Pls vote for CryptOne for ”Best Innovative IP prize”

100% safe IP Core? – CryptOne as an example of new generation of secured IP Cores

Jacek Hanke, CEO Digital Core Design

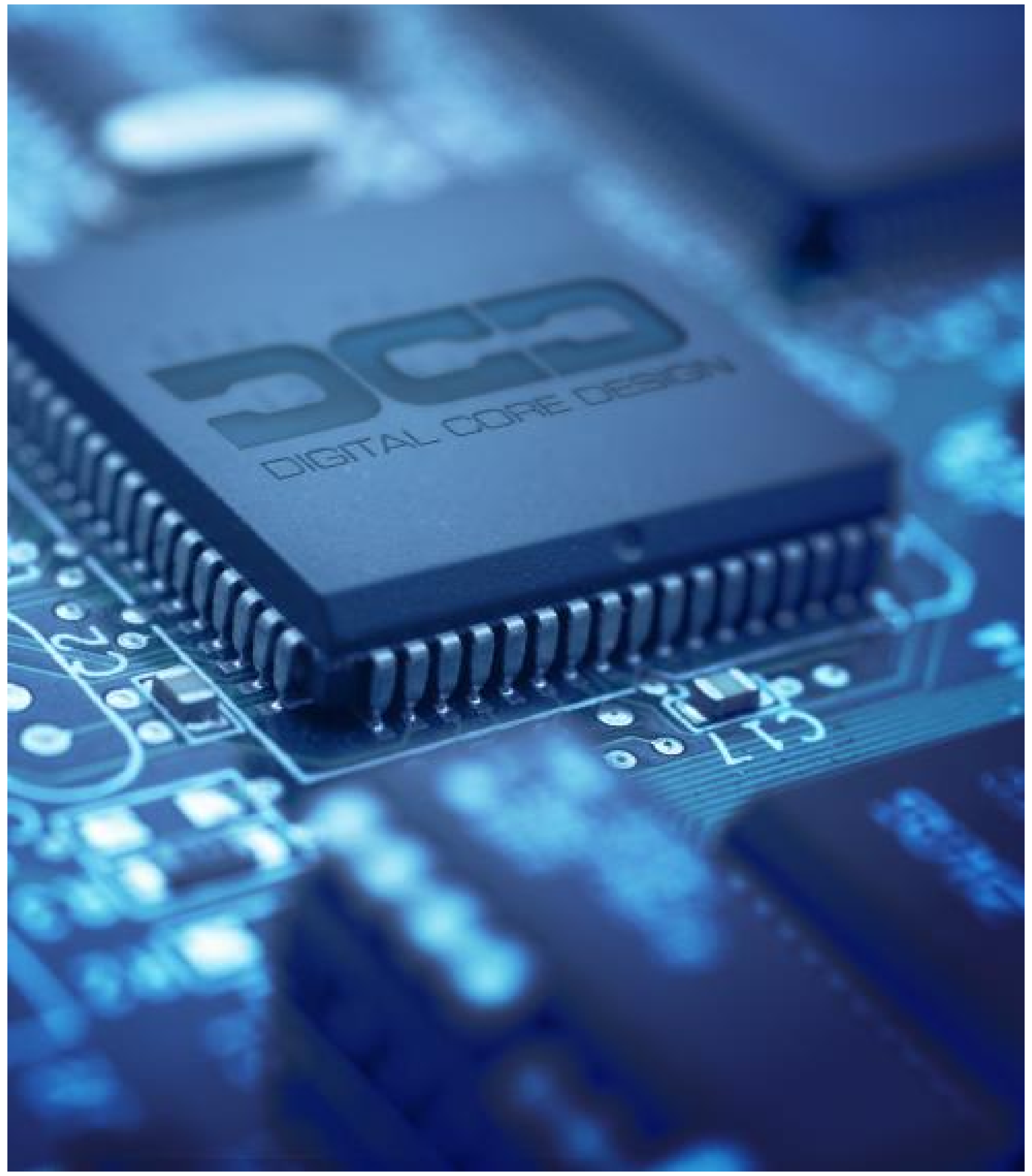
D&R IP-SOC DAYS

Shanghai, China, Septemeber 12th, 2019

DIGITAL CORE DESIGN

Agenda

1. About Digital Core Design
2. Milestones
3. Security vs hardware
4. CryptOne
5. Summary



Pls vote for CryptOne for "Best Innovative IP prize"

Digital Core Design

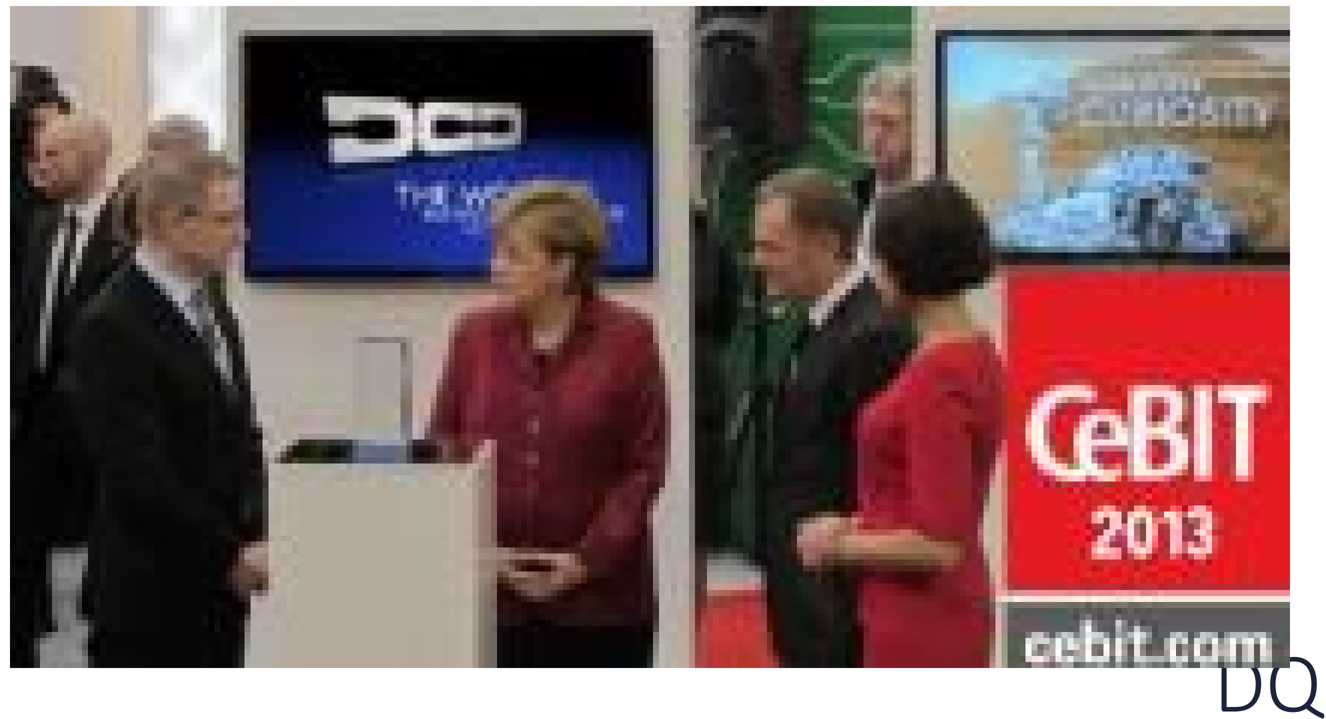
- ✓ Digital Core Design has been founded in 1999 and since the early beginings is focused in IP Cores improvement and System-on-Chip designs,
- ✓ During these two decades, DCD's launched more than 70 different architectures, among them e.g. World's Fastest 8051 – the DQ80251 and royalty-free 32-bit CPU - the D32PRO,
- ✓ DCD has sold more than 1000 license to various customers like corporations start-ups, R&D offices, universities and so on.

Pls vote for CryptOne for ”Best Innovative IP prize”

SONY PHILIPS TOYOTA

Milestones

Pls vote for CryptOne for "Best Innovative IP prize"



EDN 2013 HOT 100

European Business Awards™

BRONZE
STEVIE® WINNER
STEVIES 2013
INTERNATIONAL BUSINESS AWARDS

EDN 2012 HOT 100

99 – 1999 DCD established

02 – DP8051XP IP Core

05 – DoCD™ Hardware Debugger

2011 – DQ80251, World's Fastest 8051

12 – Product of the Year Award DQ80251

12 – EDN's Hot Products of 2012 for DQ80251 & DoCD

13 – DQ80251 presented at CeBIT 2013 opening ceremony

13 – DCD among 4 most innovative companies in Poland

14 – DRPIC 166X IP Core EDN Hot 100 Products

15 – D32PRO, royalty-free 32-bit CPU

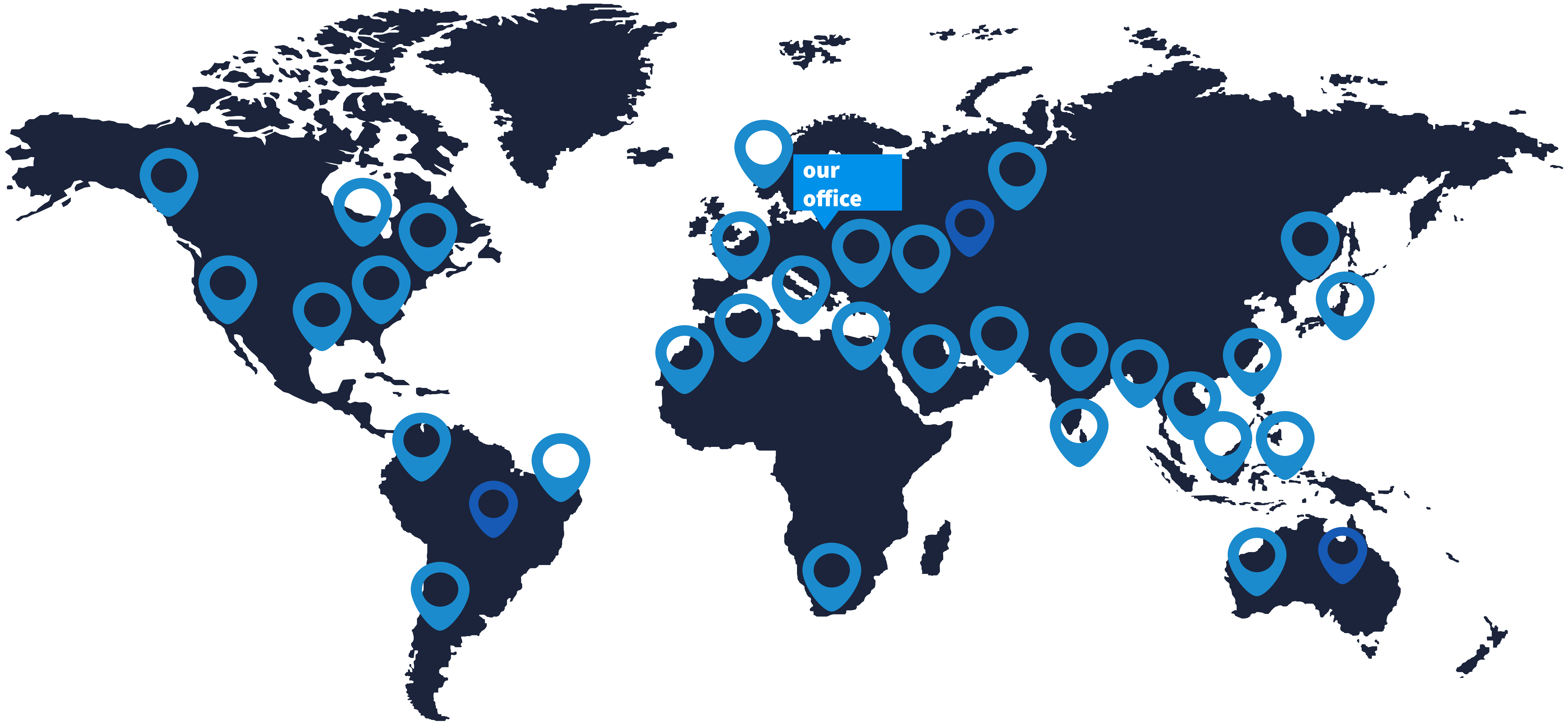
16 – D32PRO named Polish Product of the Future

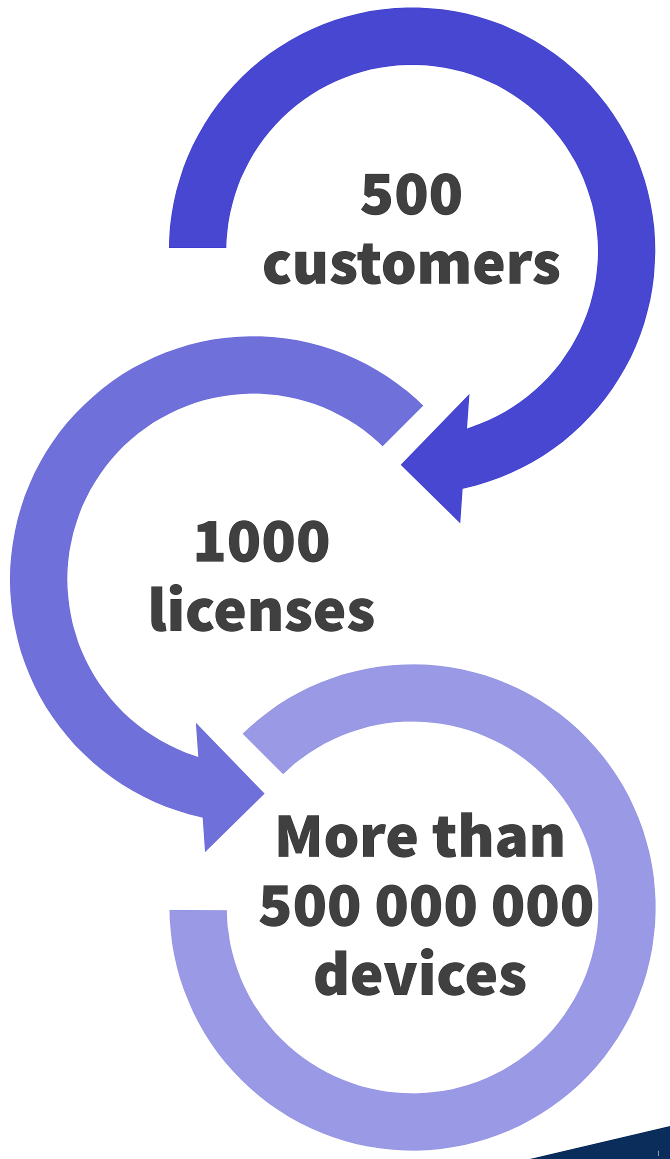
17 – D32PRO awarded with the „Teraz Polska" Prize

19 – CryptOne, 100% safe crypto CPU

DCD's IP Cores

Pls vote for CryptOne for ”Best Innovative IP prize”




500 customers

1000 licenses

More than 500 000 000 devices

DCD’s IP Cores

- ✓ One of the most experienced companies in IP Core market
  - ✓ More than 70 architectures in portfolio including 8-bit, 16-bit, 32-bit MCU, UART, I2C, SPI, I3C,
  - ✓ USB, CAN, CAN-FD LIN, floating points ...
  - ✓ Among them World’s Fastest & World’s Smallest 8051 & 80251
  - ✓ Deeply embedded, royalty-free, fully scalable 32-bit CPU
  - ✓ Technology independent (ASIC & FPGA)
  - ✓ IP Cores tailored to the project needs
  - ✓ Royalty-free solutions

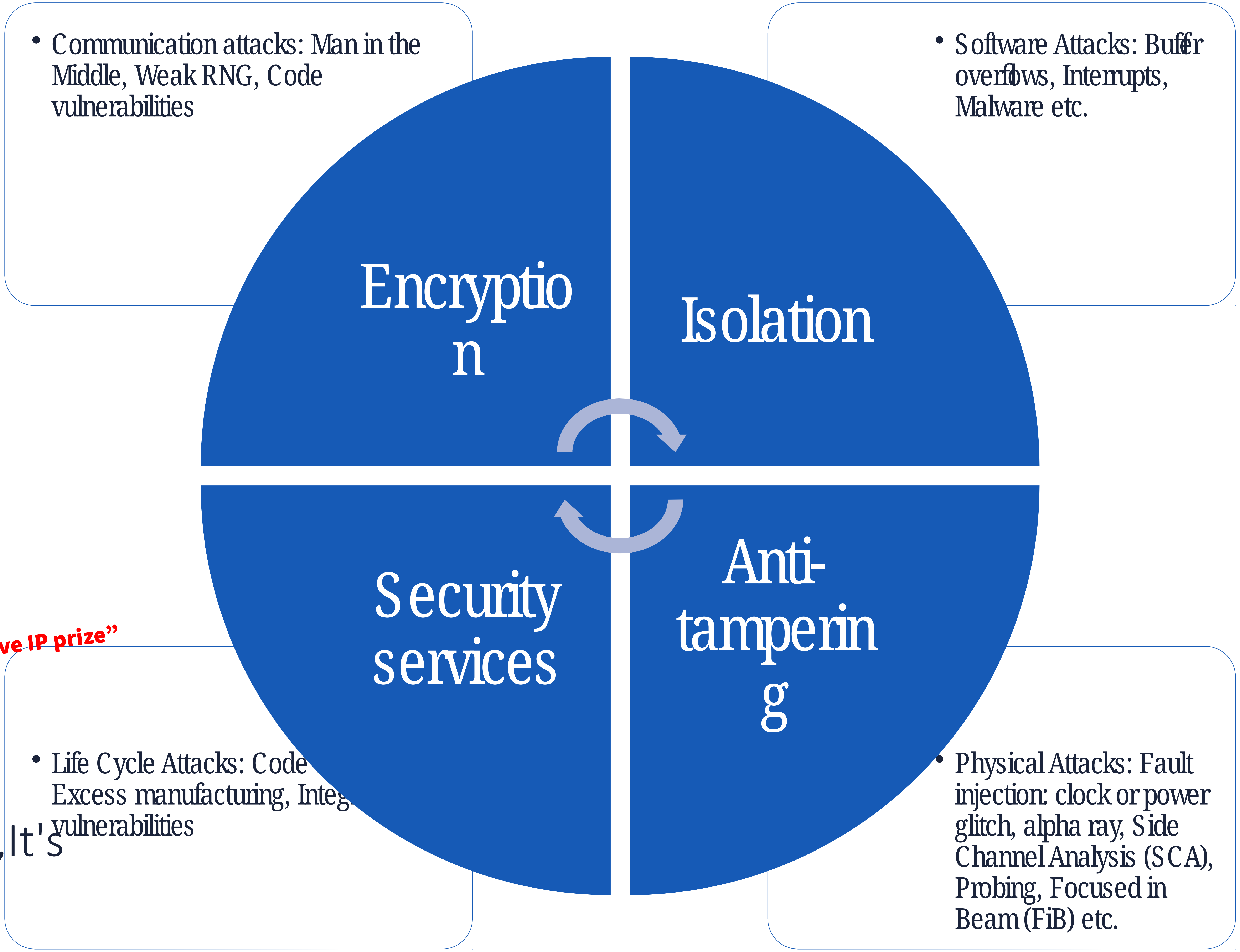
Pls vote for CryptOne for ”Best Innovative IP prize”

Security, stupid*

☑ There are a range of attack types…

Pls vote for CryptOne for ”Best Innovative IP prize”

* Paraphrised: Bill Clinton 1993 „It's the economy, stupid”

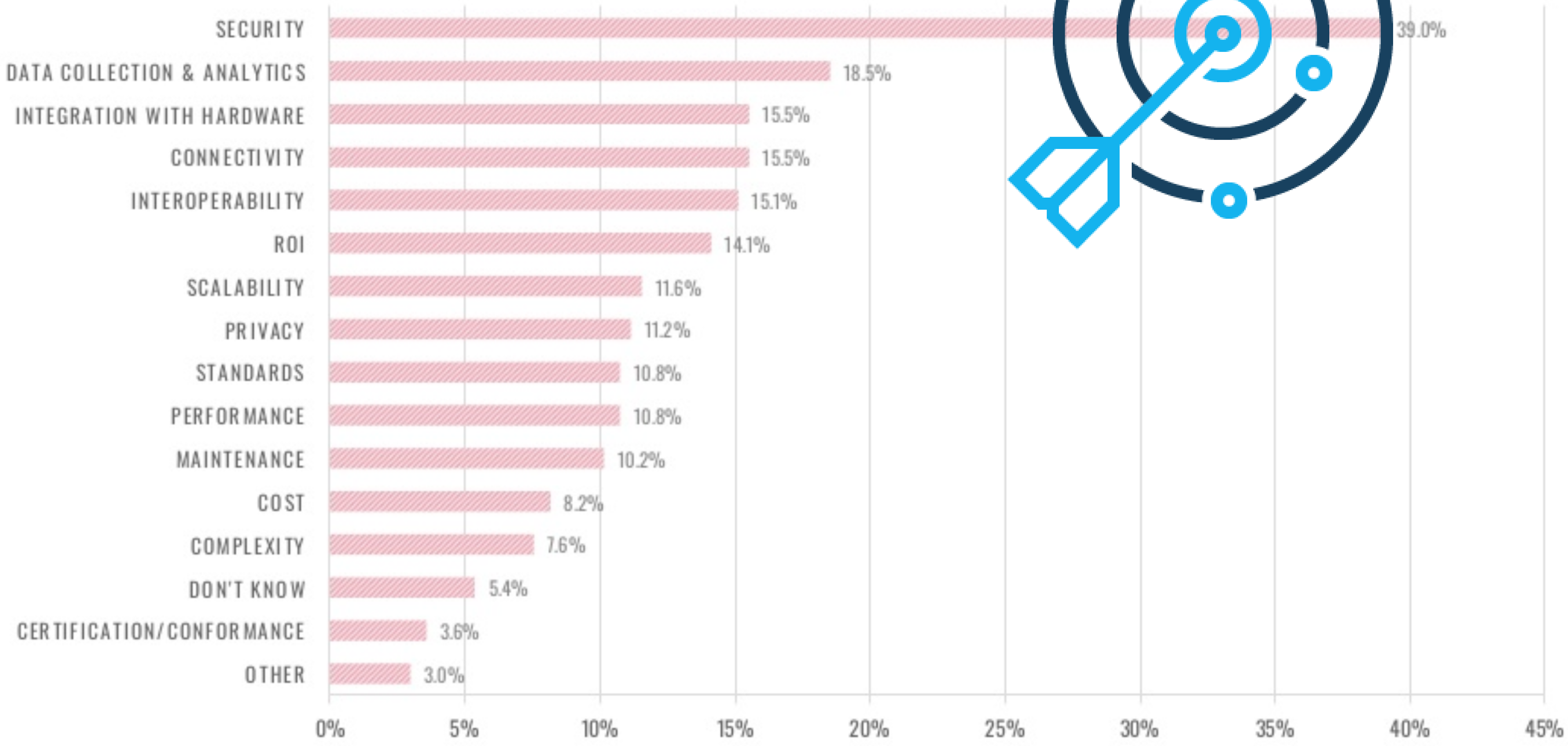


- Communication attacks: Man in the Middle, Weak RNG, Code vulnerabilities
- Software Attacks: Buffer overflows, Interrupts, Malware etc.
- Life Cycle Attacks: Code Excess manufacturing, Integ vulnerabilities
- Physical Attacks: Fault injection: clock or power glitch, alpha ray, Side Channel Analysis (SCA), Probing, Focused in Beam (FiB) etc.

Security is important?

Top IoT Concerns

What are your top 2 concerns for developing IoT solutions?

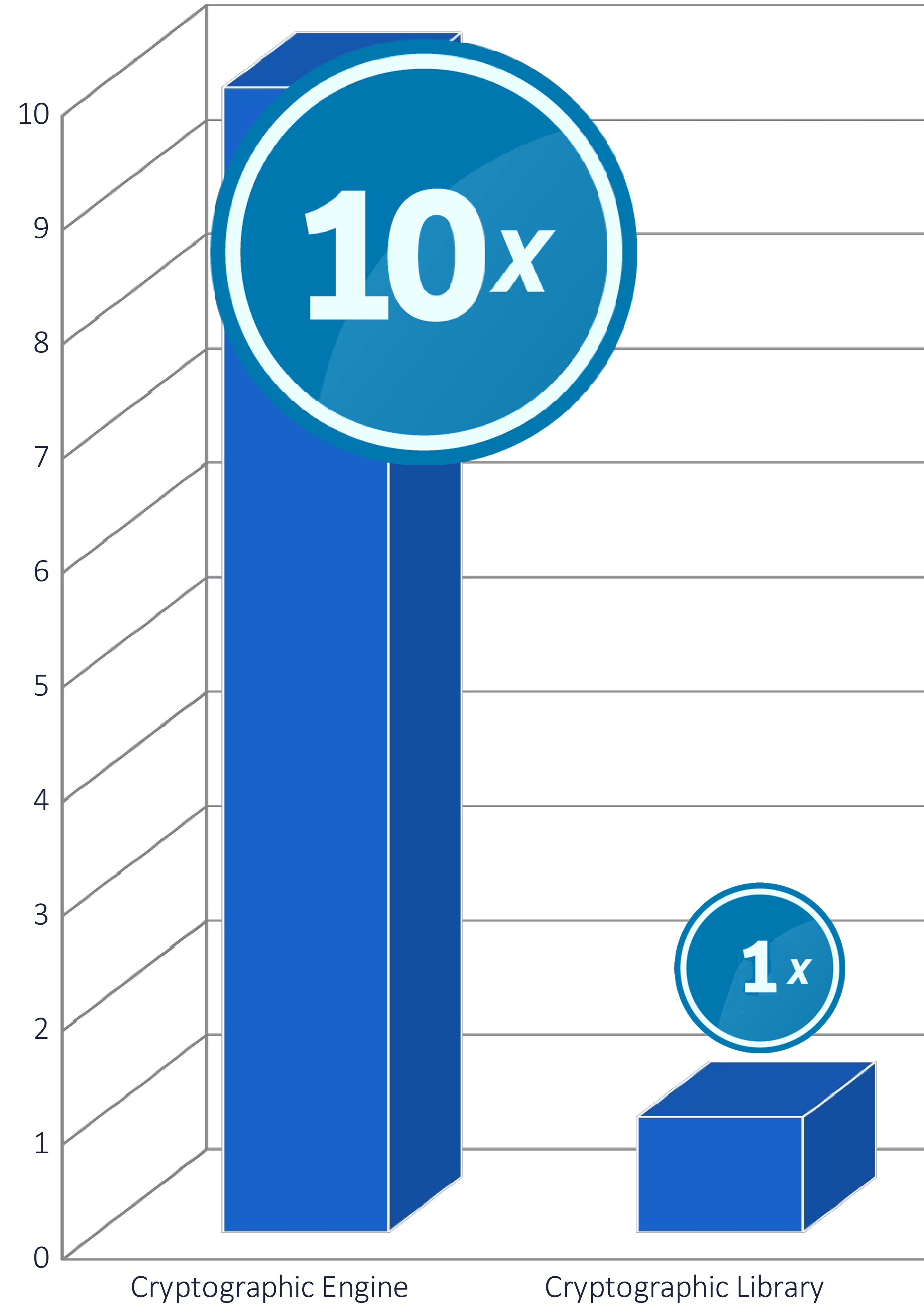


Pls vote for CryptOne for "Best Innovative IP prize"

Why security in HW is better than SW?

- ✓ **Faster:** HW cryptography performs the encryption and decryption many times the speed of SW implementation,
- ✓ **Higher Performance, Lesser Code size**,
- ✓ **Application Integrity Assurance**: hardware root of trust is more secure & higher assurance of code integrity over software,
- ✓ **Resistance to Reverse Engineering**: SF is more susceptible to RE

  Resistance to Non-intrusive Attacks: SF is more vulnerable to attacks that are based on power consumption analysis
- ✓ **Higher level of Key Protection**: keys are stored in HW not in SF



“Best Innovative IP prize”

Security vs hardware

- ✓ When implementing security countermeasures on an IoT device, best done using **hardware based security**

Ready for the highest

Security level

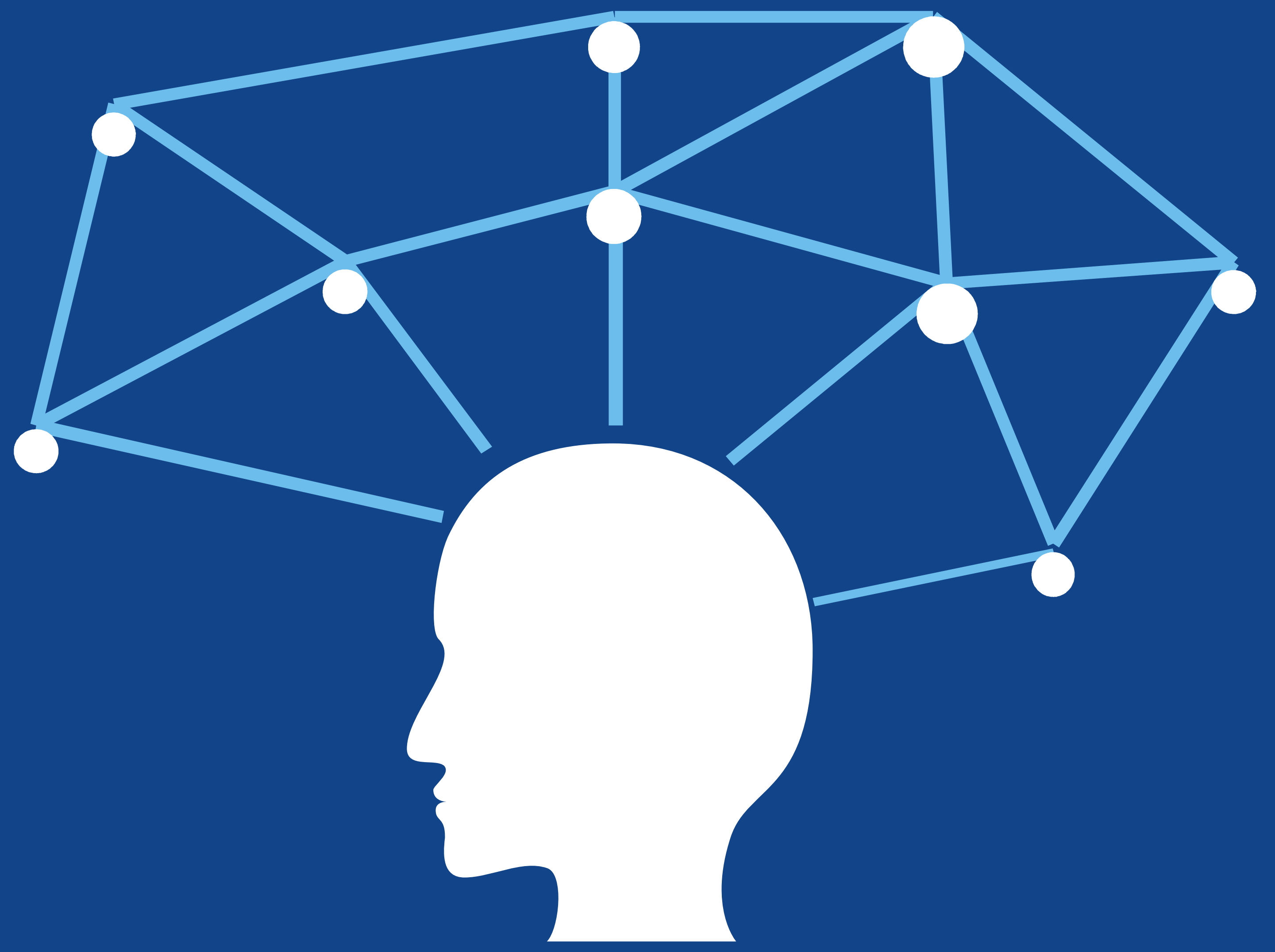
	Software	Isolated Security IP (HSM)	HW-based security
Software attacks	⚠	🔒	🔒
Micro-architecural attacks	⚠	🔒	🔒
Physical attacks	⚠	⚠	🔒

novative IP prize”

Cryptone

- CryptOne is a 100% safe crypto CPU, because...

  It involves the use of **RSA asymmetric encryption scheme** to realize a cryptosystem with a **one-time pad (OTP)**,
- DCD's solution is a broadly defined crypto system solution based on an asymmetric RSA with a **hidden value of a component of a public key susceptible to crypto analysis and implementing the OTP rules**,
- Nowadays security is the key- that's why CryptOne OTP offers the **advantages of symmetric crypto systems with one-time pad while retaining the advantages of asymmetric systems**.



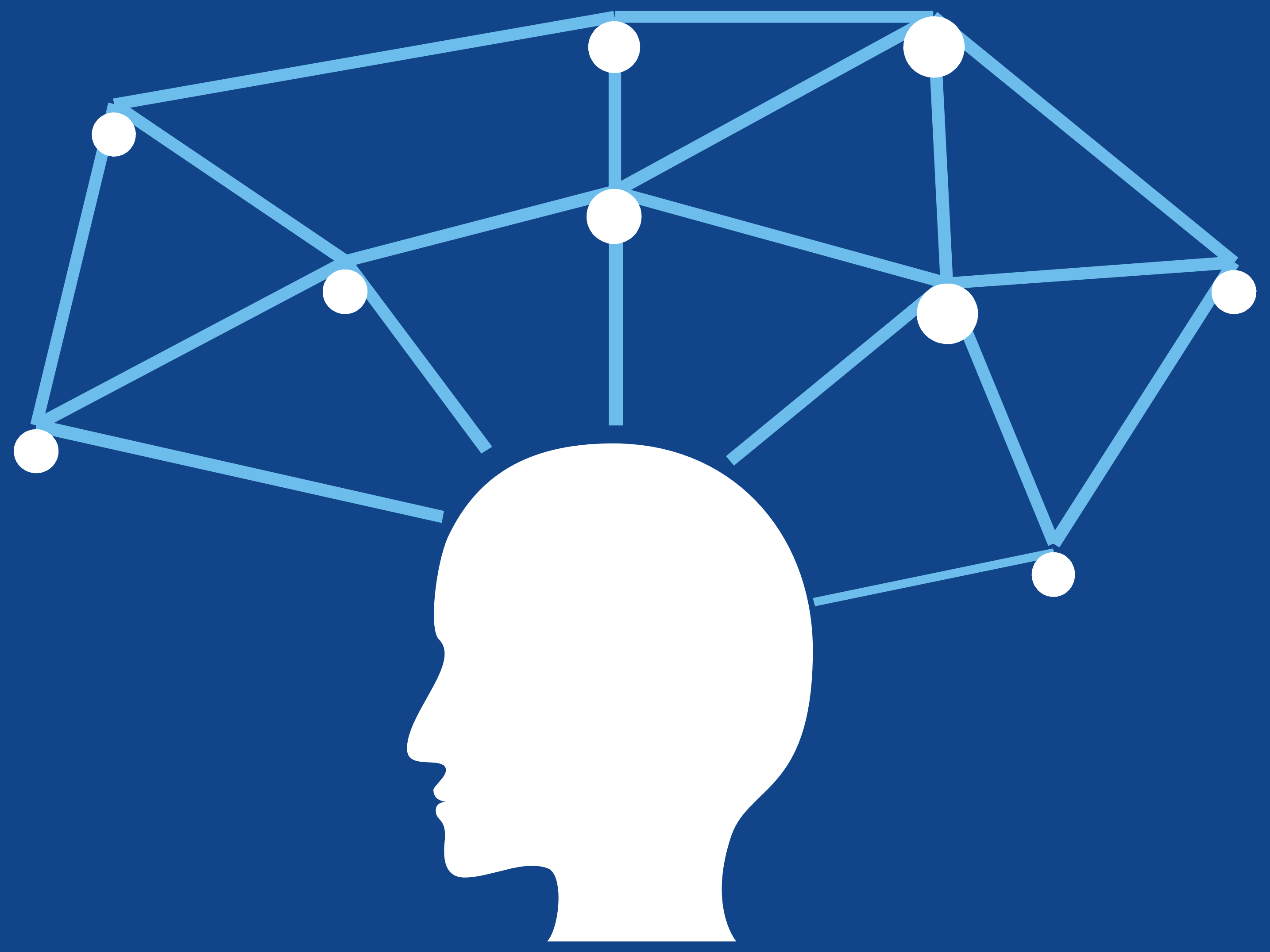
DIGITAL CORE DESIGN

Pls vote for CryptOne for ”Best Innovative IP prize”

Cryptone

Pls vote for CryptOne for ”Best Innovative IP prize”

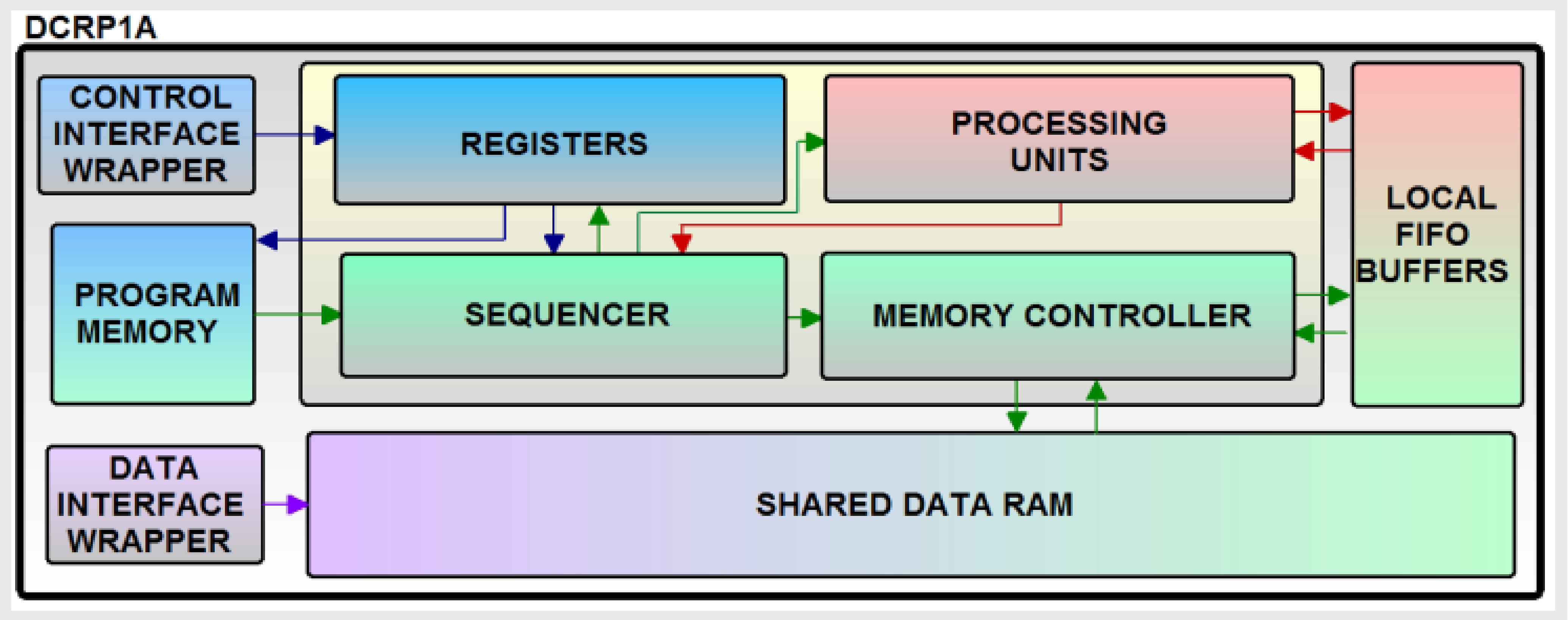
- ✓ CryptOne core is a universal, fully scalable solution which is able to boost asymmetric cryptographic algorithms like: **RSA**, **Diffie-Hellman** and **ECC**;
- ✓ It provides the efficient solution for asymmetric cryptography **boosting arithmetic operations** like: **modular exponentiation**, **multiplication**, **inversion**, **GCD finding** as also **point doubling**;
- ✓ The **energy efficient architecture** of CryptOne IP core enables the usage of the **very small silicon footprint** with **high processing speeds**.



DIGITAL CORE DESIGN

100% safe crypto CPU

- CryptOne can be provided with **various different interfaces including AMBA AHB, AXI4, APB**;
- Very **intuitive interface** enables the fast, **straightforward system integration**;
- The core is **resistant to the Differential Power Attacks (DPA) and timing attacks**



DCRP1A

CONTROL INTERFACE WRAPPER

REGISTERS

PROCESSING UNITS

LOCAL FIFO BUFFERS

PROGRAM MEMORY

SEQUENCER

MEMORY CONTROLLER

DATA INTERFACE WRAPPER

SHARED DATA RAM

Pls vote for CryptOne for ”Best Innovative IP prize”

CryptOne’s features:

- **CryptOne constant time algorithms:**
  - Modular exponentiation,
  - Parallel modular exponentiation CRT
  - ECDSA sign/verify
  - ECDH
  - Elliptic curve point multiplication
  - Modular multiplicative inverse
  - GCD
  - Modular reduction
  - Multiplication
  - Division
- **Cryptographic algorithm applications:**
  - ECDSA, ECDH
  - RSA key generation
  - RSA Sign/Verify/Encrypt/Decrypt
  - Diffie-Hellman schemes
  - Miller-Rabin Primality check
  - System applications:
- **Client-server communication:**
  - Sensor networks
  - SSL/TLS stacks
  - IoT devices
  - Embedded security/ID devices

- **AMBA AHB, AXI4, APB** interface ready
- Rapid & easy development with delivered API
- **Patent pending architecture**
- Algorithms resistant against SPA and timing attacks
- CryptOne elliptic curves with native support:
  - NIST P-192
  - NIST P-224
  - NIST P-256
  - NIST P-384
  - Koblitz P-192
  - Koblitz P-256
  - Koblitz P-384
  - Brainpool P-256
  - Brainpool P-384
  - Brainpool P-512
  - Other/custom curves optional support
- Software support:
  - **OpenSSL** engine
  - **MbedTLS** port
  - OS independent crypto library

Pls vote for CryptOne for ”Best Innovative IP prize”

CryptOne – choose the best for you

- Modular Exponentiation constant time operation algorithm support
- Parallel Modular Exponentiation CRT constant time operation algorithm support
- Secure private RSA key computation, no branch inversion
- Easy to use software library interface

CryptOne EC

- Elliptic Curves point multiplication constant time algorithm
- Constant time modular multiplicative inverse algorithm for private operations.
- Boost modular multiplicative inverse algorithm for public operations
- Native support for most popular elliptic curves
- Easy to use software library interface

CryptOne TLS

- Modular Exponentiation constant time operation algorithm support
- Modular Exponentiation CRT constant time operation algorithm support
- Secure private RSA key computation, no branch inversion
- Elliptic Curves point multiplication constant time algorithm
- Constant time modular multiplicative inverse algorithm for private operations
- Boost modular multiplicative inverse algorithm for public operations
- Native support for most popular elliptic curves
- Modular Reduction constant time algorithm
- Greatest Common Divisor algorithm
- MbedTLS and OpenSSL port libraries
- Software interface and examples for building own hardware algorithms with support for:
- Large vector addition/subtraction
- Large vector shift right/left
- Large vector modular multiplication
- Branch, execution flow controls

Pls vote for CryptOne for ”Best Innovative IP prize”

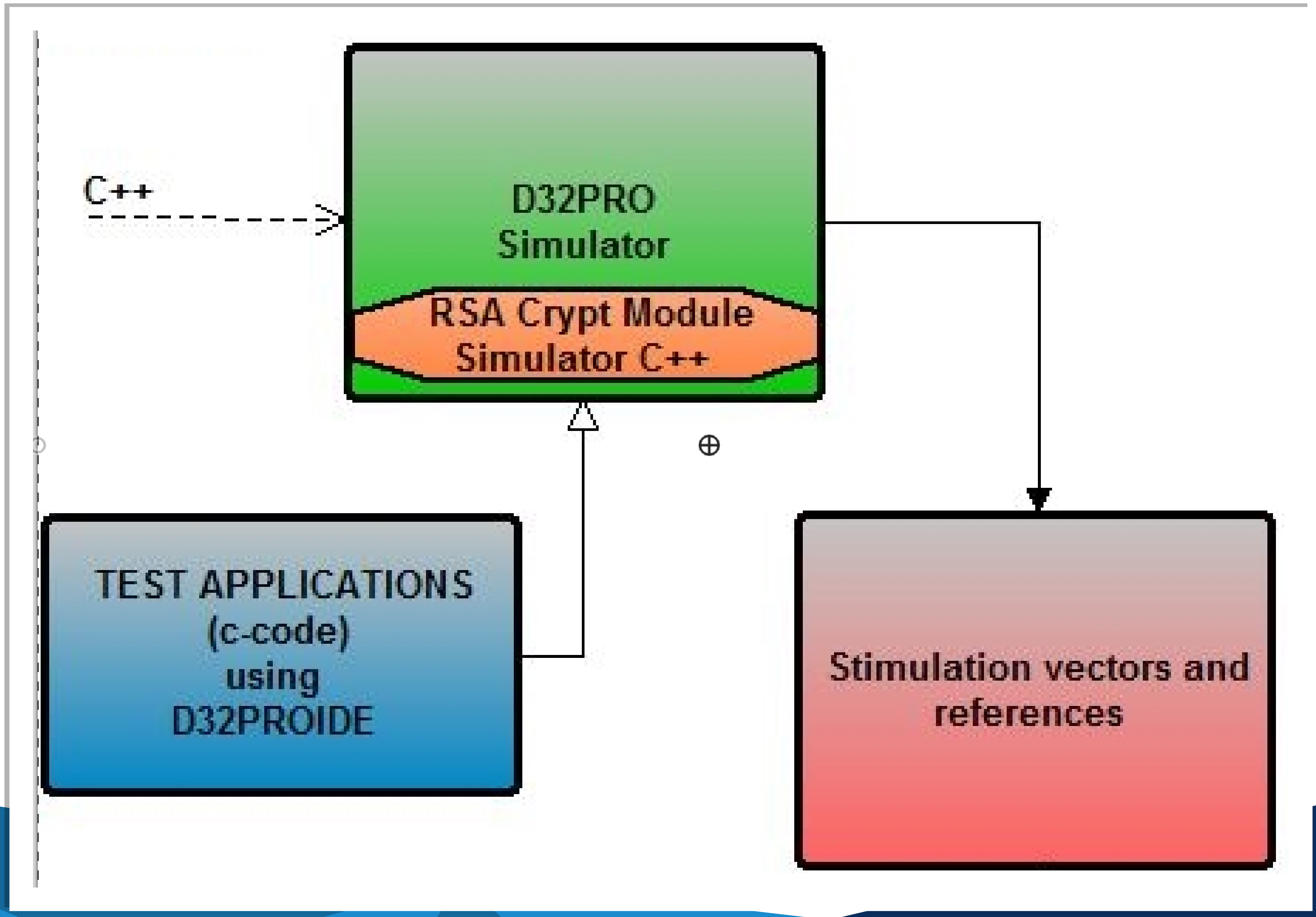
100% safe crypto CPU

- ✓ CryptOne consists of technologically independent hardware crypto processor in the form of synthesizable IP Core module prepared for integration and implementation in an IC (ASIC or FPGA)

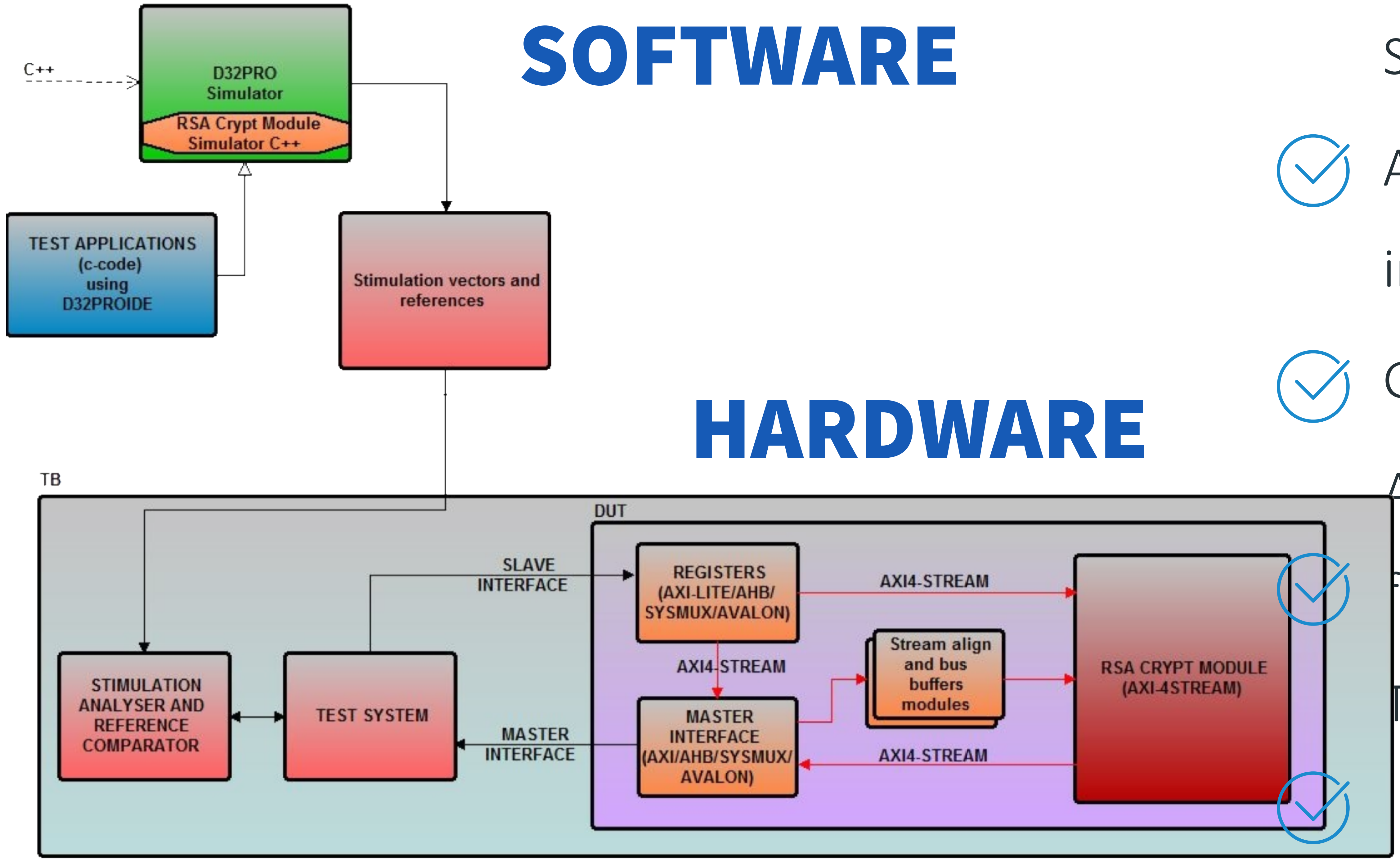
  CryptOne offers both software
- ✓ and hardware cryptography advantages

Pls vote for CryptOne for "Best Innovative IP prize"

SOFTWARE


C++
D32PRO Simulator
RSA Crypt Module Simulator C++
TEST APPLICATIONS (c-code) using D32PROIDE
Stimulation vectors and references

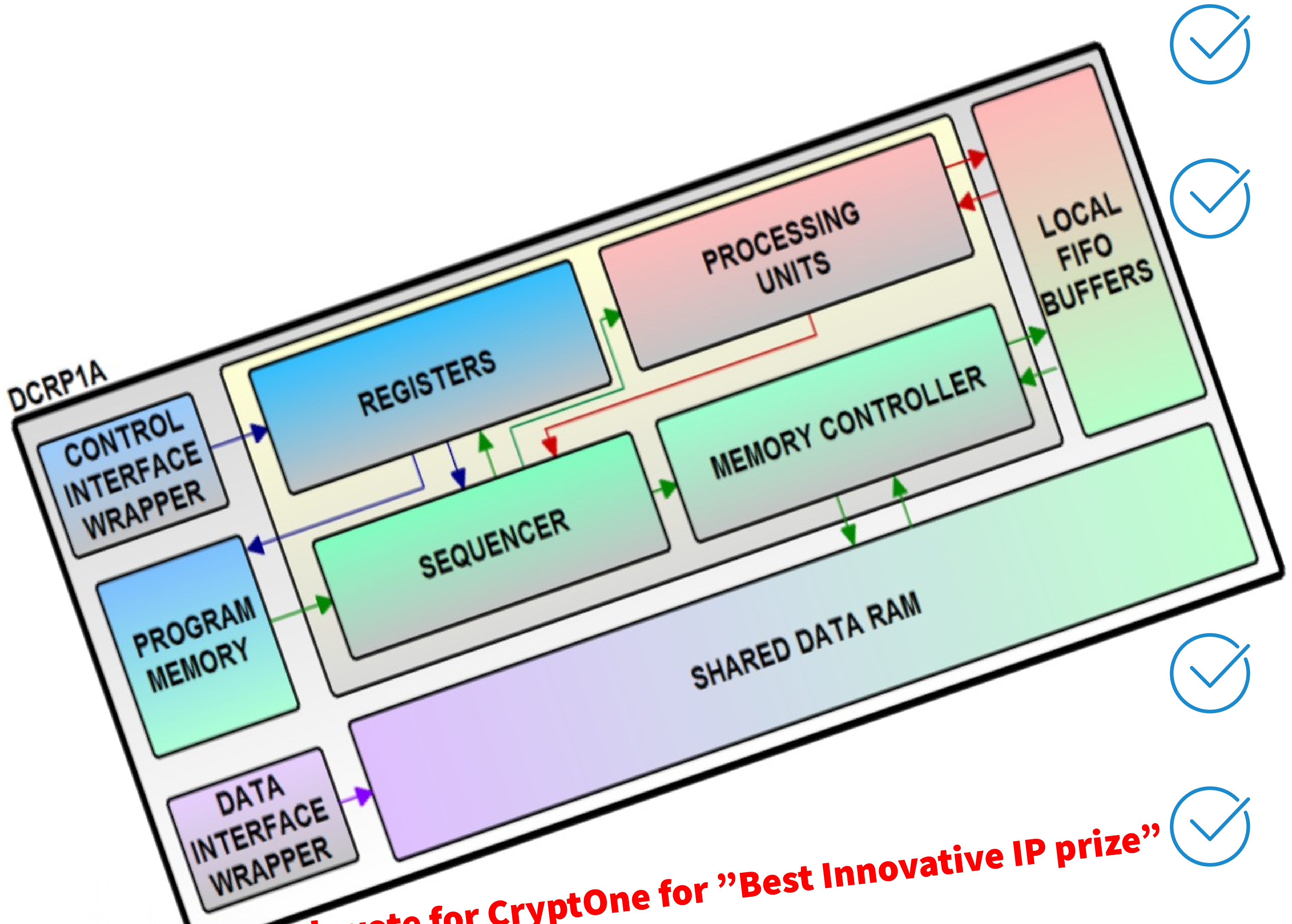
CryptOne


SOFTWARE
C++
D32PRO Simulator
RSA Crypt Module Simulator C++
TEST APPLICATIONS (c-code) using D32PROIDE
Stimulation vectors and references
HARDWARE
TB
DUT
STIMULATION ANALYSER AND REFERENCE COMPARATOR
TEST SYSTEM
SLAVE INTERFACE
MASTER INTERFACE
REGISTERS (AXI-LITE/AHB/ SYSMUX/AVALON)
AXI4-STREAM
AXI4-STREAM
MASTER INTERFACE (AXI/AHB/SYSMUX/ AVALON)
Stream align and bus buffers modules
AXI4-STREAM
RSA CRYPT MODULE (AXI-4STREAM)

- ✓ Hardware & software co-design
- ✓ Test stimulation vectors are generated with the usage if D32PRO Simulator – the sub-module for RSA crypter is written in C++
- ✓ All tests are written in C using D32PRO software – they can be easily used in hardware through D32PRO platform
- ✓ Generated stimulation vectors are also used for reference comparison
- ✓ All internal data is exchanged through the AXI4-Stream protocol in simple format = higher flexibility
- ✓ The internal RSA CRYPT MODULE can work in a separate domain

Pls vote for CryptOne for ”Best Innovative IP prize”

Receiveables



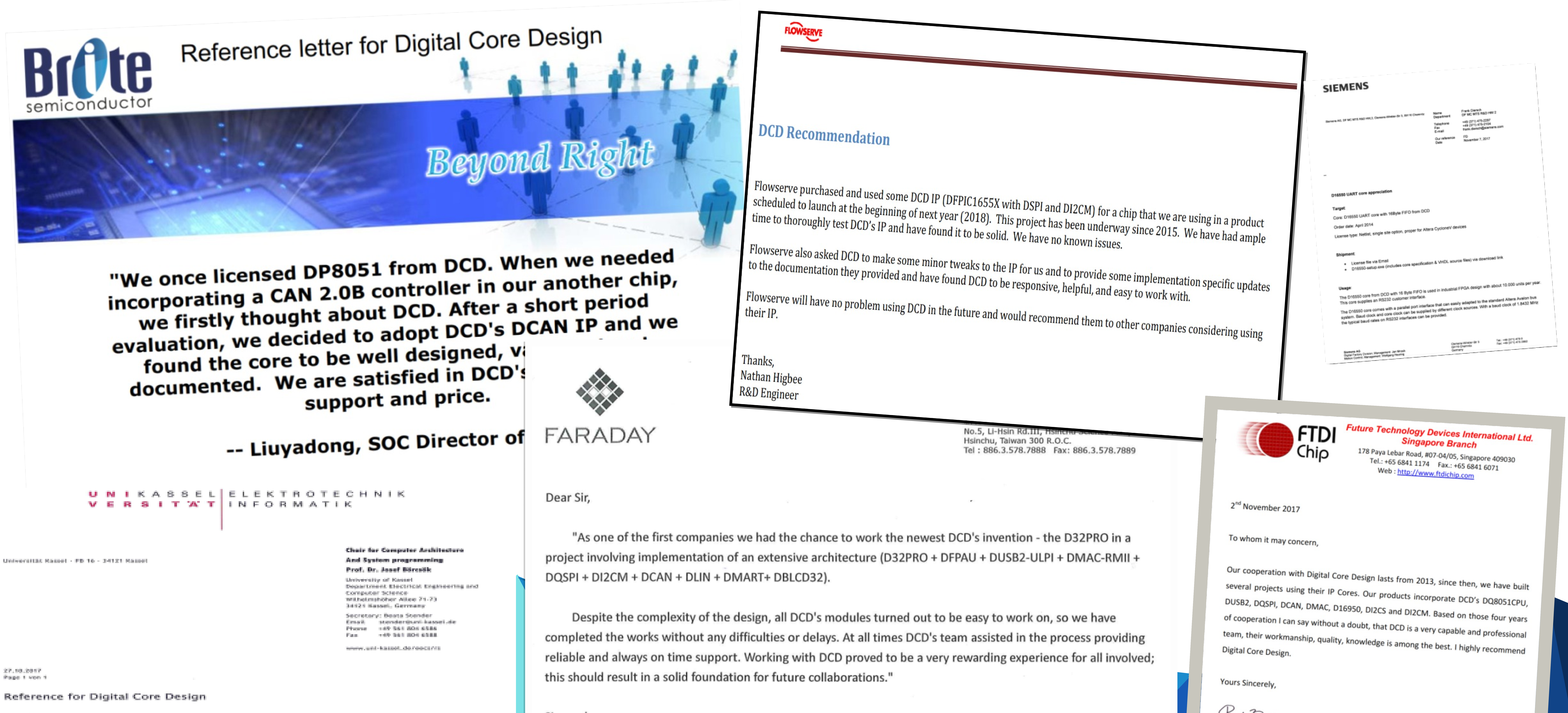
Pls vote for CryptOne for ”Best Innovative IP prize”

- ✓ C software drivers with API
- ✓ Silicon proven architecture
- ✓ Hardware code:
  - VERILOG Source Code or
  - FPGA Netlist
- ✓ VERILOG test bench environment
- ✓ Technical documentation
- ✓ Synthesis scripts
- ✓ 12 months of free technical support included

Summary

Pls vote for CryptOne for "Best Innovative IP prize"

- Success stories are the best confirmation for DCD's quality



Brite semiconductor

Reference letter for Digital Core Design

Beyond Right

"We once licensed DP8051 from DCD. When we needed incorporating a CAN 2.0B controller in our another chip, we firstly thought about DCD. After a short period evaluation, we decided to adopt DCD's DCAN IP and we found the core to be well designed, va documented. We are satisfied in DCD's support and price.

-- Liuyadong, SOC Director of

FLOWSERVE

DCD Recommendation

Flowserve purchased and used some DCD IP (DFPIC1655X with DSPI and DI2CM) for a chip that we are using in a product scheduled to launch at the beginning of next year (2018). This project has been underway since 2015. We have had ample time to thoroughly test DCD's IP and have found it to be solid. We have no known issues.

Flowserve also asked DCD to make some minor tweaks to the IP for us and to provide some implementation specific updates to the documentation they provided and have found DCD to be responsive, helpful, and easy to work with.

Flowserve will have no problem using DCD in the future and would recommend them to other companies considering using their IP.

Thanks,
Nathan Higbee
R&D Engineer

SIEMENS

Siemens AG, DF MC MTS R&D HW 2, Clemens-Winkler-Str 3, 09116 Chemnitz

Name	Frank Diersch
Department	DF MC MTS R&D HW 2
Telephone	+49 (371) 475-2297
Fax	+49 (371) 475-2104
E-mail	frank.diersch@siemens.com
Our reference	FD
Date	November 7, 2017

D16550 UART core appreciation

Target:

Core: D16550 UART core with 16Byte FIFO from DCD

Order date: April 2014

License type: Netlist, single site option, proper for Altera CycloneV devices

Shipment:

- License file via Email
- D16550-setup.exe (includes core specification & VHDL source files) via download link

Usage:

The D16550 core from DCD with 16 Byte FIFO is used in industrial FPGA design with about 10.000 units per year. This core supplies an RS232 customer interface.

The D16550 core comes with a parallel port interface that can easily adapted to the standard Altera Avalon bus system. Baud clock and core clock can be supplied by different clock sources. With a baud clock of 1.8432 MHz the typical baud rates on RS232 interfaces can be provided.

Siemens AG
Digital Factory Division; Management: Jan Mrosik
Motion Control; Management: Wolfgang Heuring

Clemens-Winkler-Str 3
09116 Chemnitz
Germany

Tel.: +49 (371) 475 0
Fax: +49 (371) 475 2992

UNIKASSEL VERSITÄT | ELEKTROTECHNIK INFORMATIK

Universität Kassel · FB 16 · 34121 Kassel

Chair for Computer Architecture
And System programming
Prof. Dr. Josef Börcsök

University of Kassel
Department Electrical Engineering and
Computer Science
Wilhelmshöher Allee 71-73
34121 Kassel, Germany

Secretary: Beata Stender
Email stender@uni-kassel.de
Phone +49 561 804 6586
Fax +49 561 804 6588

www.uni-kassel.de/eecs/rs

27.10.2017
Page 1 von 1

Reference for Digital Core Design

FARADAY

No.5, Li-Hsin Rd.III, Hsinchu Science
Hsinchu, Taiwan 300 R.O.C.
Tel : 886.3.578.7888 Fax: 886.3.578.7889

Dear Sir,

"As one of the first companies we had the chance to work the newest DCD's invention - the D32PRO in a project involving implementation of an extensive architecture (D32PRO + DFPAU + DUSB2-ULPI + DMAC-RMII + DQSPI + DI2CM + DCAN + DLIN + DMART+ DBLCD32).

Despite the complexity of the design, all DCD's modules turned out to be easy to work on, so we have completed the works without any difficulties or delays. At all times DCD's team assisted in the process providing reliable and always on time support. Working with DCD proved to be a very rewarding experience for all involved; this should result in a solid foundation for future collaborations."

FTDI Chip

Future Technology Devices International Ltd.
Singapore Branch
178 Paya Lebar Road, #07-04/05, Singapore 409030
Tel.: +65 6841 1174 Fax.: +65 6841 6071
Web : http://www.ftdichip.com

2nd November 2017

To whom it may concern,

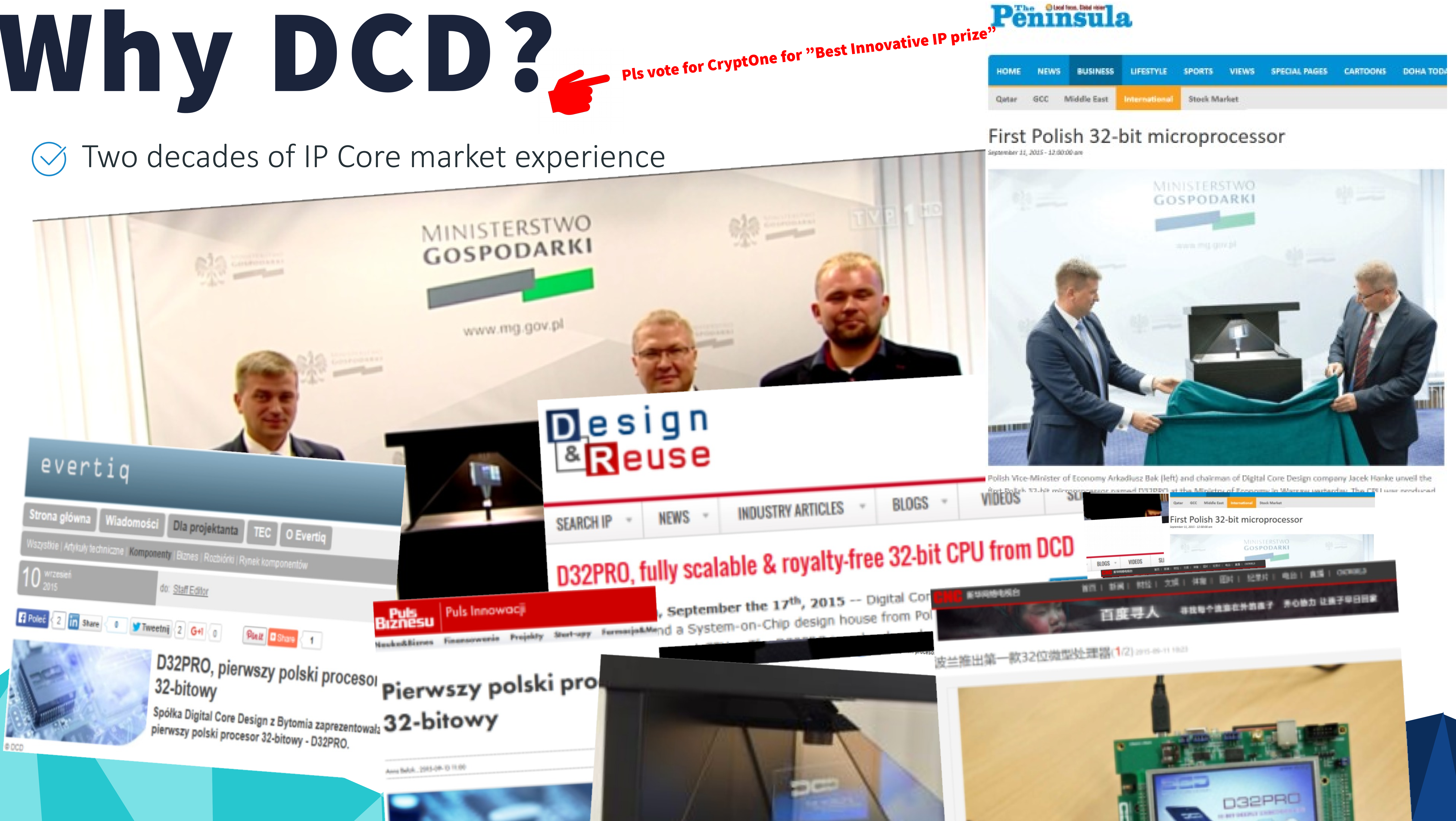
Our cooperation with Digital Core Design lasts from 2013, since then, we have built several projects using their IP Cores. Our products incorporate DCD's DQ8051CPU, DUSB2, DQSPI, DCAN, DMAC, D16950, DI2CS and DI2CM. Based on those four years of cooperation I can say without a doubt, that DCD is a very capable and professional team, their workmanship, quality, knowledge is among the best. I highly recommend Digital Core Design.

Yours Sincerely,

Why DCD?

Pls vote for CryptOne for ”Best Innovative IP prize”

- ✓ Two decades of IP Core market experience



The Peninsula

HOME | NEWS | BUSINESS | LIFESTYLE | SPORTS | VIEWS | SPECIAL PAGES | CARTOONS | DOHA TODA

Qatar | GCC | Middle East | International | Stock Market

First Polish 32-bit microprocessor

September 11, 2015 - 12:00:00 am

Polish Vice-Minister of Economy Arkadiusz Bak (left) and chairman of Digital Core Design company Jacek Hanke unveil the first Polish 32-bit microprocessor named D32PRO at the Ministry of Economy in Warsaw yesterday. The CPU was produced

Design & Reuse

SEARCH IP | NEWS | INDUSTRY ARTICLES | BLOGS | VIDEOS | SL

D32PRO, fully scalable & royalty-free 32-bit CPU from DCD

, September the 17th, 2015 -- Digital Cor …nd a System-on-Chip design house from Pol

evertiq

Strona główna | Wiadomości | Dla projektanta | TEC | O Evertiq

Wszystkie | Artykuły techniczne | Komponenty | Biznes | Rozbiórki | Rynek komponentów

10 wrzesień 2015 do: Staff Editor

D32PRO, pierwszy polski procesor 32-bitowy

Spółka Digital Core Design z Bytomia zaprezentowała pierwszy polski procesor 32-bitowy - D32PRO.

© DCD

Puls Biznesu | Puls Innowacji

Nauka&Biznes | Finansowanie | Projekty | Start-upy | Formacja&Men

Pierwszy polski pro 32-bitowy

CNC 新华网络电视台

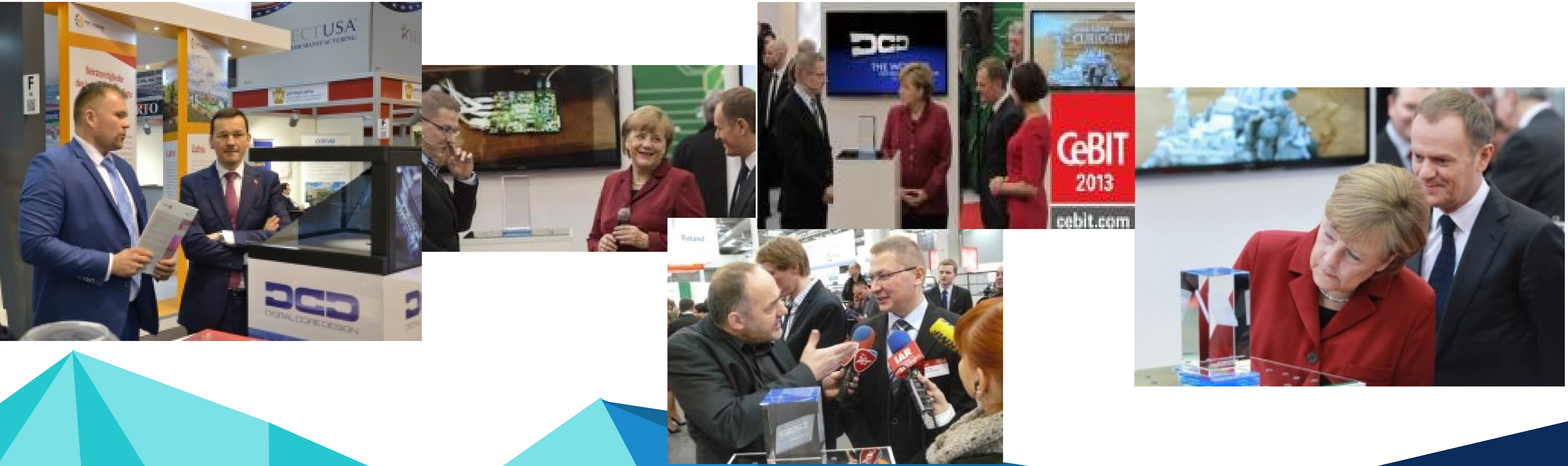
百度寻人

波兰推出第一款32位微型处理器(1/2) 2015-09-11 18:23

Why DCD?

Pls vote for CryptOne for ”Best Innovative IP prize”

- DCD presented World’s fastest 8051 CPU during CeBIT 2013 official opening ceremony (in front of German Chancellor A. Merkel and EU President D. Tusk)
- D32PRO has been presented during EXPO in Milan and Hannover Messe

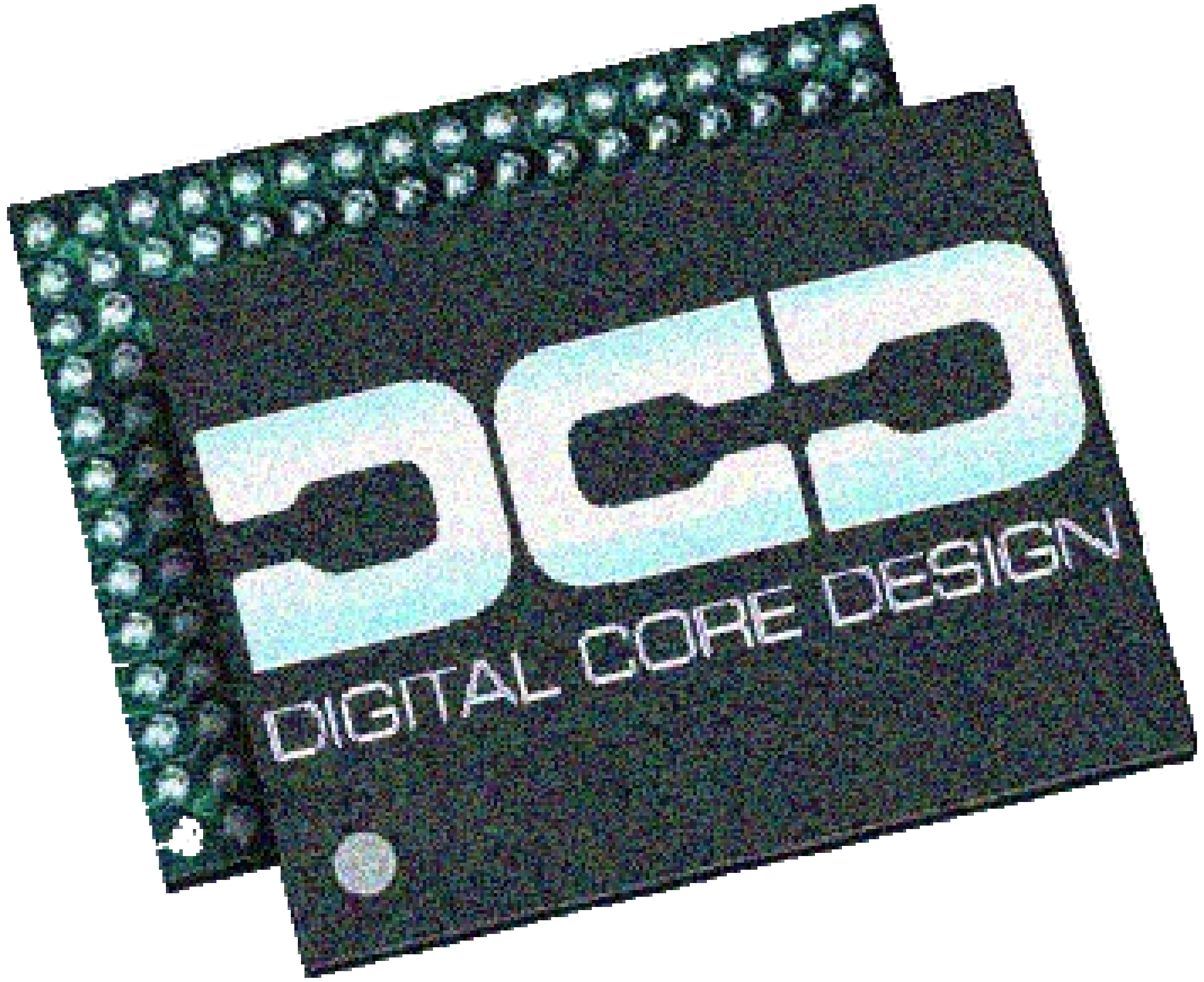


Why DCD?

Pls vote for CryptOne for ”Best Innovative IP prize”

- Innovative products – always step ahead before competitors
- Know-how based on two decades of market exprience
- Optimal solutions which answers market needs
- Significant Time-to-market reduction
- Coherent IP Core portfolio
- IP Cores tailored to the project needs
- Complete solution from one company

  like e.g.: IP Core + debugger + ...



Pls vote for CryptOne for ”Best Innovative IP prize”

Thank you!

Any questions?

info@dcd.pl