MHz CPU performance (Arm® Cortex®-M4) with three accelerators



Number of Wait States	0	1	2	3	4
CPU Clock (MHz)	34	68	102	136	170

Arm® Cortex®-M4 with **FPU**

Up to 170 MHz CPU frequency

Up to 213 DMIPS and 569 CoreMark® results

3 different **hardware accelerators**:

- **ART Accelerator** (~dynamic cache) → full code acceleration (average)
- **Routine booster** CCM-SRAM (~static cache) → determinism preserved
- **Mathematical** (Cordic + FMAC)

Mathematical accelerators

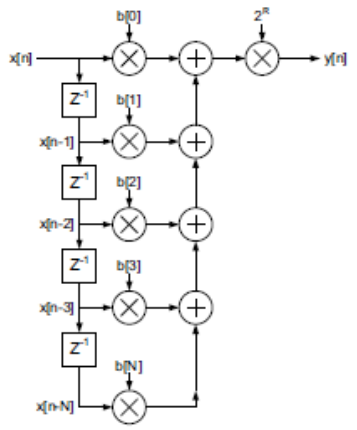
Function acceleration and CPU offload

1. **Cordic (Trigo)**
   - Very helpful for field oriented motor control method (FOC)

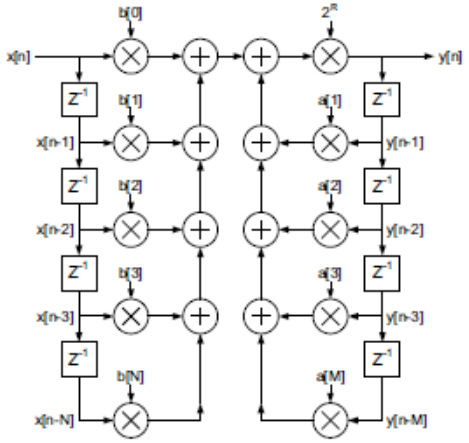
- Vector rotation (polar to rectangular): Sin, Cos
- Vector translation (rectangular to polar): Atan2, modulus
- Sinh, Cosh, Exp
- Atan, Atanh
- Square root
- Ln

2. **Filter math accelerator (FMAC)**
   - Can be used to create
     - 3p3z compensator (→ digital power)
     - Sigma Delta modulator
     - Noise shaper

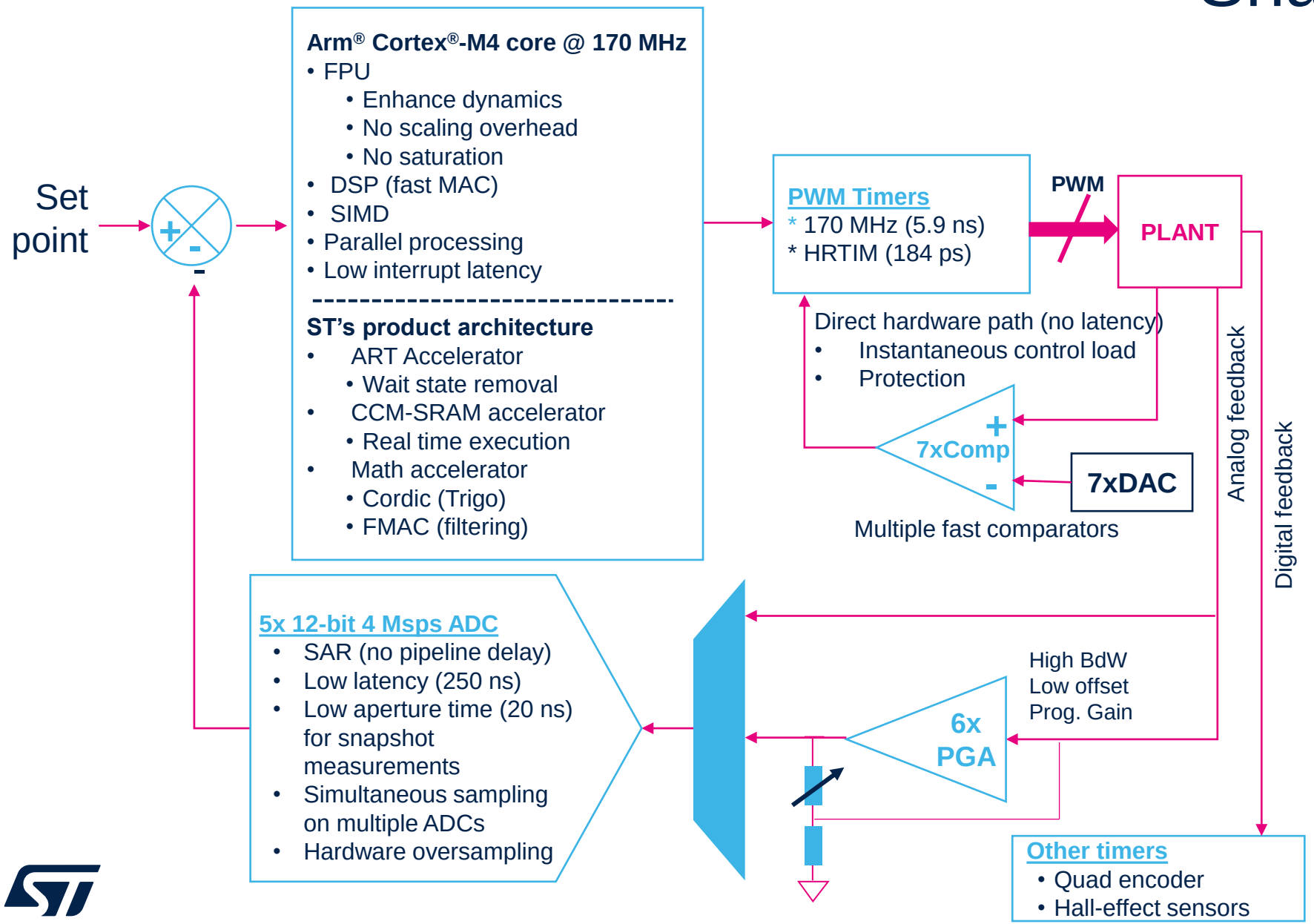
FIR filter



IIR filter



Shaped for control

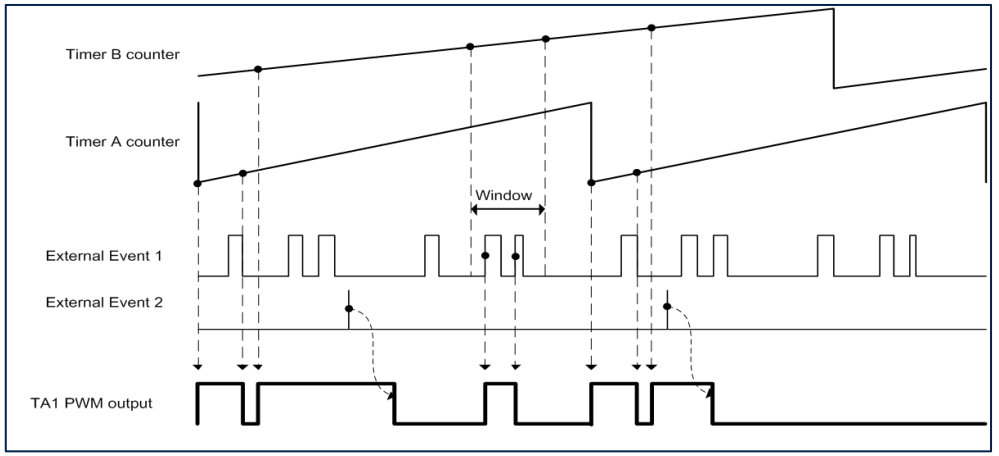


Easy use of the analog and digital resources thanks to high peripheral interconnect and flexible bus matrix

HRTimer – High resolution and much more

High resolution PWM

- 12 channels with 184 ps resolution on frequency and duty cycle
- 184 ps is equivalent to a 5.4GHz timer clock



Flexible PWM generation

- 7 x independent time base to create various shape of PWM
- 6 x complementary pair PWM outputs
- Up to 32 set/reset transitions per PWM period thanks to the built-in crossbar
- Controller/target configuration for multi phase converter

Multiple Event handlers

- 6 x digital and analog fault input
- 10 x events cycle to cycle current control or PWM restart (constant Ton/Toff)
- Blanking, windowing, and digital filter

12 independent channels

- Any topology supported from 1x 12 PWM (triple interleaved LLC (server application) up to 12 x 1 PWM (multiple independent buck converters (lighting))

Cybersecurity in Digital Power

M-CRPS and SPDM for server power supply

OPEN Compute Project

M-CRPS V1.05 RC5 (Sept'24), 12.9 Security Chapter

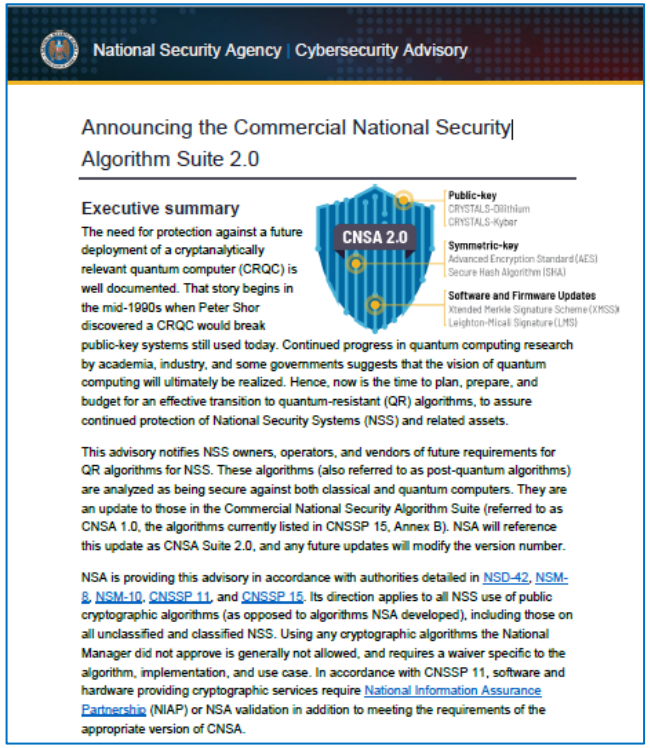
- 12.9.2 Security Boot
- 12.9.3 Security Firmware Update
- 12.9.5 Security Algorithm support
  - OCP HW Security Boot White Paper*

Strength →

Crypto algorithms:

- Symmetric crypto : AES-256
- Asymmetric crypto : ECDSA P384, ECDH P384, RSA
- Hash : SHA2 384
- PQC : Not mandatory with SPDM1.2, but SPDM1.4

PQC in CNSA 2.0
Commercial National Security Algorithm



National Security Agency | Cybersecurity Advisory

Announcing the Commercial National Security Algorithm Suite 2.0

Executive summary

The need for protection against a future deployment of a cryptanalytically relevant quantum computer (CRQC) is well documented. That story begins in the mid-1990s when Peter Shor discovered a CRQC would break public-key systems still used today. Continued progress in quantum computing research by academia, industry, and some governments suggests that the vision of quantum computing will ultimately be realized. Hence, now is the time to plan, prepare, and budget for an effective transition to quantum-resistant (QR) algorithms, to assure continued protection of National Security Systems (NSS) and related assets.

This advisory notifies NSS owners, operators, and vendors of future requirements for QR algorithms for NSS. These algorithms (also referred to as post-quantum algorithms) are analyzed as being secure against both classical and quantum computers. They are an update to those in the Commercial National Security Algorithm Suite (referred to as CNSA 1.0, the algorithms currently listed in CNSSP 15, Annex B). NSA will reference this update as CNSA Suite 2.0, and any future updates will modify the version number.

NSA is providing this advisory in accordance with authorities detailed in NSD-42, NSM-8, NSM-10, CNSSP 11, and CNSSP 15. Its direction applies to all NSS use of public cryptographic algorithms (as opposed to algorithms NSA developed), including those on all unclassified and classified NSS. Using any cryptographic algorithms the National Manager did not approve is generally not allowed, and requires a waiver specific to the algorithm, implementation, and use case. In accordance with CNSSP 11, software and hardware providing cryptographic services require National Information Assurance Partnership (NIAP) or NSA validation in addition to meeting the requirements of the appropriate version of CNSA.

**Hardware Secure Boot, Version 1.0, Open Compute Project Security Workgroup, https://www.opencompute.org/documents/secure-boot-2-pdf*

PQC Algorithms standardized by NIST

NIST standards released in August 2024

Algorithm	Purpose	FIPS standards
CRYSTALS-Kyber (Lattice-based)	Key encryption	FIPS-203 (ML-KEM)
CRYSTALS-Dilithium (Lattice-based)	Digital signature	FIPS-204 (ML-DSA)
SPHINCS+ (Stateless hash-based¨)**	Digital signature	FIPS-205 (SLH-DSA)
FALCON (Lattice-based)*	Digital signature	FIPS-206 (FN-DSA) not yet released

* NIST: *"…since there may be use cases for which CRYSTALS-Dilithium signatures are too large."*
** NIST: *"to avoid relying only on the security of lattices for signatures"*

Algorithms previously standardized by NIST

- XMSS and LMS are 2 PQC Statefull hash-based signature schemes standardized in Oct/2020
- Typical use case: Firmware upgrade signature

Statefull signature	Standard
XMSS	SP800-208
LMS	

STM32 PQC offer

- PQC library already available for download on st.com : X-CUBE-PQC
  - Cryptographic algorithms:
    - LMS + XMSS with HW SHA-2 acceleration
      - LMS signature verification perf.: 4 ms for 2.5 Kbytes signature (20 ms w/o acceleration) on STM32H5
    - ML-DSA+ML-KEM without HW acceleration
      - CAVP certified to guarantee bug free implementation: certificate available here
  - Currently supports STM32H563
  - Support of STM32G4 as alpha version.
- PQC integrated in X-CUBE-CRYPTOLIBV5 in 2026Q1
  - Classic cryptography + PQC
  - All STM32 products supported
  - CAVP certification

STM32 X-CUBE-PQC offer summarized

Part Nb.	PQC Support date	LMS	XMSS	ML-KEM	ML-DSA
STM32H5	Now	√ HW accelerated(1)	√ HW accelerated(1)	√ CAVP certified	√ CAVP certified
STM32G4	October 2025	√	√	√	√
All other parts	2026Q1	√ Acceleration subject to SHA2 IP availability CAVP certified	√ Acceleration subject to SHA2 IP availability CAVP certified	√ Acceleration subject to SHA3 IP availability CAVP certified	√ Acceleration subject to SHA3 IP availability CAVP certified

(1) Hardware acceleration increases performance by approximately five times

STM32 Digital Power Ecosystem

STM32 Digital Power: an ecosystem tailored to your needs

eDesignSuite

Expert level

5 Turn-Key solutions (PSU + PFC)
(eDesignSuite - DPower workbench)

Advanced

4 STM32 D-Power SDK
(ST-WDS/ST-PLD + STM32CubeMX)

STM32 Cube

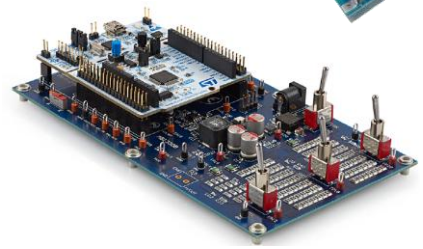
STM32

BIRICHA DIGITAL

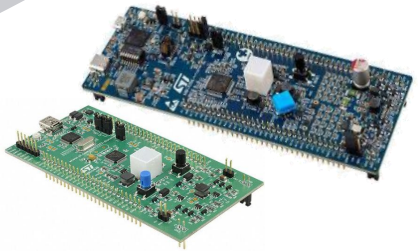
Partnership

Advanced

3 Biricha workshops



2 STM32 D-Power discovery kits



1 D-Power for beginners

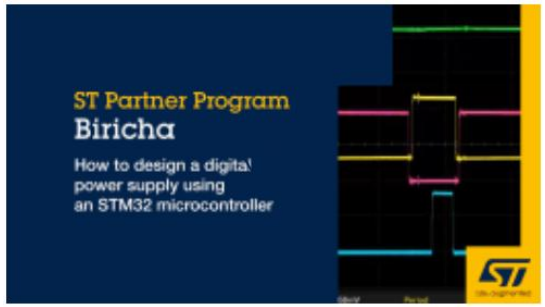
Digital Power for Beginners

Videos and webinars

- **Understanding the basics of digital with online videos and webinars**

The basics of Digital Power in Power Supply and Factor Correction applications (19:22)

Designing Digital Power Supply Units (10:49)

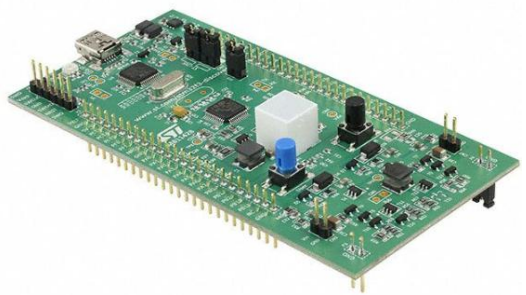


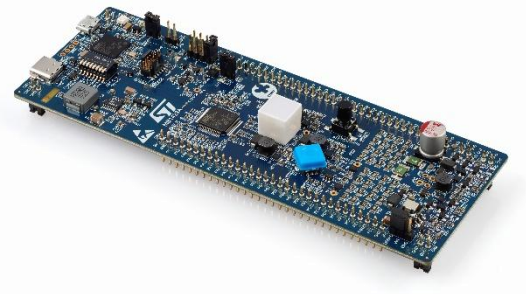
How to design a digital power supply using an STM32 microcontroller (55:32)

How to design a digital PFC step by step using an STM32 microcontroller (01:14:02)

STM32 Discovery kit and application notes

- **STM32F334 and STM32G474 discovery kits**
  - Complete demonstration and development platform with free example code.
- Application notes
  - AN4539: HRTimer V2 cookbook
  - AN5496: buck converter in voltage mode
  - AN5497: buck converter in current mode

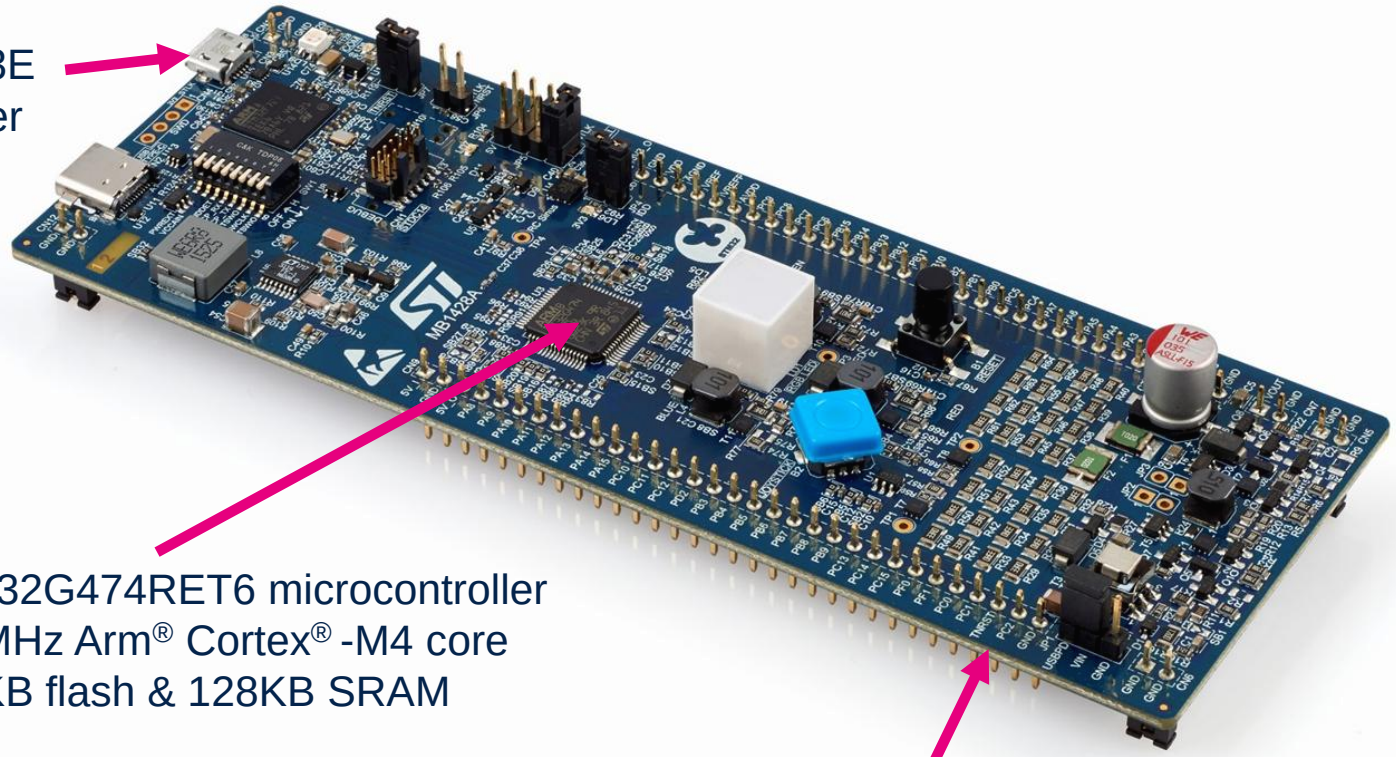




Synchronous Buck Converter

B-G474E-DPOW1

On-board STLINK-V3E
debugger/programmer



STM32G4

STM32G474RET6 microcontroller
170MHz Arm® Cortex® -M4 core
512KB flash & 128KB SRAM

Buck converter circuit with
onboard resistor loads

Digital Power Workshops with Biricha

Implement digital power supplies and power factor correction

Biricha digital power:
World leading expertise and training in digital power

Workshop based on STM32F334 and STM32G474 Nucleo and its dedicated digital power expansion board

STMicroelectronics brings industry leading ST MCUs together with Biricha's tools and training

STM32 System Solutions

STDES-3KWTLCP

STM32G4

3 kw digital power supply
(Totem pole PFC +
FB LLC + SR)

STDES-VRECTFD

STM32G4

15 kW 3-ph
Vienna PFC Converter

STDES-PFCBIDIR

STM32G4

15 kW 3-ph
Bidirectional AC/DC DC/AC
Convertor

STDES-30KWVRECT

STM32G4

30 kW Vienna PFC rectifier

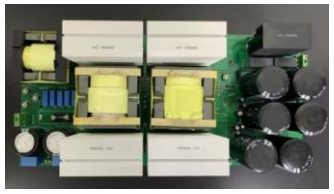
STDES-2KW5CH48V

STM32G4

2.5 kW - 48 V battery charger for industrial LEVs
(CCM PFC and FB LLC converter)

STDES-6KWHVDCDC

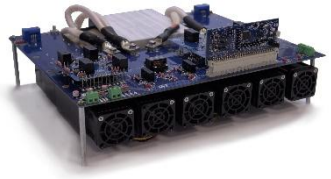
STM32G4



6 kW high voltage DC-DC converter for EV charging
(FB LLC)

STDES-30KWVRECT

STM32G4



25 kW Dual Active Bridge Converter
(Bidirectional DC/DC converter)

STM32 system evaluation tools

STEVAL-ISA172V2

2 kW fully digital power supply
(PFC 2ph interleaved +
DC-DC FB phase shift)

STM32F3

STEVAL-DPSLLCK1

3 kW DC-DC digital power supply
(Full bridge LLC resonant
with synch rectification)

STM32F3

STEVAL-DPSTPFC1

3.6 kW PFC Totem Pole with inrush current limiter
(PFC Bridgeless Totem Pole)

STM32F3

STEVAL-TTPPFC01

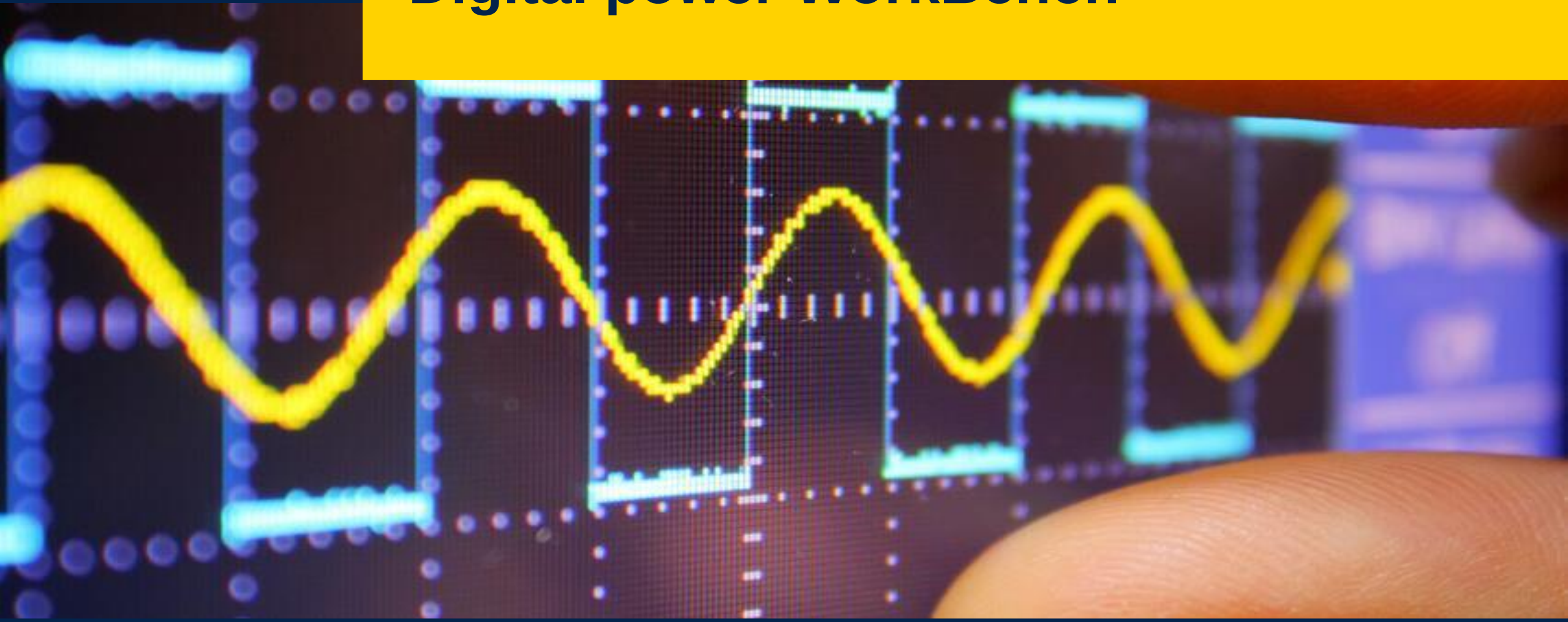
2 kW, 3-channel interleaved totem-pole PFC

STM32G4

Reference Board Resource

- Documentation : User Manual, Product Specification
- CAD Resources : Schematic, Gerber file, BOM
- Tools & Software : Firmware binary image (No source code)

Digital power WorkBench



Digital power WorkBench in eDesignSuite

System design tool addressing BOM-rich applications

Power stage optimizer

Electrical simulation in signal conditioning

STM32 FW generator

Evaluation board selector

Supported topologies (AC/DC, DC/DC)

- ZVS&CCM Interleaved Totem-Pole, Vienna Rectifier, 3-Level T-Type Converter
- FB LLC, DAB

2024 roadmap

eDesignSuite

D-power @ eDesignSuite

GUI

- Schematic view, BOM, Bode Diagrams, Power losses (for Power Transistors and Diodes)
- Wizard based design customization

Hardware sizing

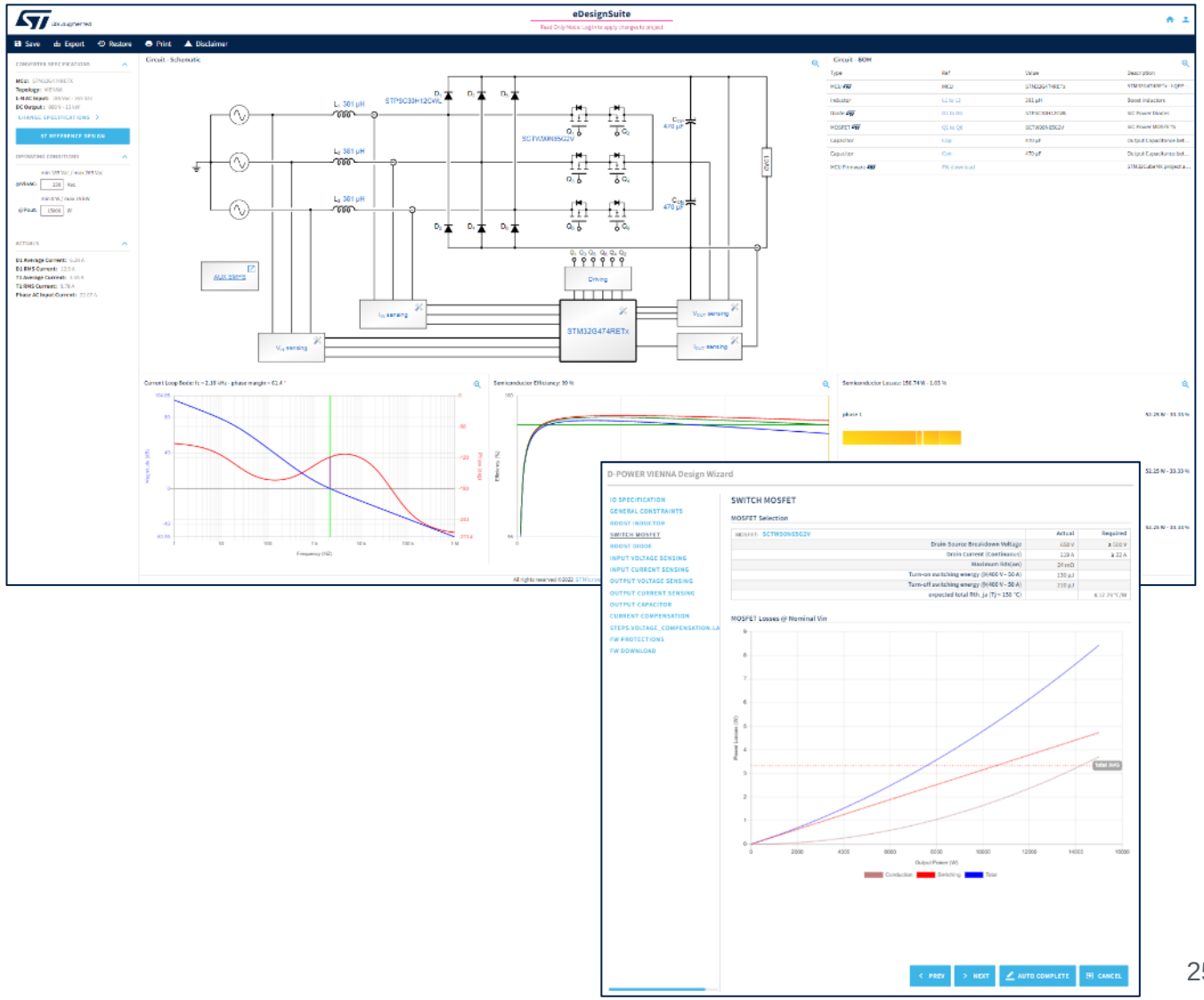
- Magnetics, power switch selection, diodes selection, current Loop and voltage loop compensation

Firmware customization

- Sensing, protections, voltage control and Current Control

Firmware delivery

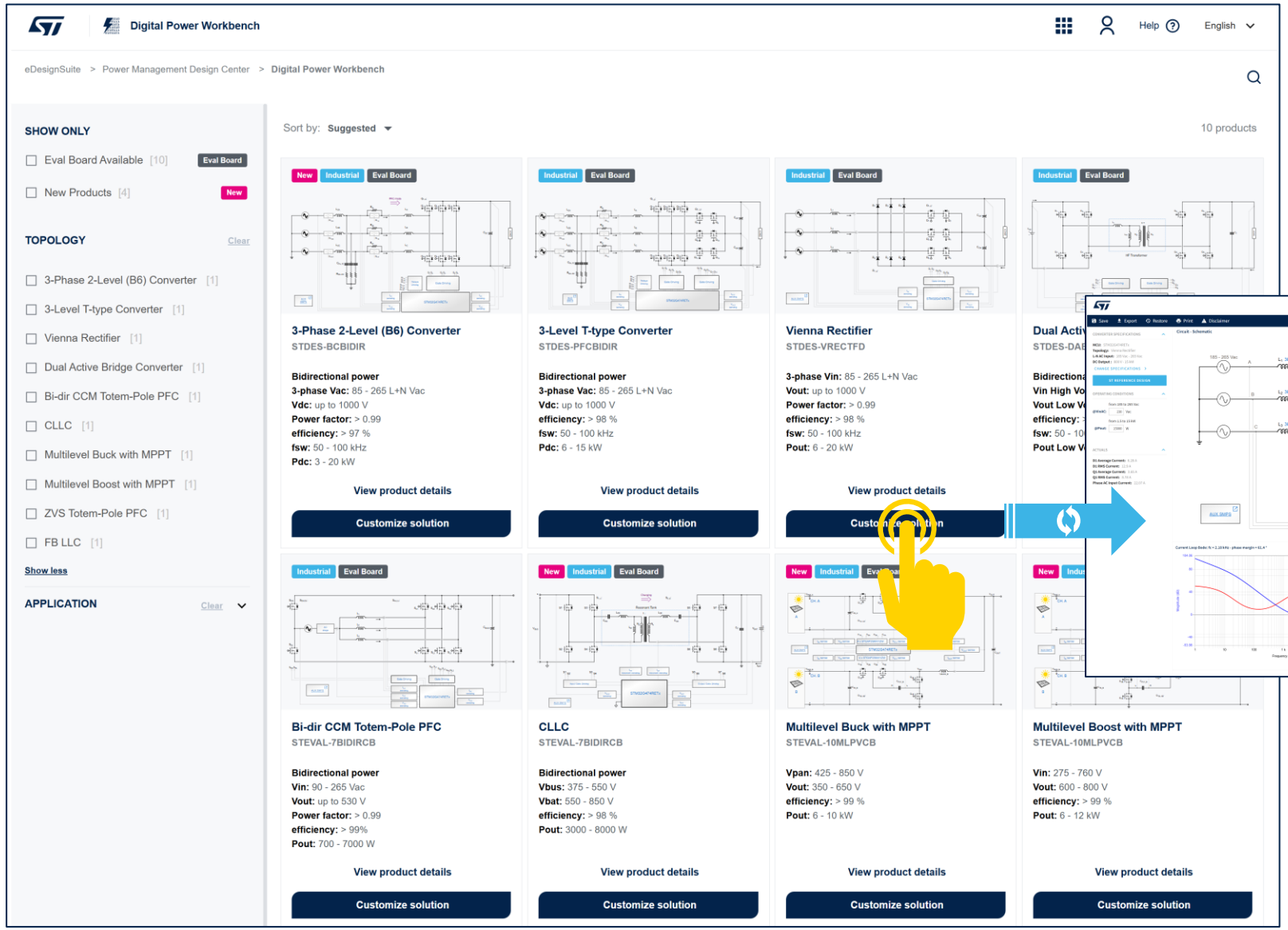
- Compatibility with STM32Cube tools: delivery of custom STM32Cube expansion pack for Vienna Rectifier solution + STM32CubeMX project (.ioc file) reflecting all current solution customization



eDesignSuite

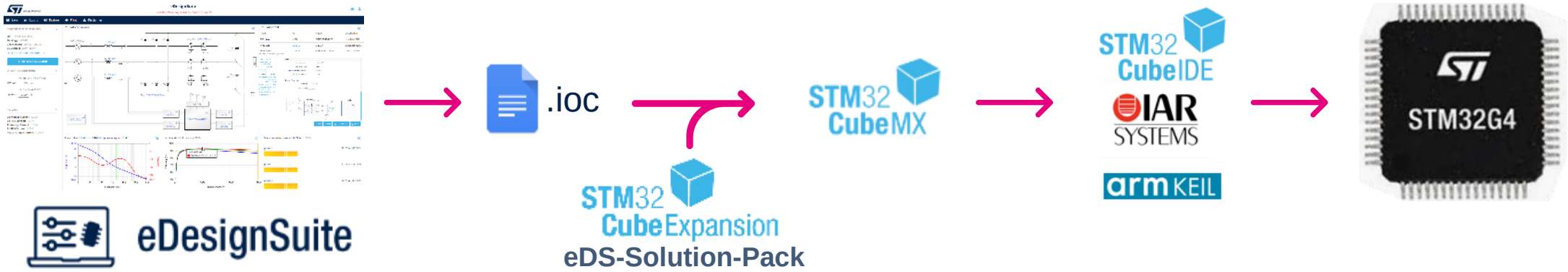
Evaluation boards advisor

Clicking on the button the to start your design, hardware sizing, and firmware customization based on ST reference Design.



EDS D-power firmware

FW generation and delivery workflow



Firmware delivery

Compatibility with STM32Cube tools: delivery of custom STM32Cube expansion pack for Vienna Rectifier solution + STM32CubeMX project (.ioc file) reflecting all current solution customization

Our technology starts with You

Find out more at www.st.com/STM32G4