NANOXPLORE FPGA ULTRA300 SECURITY FEATURES

24/10/2024

Patrice Brossard

NanoXplore

ABSTRACT

Nanoxplore leads Europe in the design and development of SoC FPGAs made for harsh environment applications including Space and Avionics.

Nowadays, in all domains including Space, there is an expectation of a solution that meets security requirements by at least securing the bitstream and controlling the lifecycle of the device. Attackers have many motivations to recover and manipulate bitstream, including design cloning or manipulation, IP theft, etc.

Thus, in the ULTRA family, bitstream encryption has been introduced. During this session, we will present Nanoxplore solutions and its key differentiators with a focus on the latest ULTRA300 FPGA that includes dedicated security features.

Agenda

- **NanoXplore intro**
  - Who are we
  - Key differentiators
  - Key market targeted
- Solutions overview
  - Products (FPGA / SoC) and tools
  - Flight Heritage
- Security and NanoXplore
  - Important Features
- Summary - Q&A

NanoXplore

European Leader in FPGA and SoC FPGA

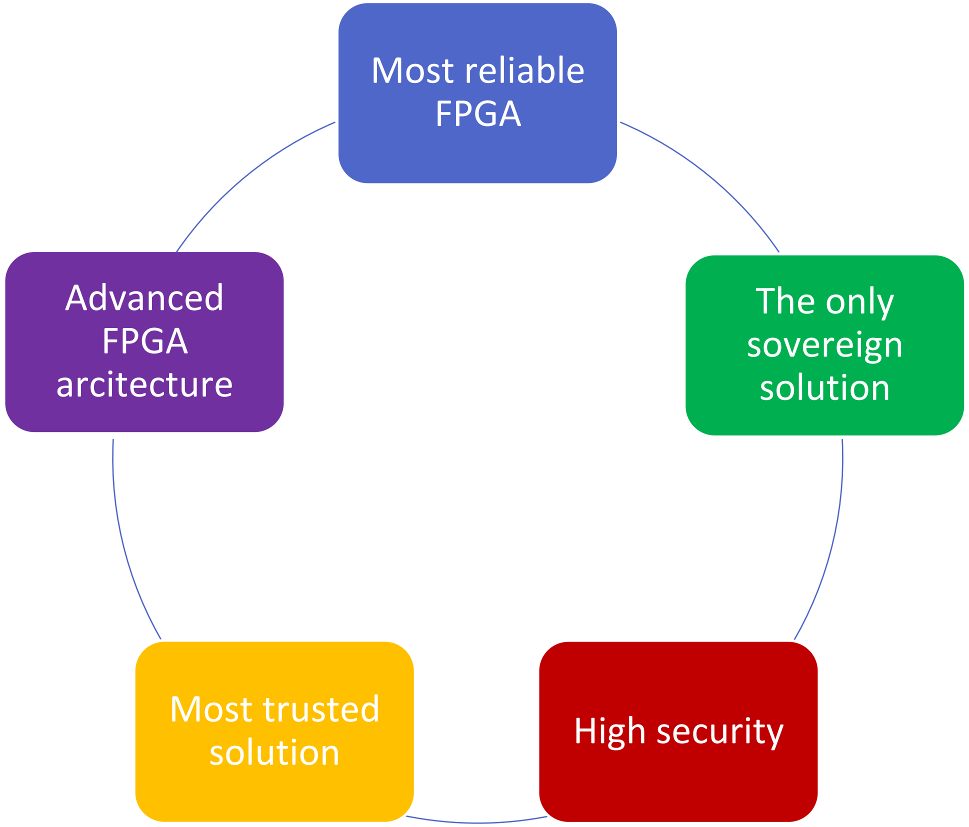
NanoXplore is the EU solution for Programmable Logic Devices

- Nanoxplore has a complete range of radiation-resistant FPGAs with associated tools
- All the tools and IPs required to develop simple to complex designs
  - IMPULSE is the graphical software suite that translates an RTL model into a bitstream
  - NXBASE2 / OpenOCD performs bitstream loading and debugging
  - NX NG-ULTRA SDK with BSP to build system for embedded software

NX Key Differentiators vs. Competition

Compared to current competition, NX offers key differentiators

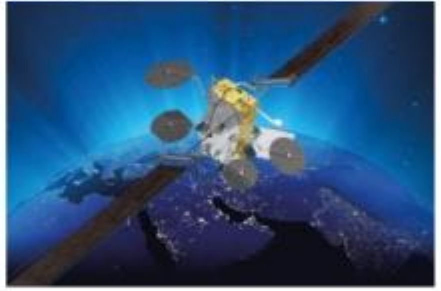
1. Expert in design reliability (radiation, aging etc) → main reason why end-users are selecting NX offering in Space
2. Sovereign offering → most trusted FPGA vendor for European end-users
3. High security features → more and more required for strategic markets
4. Leverage STMicroelectronics supply chain to offer low-cost version of our components
   - ST is well known for setting up very cost-effective supply chain for consumer markets
5. Improve our low-power and high-density FPGA architecture
   - Better address application at the edge
   - Clear differentiator high end FPGA



Key targeted markets

- First mission for the company is to offer SoC FPGA for Hi-Rel markets
- Focusing on key market differentiators like ITAR free, radiation hardening, very high reliability, etc
- Become quickly a clear leader on Space, Defense and Avionic market

Space



Avionic

Défense

Agenda

- NanoXplore intro
  - Who are we
  - Key differentiators
  - Key market targeted
- **Solutions overview**
  - Products (FPGA / SoC) and tools
  - Flight Heritage
- Security and NanoXplore
  - Important Features
- Summary - Q&A

NanoXplore

Current products and tools

2017

NG medium

Low-End FPGA

- 35kLUTs/32kDFFs
- 3Mb RAM
- 112 DSP
- No HSSL
- No Hard IP Processor

2021

NG ultra

High-End SoC FPGA

- 537kLUTs/505kDFFs
- 32Mb RAM
- 1344 DSP
- 32x HSSL 12G
- Quad-core ARM-R52

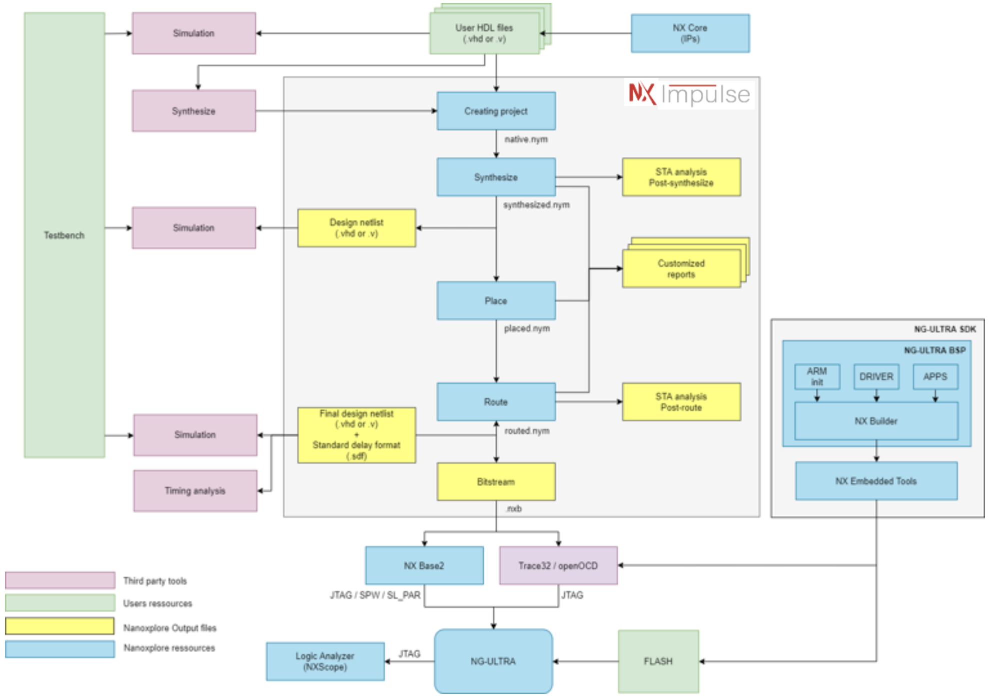
2024

ultra300

Mid-End FPGA

- 290kLUTs/273kDFFs
- 21Mb RAM
- 896 DSP
- 16x HSSL 12G
- ADC/DAC

Nxdesign suite :
a complete design flow



Flight heritage

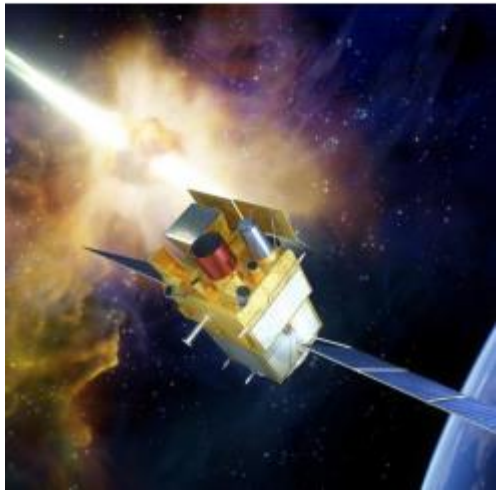
- Hera mission (ESA)
  launch Oct 7th

- NG-MEDIUM

- DORn
  Detection of
  Outgassing RadoN on
  the moon

- NG-MEDIUM

- SVOM
  Space Variable Objects Monitor.
  Study the gamma-ray bursts
  from explosion of stars (LEO)



- NG-MEDIUM

Flight to come - 2025

- Galileo CMCU
  MEO Mission

- NG-MEDIUM

- SMILE (ESA)
  LEO Mission

- NG-MEDIUM

- More to come ....

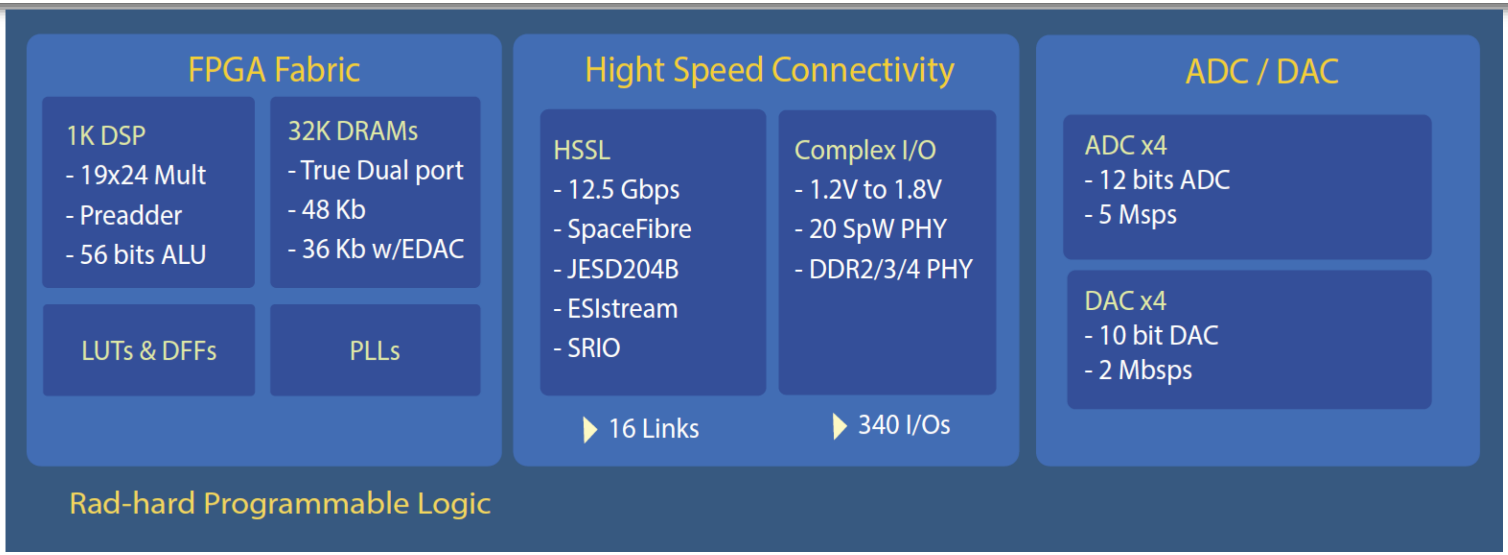
Agenda

- NanoXplore intro
  - Who are we
  - Key differentiators
  - Key market targeted
- Solutions overview
  - Products (FPGA / SoC) and tools
  - Flight Heritage
- **Security and NanoXplore**
  - Important Features
- Summary - Q&A

NanoXplore

ULTRA300

Overview



FPGA Fabric

1K DSP
- 19x24 Mult
- Preadder
- 56 bits ALU

32K DRAMs
- True Dual port
- 48 Kb
- 36 Kb w/EDAC

LUTs & DFFs

PLLs

Hight Speed Connectivity

HSSL
- 12.5 Gbps
- SpaceFibre
- JESD204B
- ESIstream
- SRIO

Complex I/O
- 1.2V to 1.8V
- 20 SpW PHY
- DDR2/3/4 PHY

16 Links

340 I/Os

ADC / DAC

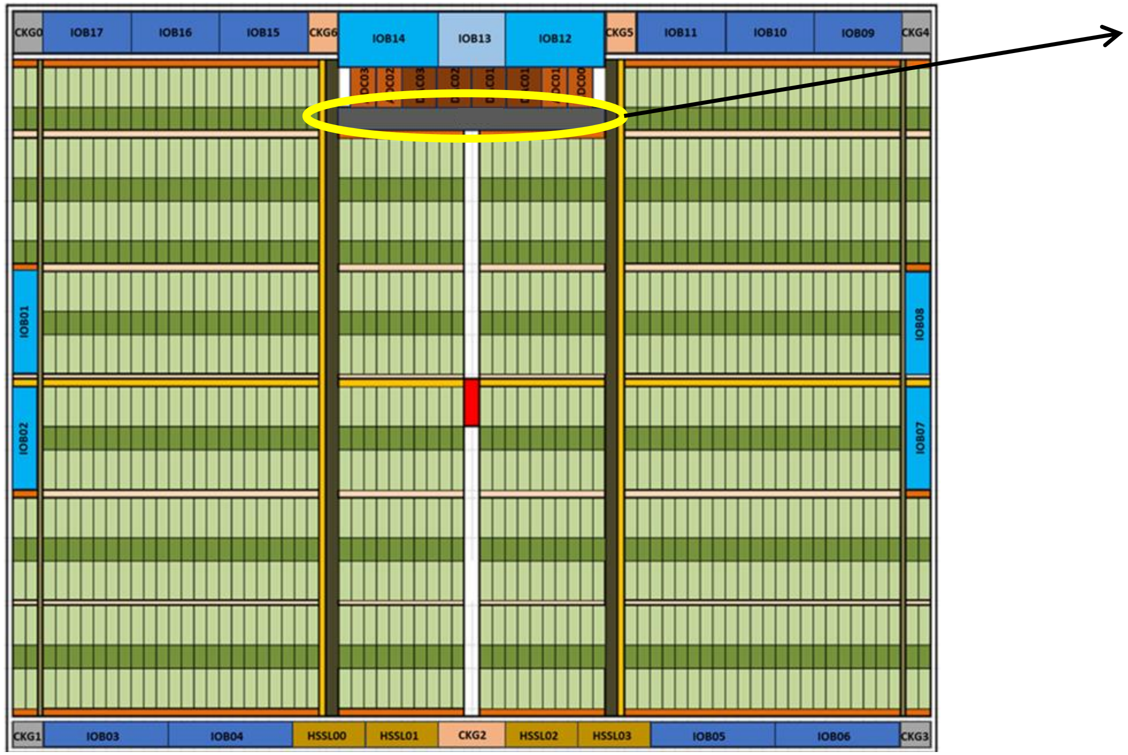
ADC x4
- 12 bits ADC
- 5 Msps

DAC x4
- 10 bit DAC
- 2 Mbsps

Rad-hard Programmable Logic

- ULTRA300 is a pure 300kLUTs FPGA based on the architecture of the NG-ULTRA’s fabric 28nm FDSOI (ST)
- Rad Hard by design
- DAC and ADC has been added for current and voltage monitoring for example
- Bitstream management for
  - Confidentiality (Encryption)
  - Authentification
  - Integrity (Configuration Memory Integrity Check)
- Environment monitoring

ULTRA300 – security features



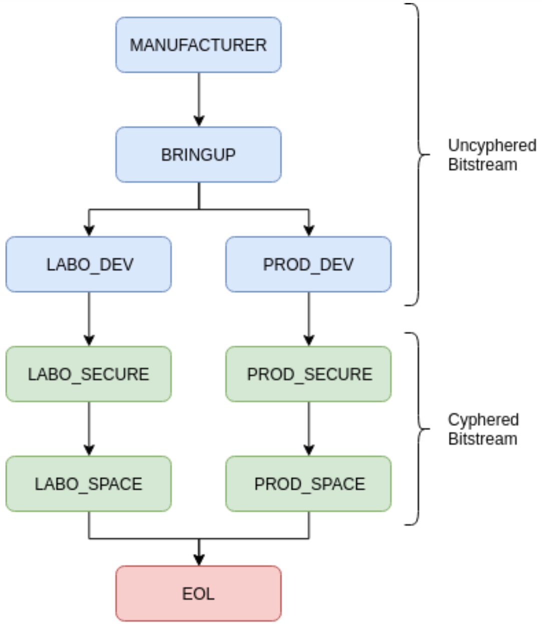
- The **FPGA_manager** block embeds secure **bitstream manager** and other security features
- Embedded AES256 encryption in the bitstream manager (BSM)
  - The EAX mode is supported that implements authenticated encryption with additional data (AEAD)
- True Number Random Generator (TNRG).
- Environmental analysis for side attack - temperature and voltage sensors (VTSENS)
- OTP security registers
- Internal ring oscillator and internal Power On Reset dedicated to the BSM (BitStream Manager)
  - The TNRG is using this specific ring oscillator with several frequencies to generate internal random numbers made to protect the keys used to decrypt and authenticate the bistream.

ULTRA300 – Bitstream Manager

- Bitstream manager includes the **security manager** and **security OTP** that can be configured by the user.
- **Security OTP** register stores security assets :
  - Life cycle
  - Encryption Key
  - Authentification Key
  - Anti-Rollback Counter
  - Security configuration
- **Security manager** will generate some security alert :
  - The integrity of the non-volatile memory is not valid
  - The key integrity is not valid
  - An IO controller performs a non-permitted access
  - The authentication is not valid
  - The rollback counter is not valid
  - The bitstream integrity is not valid
  - The Voltage or Temperature is out of range

ULTRA300 – Life Cycle

- “Life Cycle” OTP registers:
  - It is made to track the Life cycle of the device after manufacturing :



- Life cycle status has an impact on access to some features and interfaces :

	Test Mode	Bitstream Encrypted and authenticated	Anti-rollback check	Always Reset
MANUFACTURER	Enable	No	N/A	No
BRINGUP	Disable	No	N/A	No
LABO_DEV	Disable	No	N/A	No
LABO_SECURE	Disable	Yes	Equal	No
LABO_SPACE	Disable	Yes	Greater or Equal	No
PROD_DEV	Disable	No	N/A	No
PROD_SECURE	Disable	Yes	Equal	No
PROD_SPACE	Disable	Yes	Greater or Equal	No
EOL	Disable	N/A	N/A	Yes

ULTRA300 – Environment monitoring

- Voltage and Temperature are monitored during bitstream download
- Voltage Range is configurable
- Temperature Range is configurable
- In “Space” Life Cycle stage, this Security Alert can be disable (User specification)

- *When Voltage and Temperature are out of range, security alert is asserted*

Addionnal details on the crytpo mechanism implemented

- As said previously, the symmetric-key algorithm AES in mode EAX AEAD (authenticated encryption with additional data) with 256 bits key size is used for bitstream encryption.
- The keys (encryption key and authentication key) can be stored in the FPGA during the life cycle "DEV" (prod-dev or labo-dev) and it is not reconfigurable.
- The user can then move to life cycle "SECURE" (prod-secure or labo-secure). The access to the FPGA will be always crypted and authenticate.
- A TNRG is used to generate some internal random numbers made to protect the keys that has been stored and the decrypted bitstream is no more accessible by the FPGA user.

- Any side attack using voltage or temperature will generate a security alert.

NanoXplore

Summary => Advanced products for an advanced market

☢ Radiation Hardened	• Amazing radiations results • No need for design mitigations (28 nm)
Local Supply chain	• STMicroelectronics foundry • European Sovereignty • ITAR Free
High Tech	• High Density FPGAs • High Performances • (HSSL)
🔒 Security	• Cryptographic Services

Q&A

NanoXplore