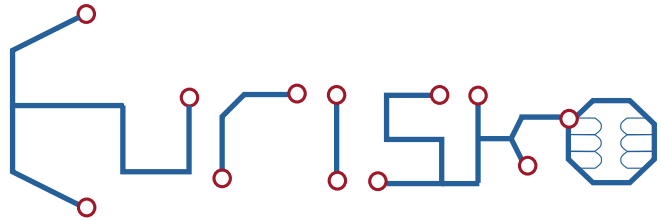


Développement d'une carte électronique sécurisée

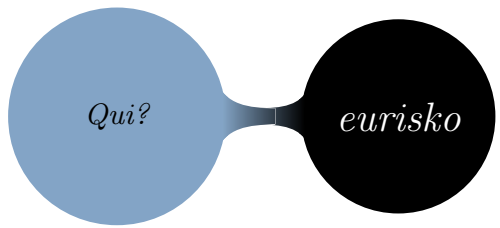
{LAM,LCR,LRP,LSC}@ANSSI

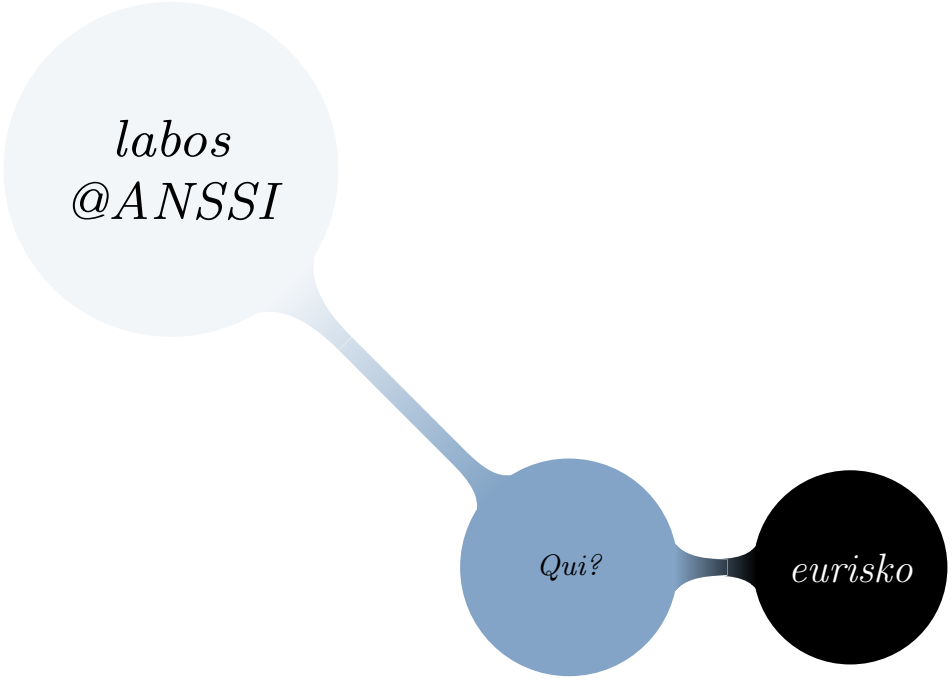
prenom.nom@ssi.gouv.fr

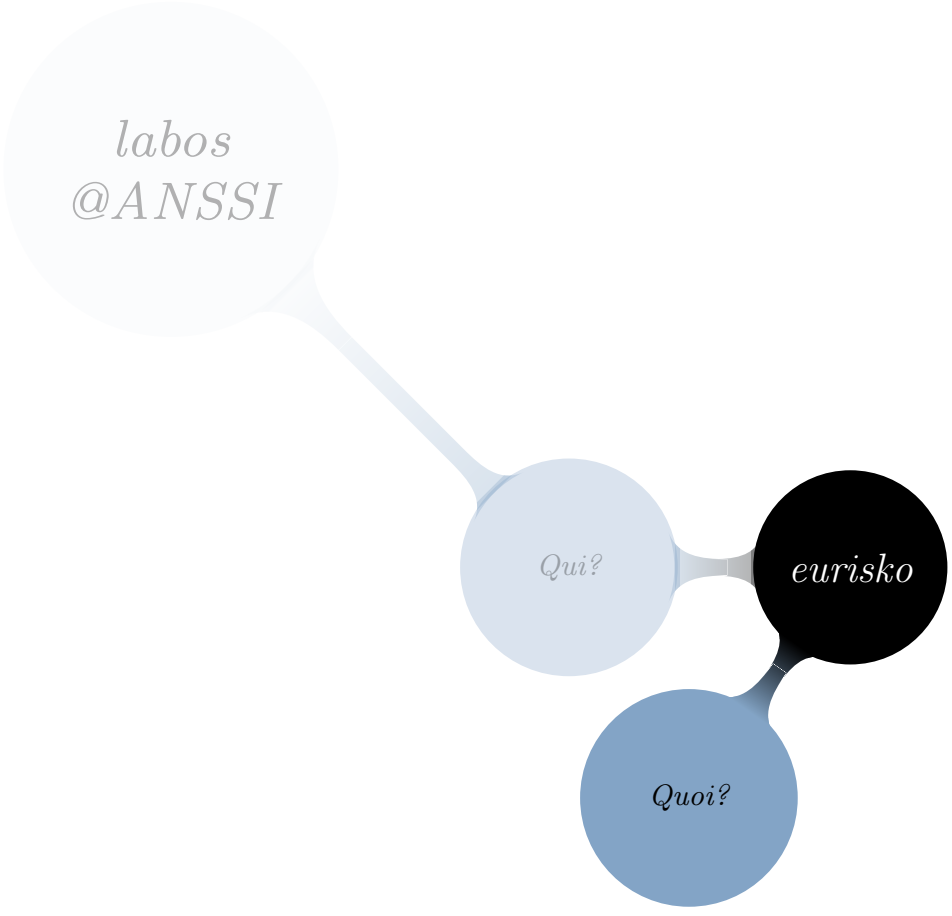
Symposium sur la
Sécurité des
Technologies de
l'**I**nformation et des
Communications

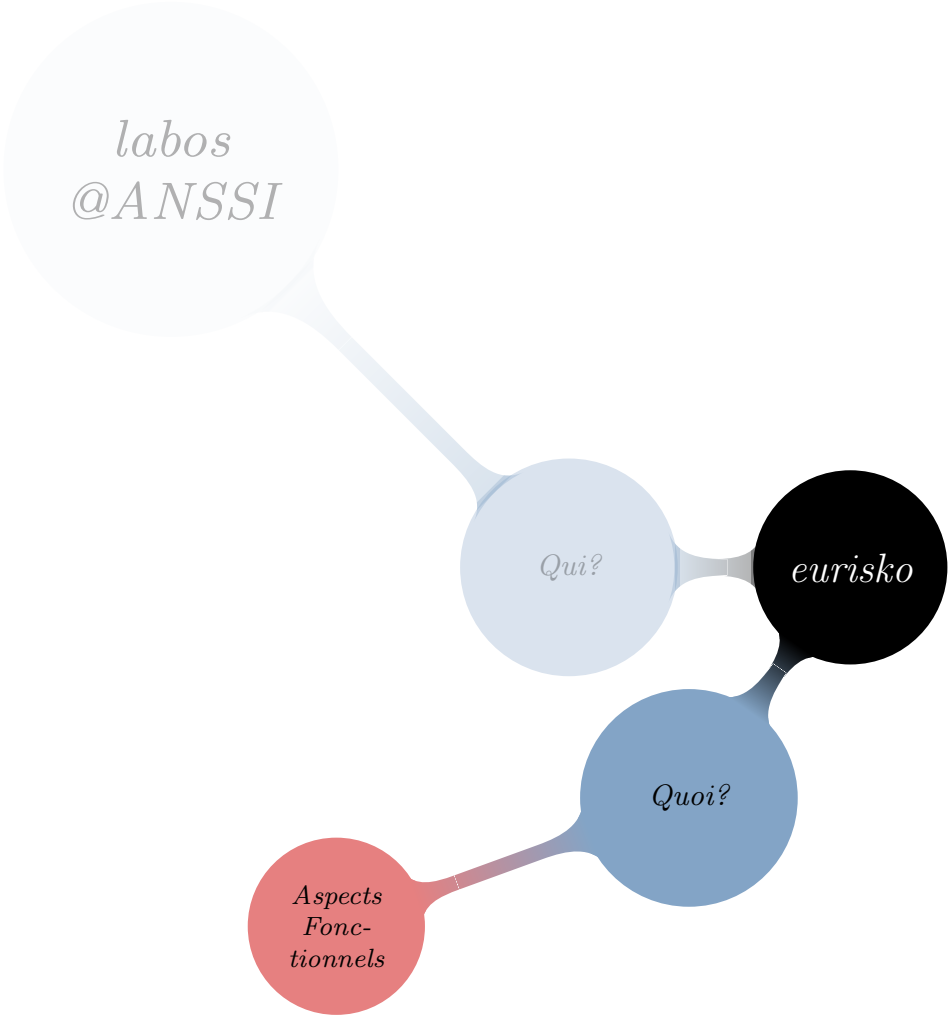
1er juin 2016

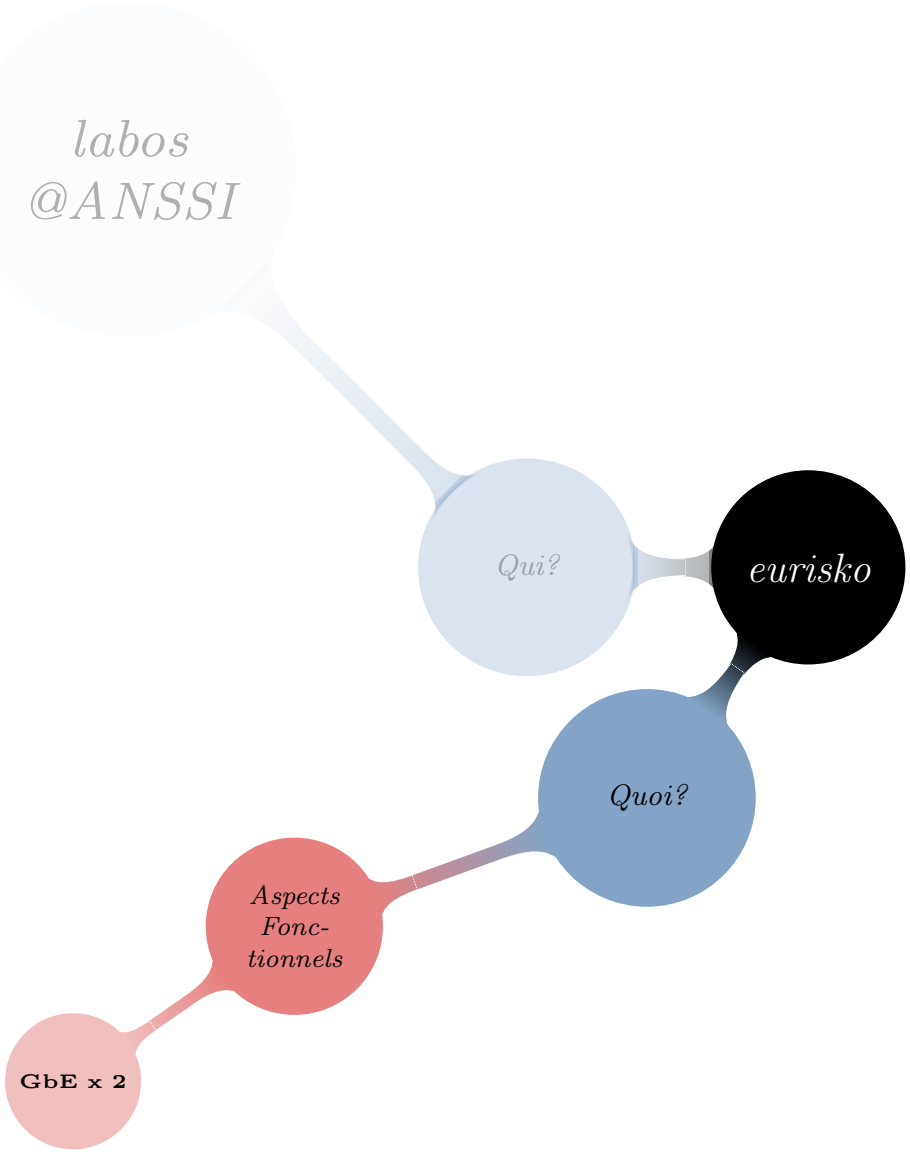

eurisko

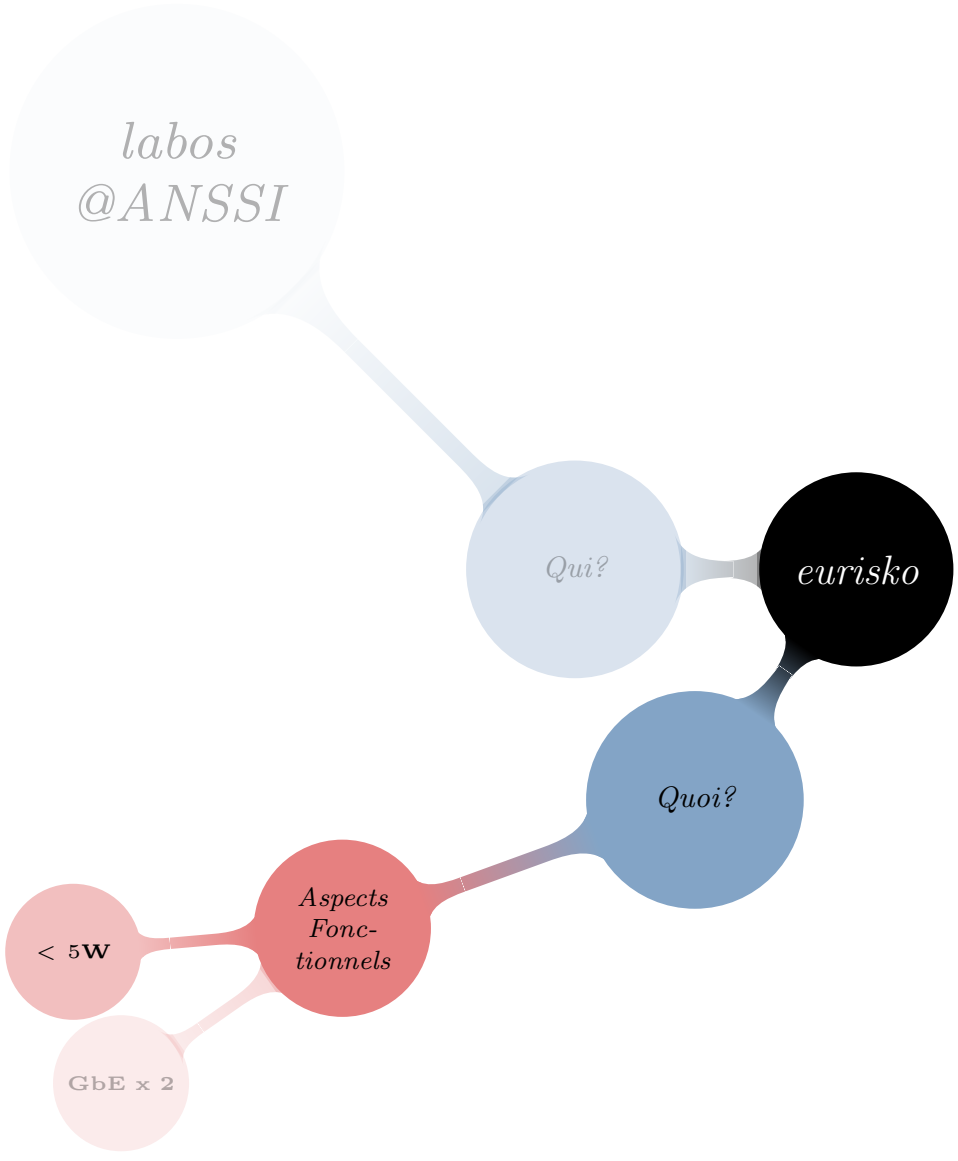

Qui?
eurisko

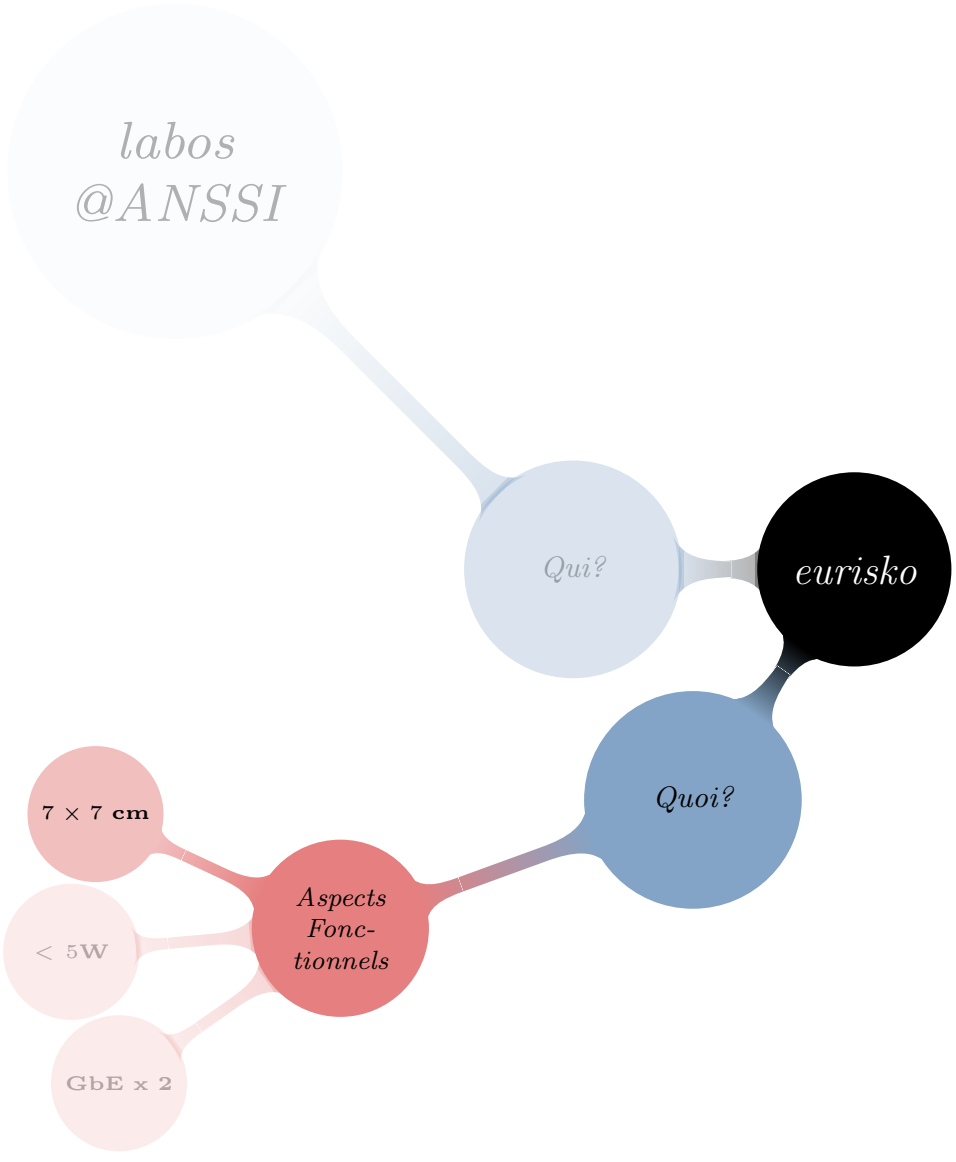

labos
@ANSSI
Qui?
eurisko

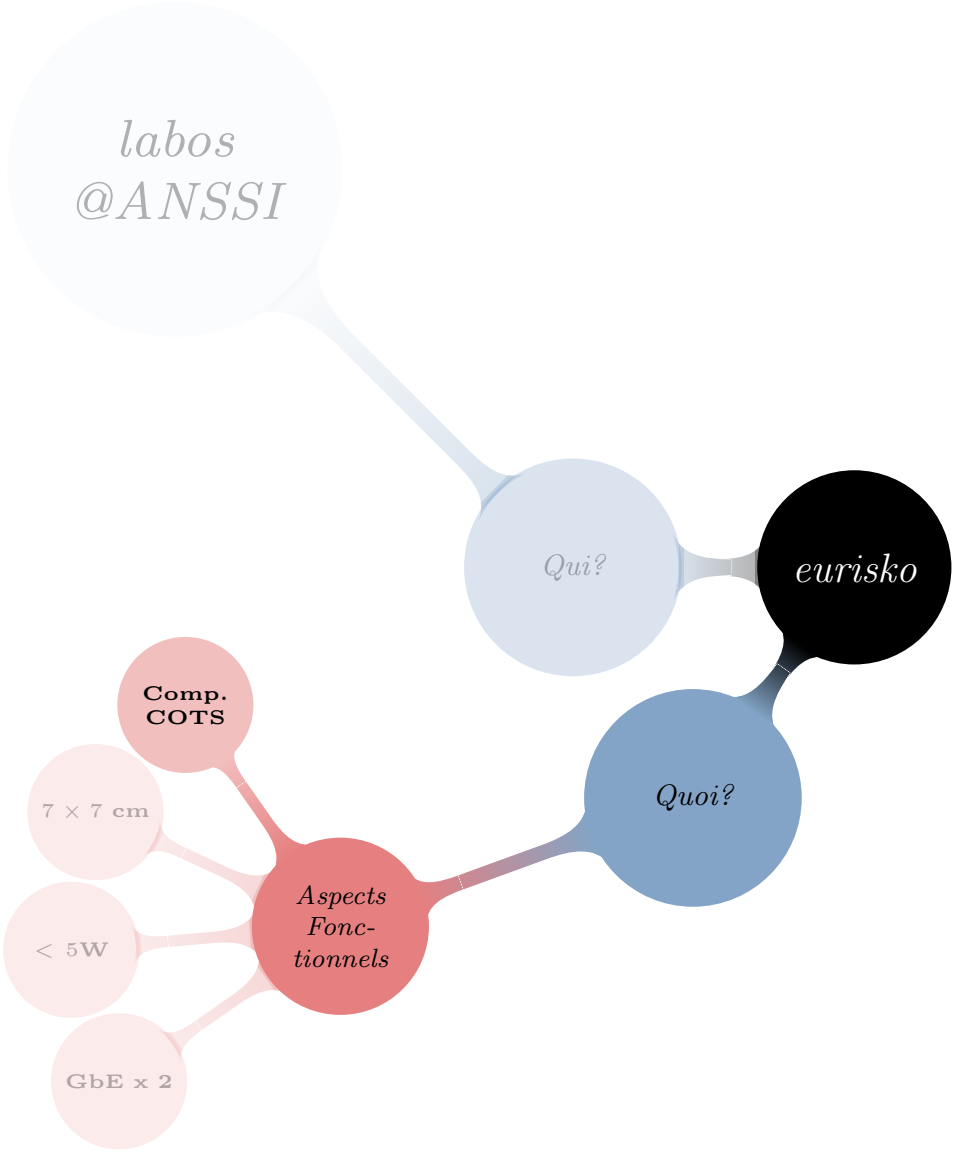

labos
@ANSSI
Qui?
eurisko
Quoi?

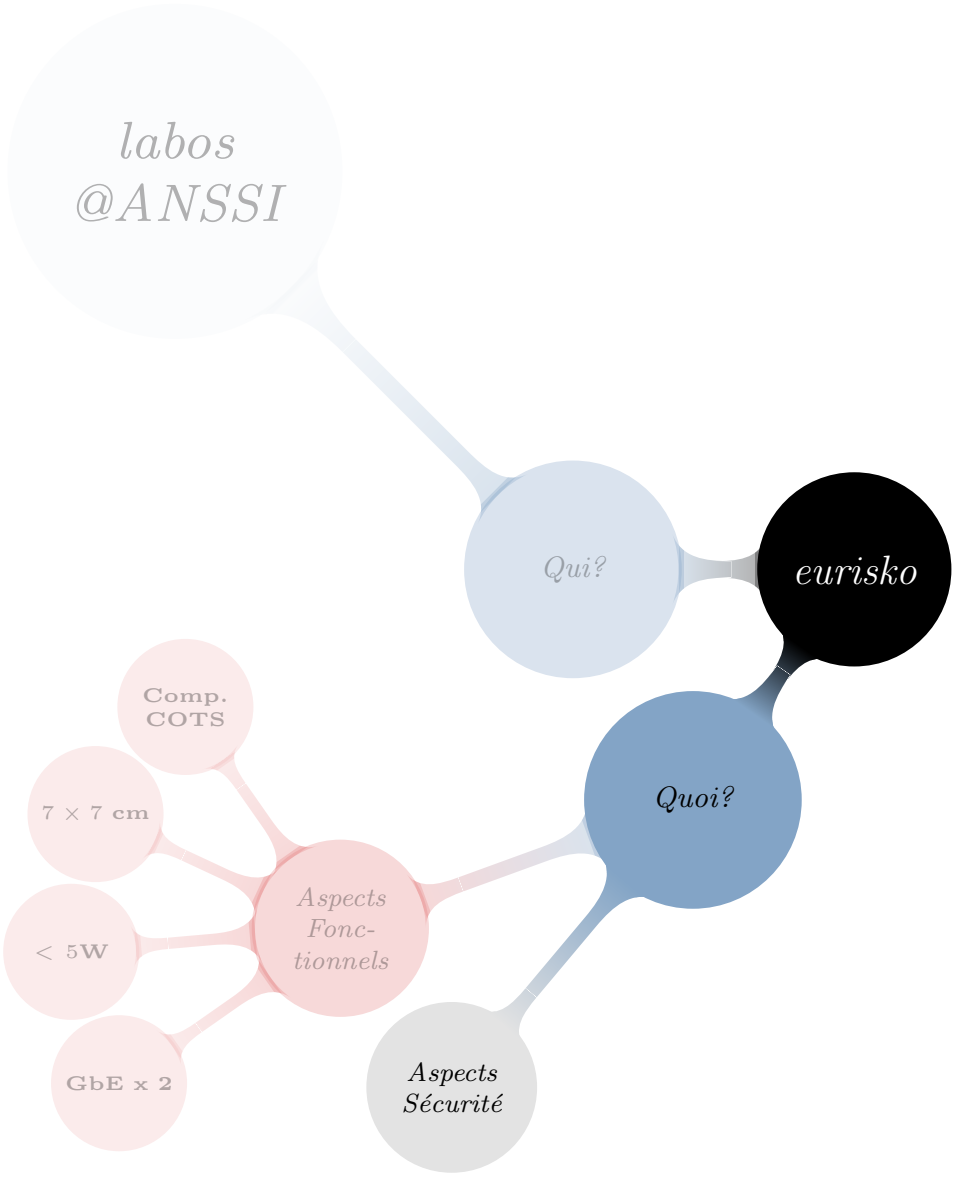

labos
@ANSSI
Qui?
eurisko
Quoi?
Aspects
Fonc-
tionnels

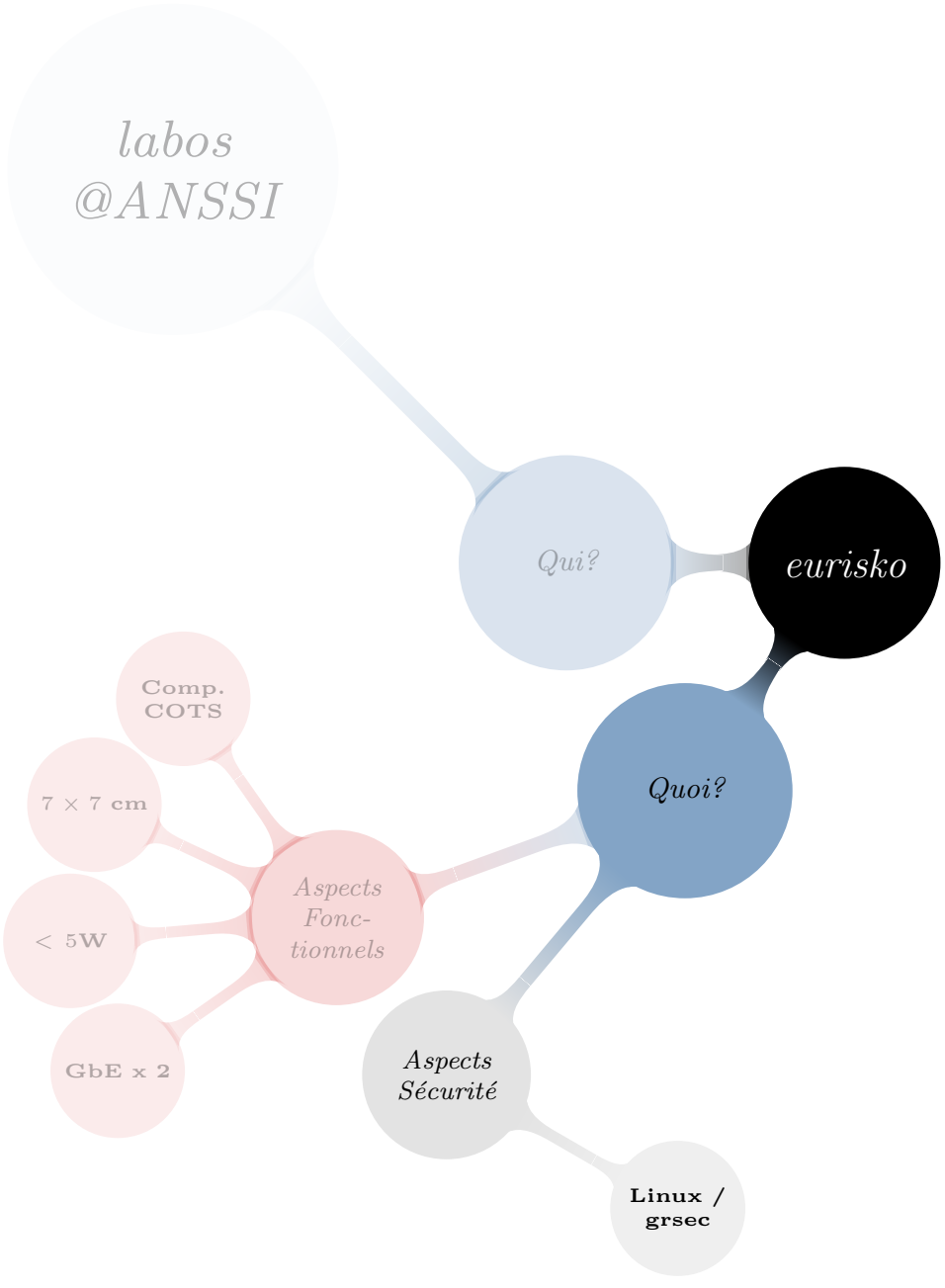

labos
@ANSSI
Qui?
eurisko
Quoi?
Aspects
Fonc-
tionnels
GbE x 2

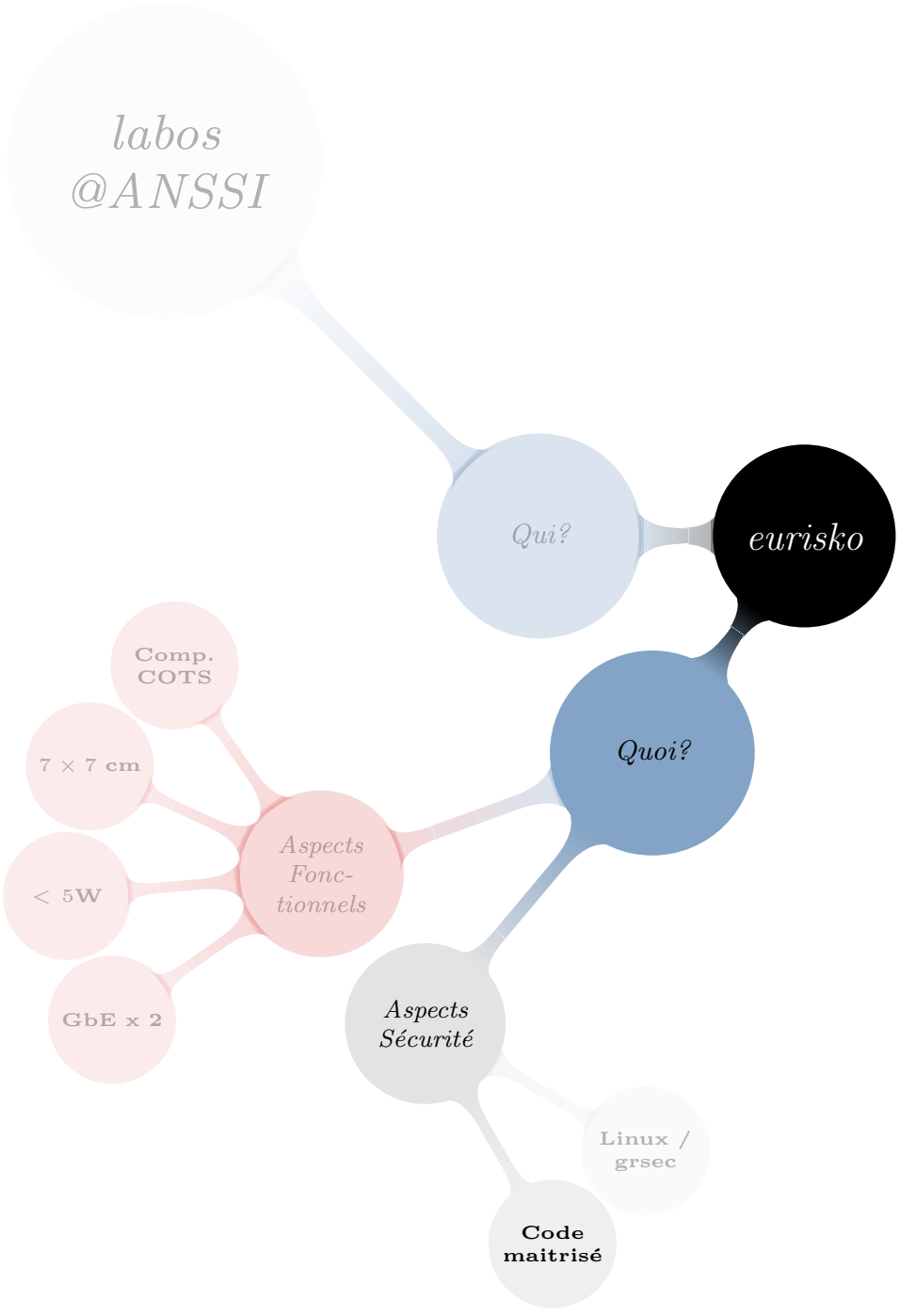

labos
@ANSSI
Qui?
eurisko
Quoi?
Aspects
Fonc-
tionnels
< 5W
GbE x 2

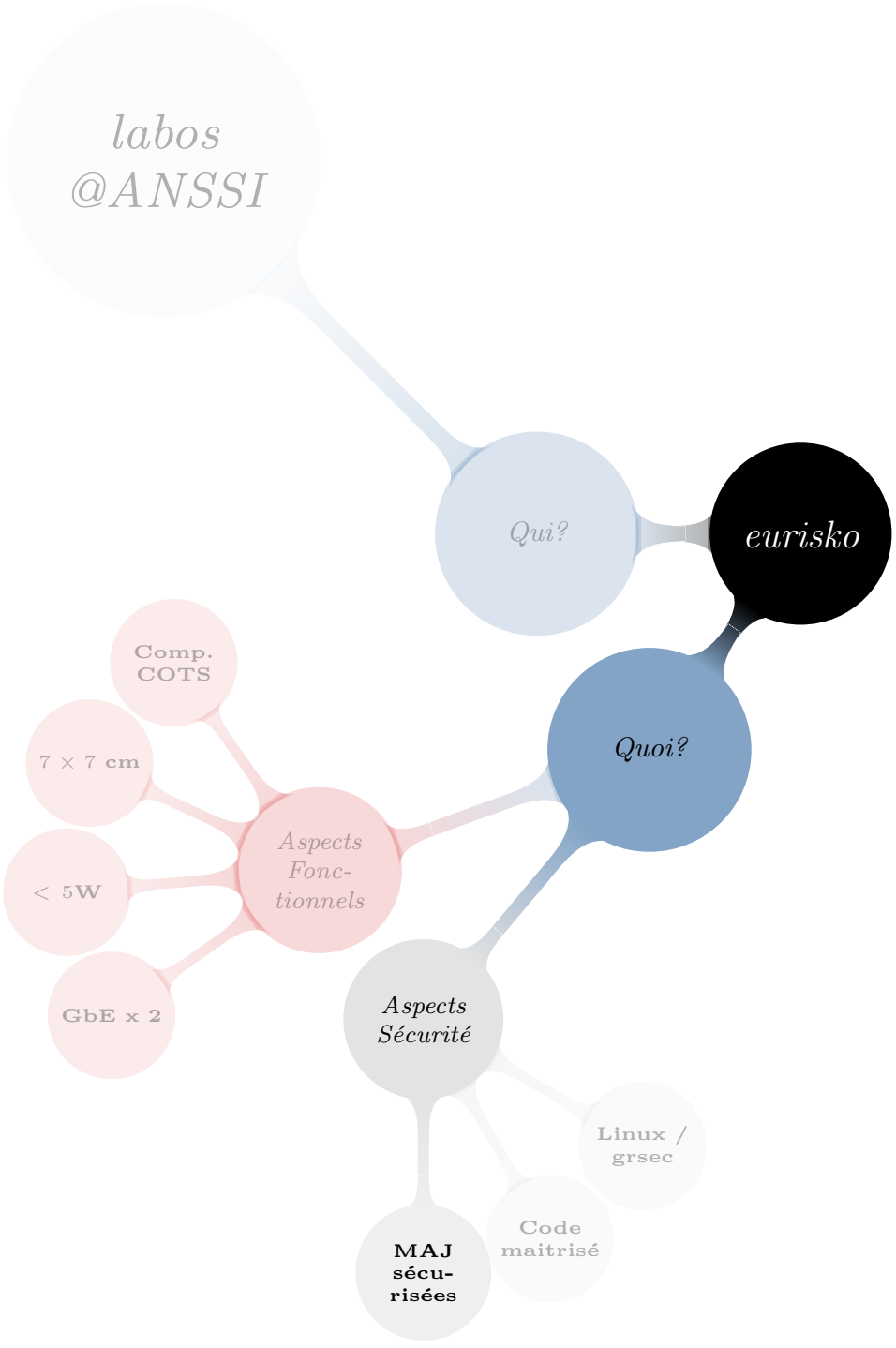

labos
@ANSSI
Qui?
eurisko
Quoi?
7 × 7 cm
Aspects
Fonc-
tionnels
< 5W
GbE x 2

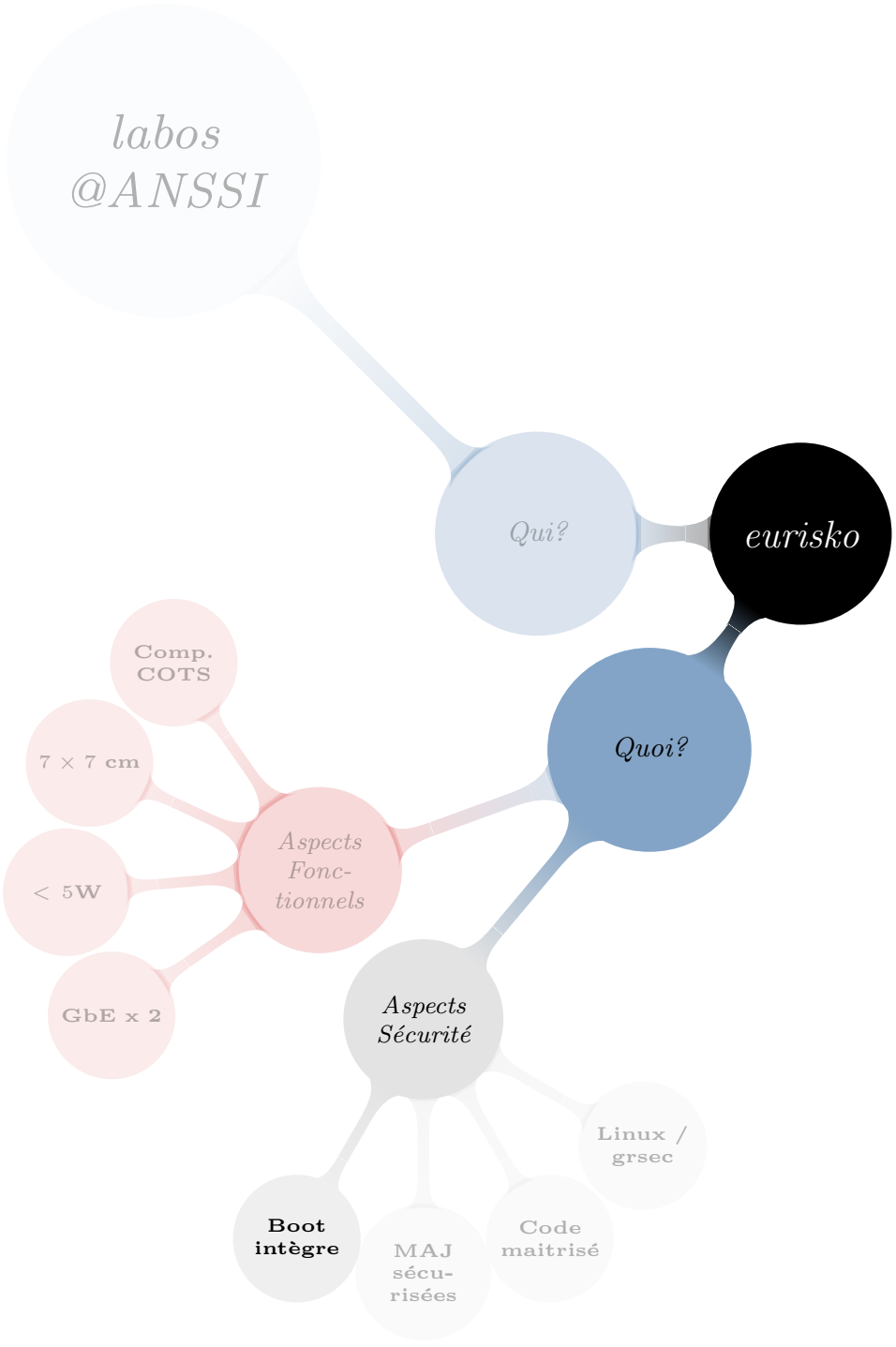

labos
@ANSSI
Qui?
eurisko
Quoi?
Comp.
COTS
7 × 7 cm
< 5W
GbE x 2
Aspects
Fonc-
tionnels

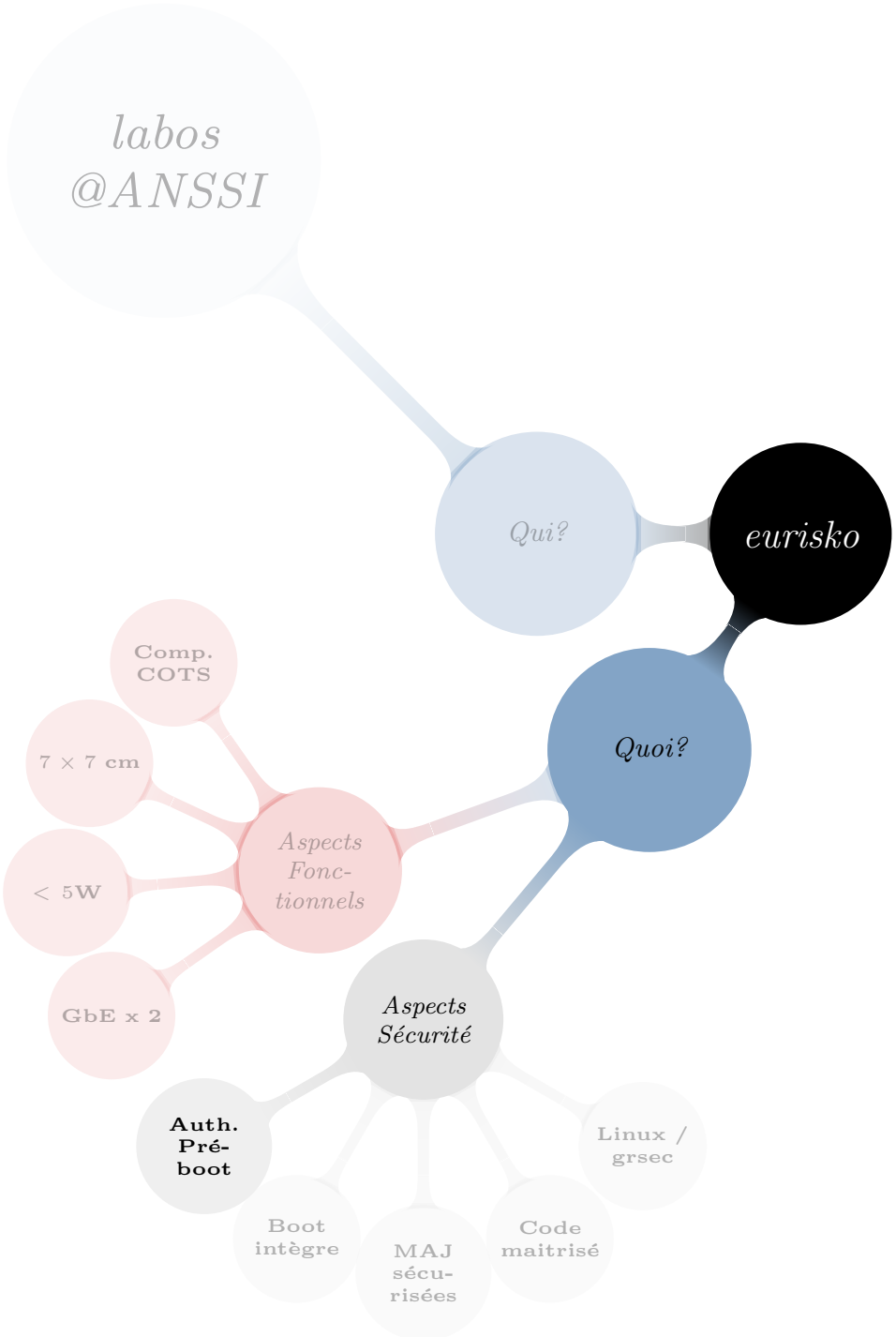

labos
@ANSSI
Qui?
eurisko
Quoi?
Comp.
COTS
7 × 7 cm
Aspects
Fonc-
tionnels
< 5W
GbE x 2
Aspects
Sécurité

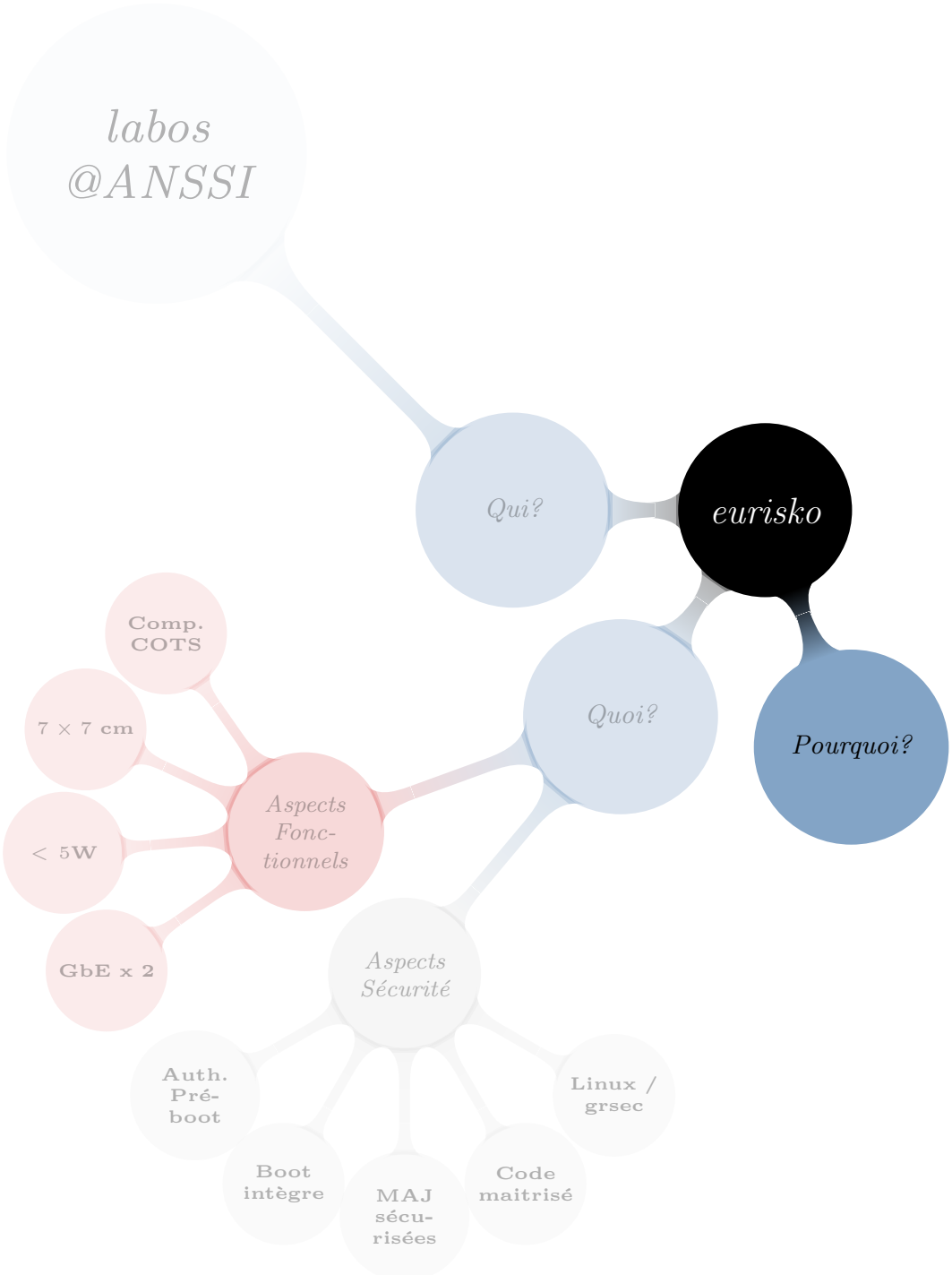

labos
@ANSSI
Qui?
eurisko
Quoi?
Comp.
COTS
7 × 7 cm
< 5W
GbE x 2
Aspects
Fonc-
tionnels
Aspects
Sécurité
Linux /
grsec

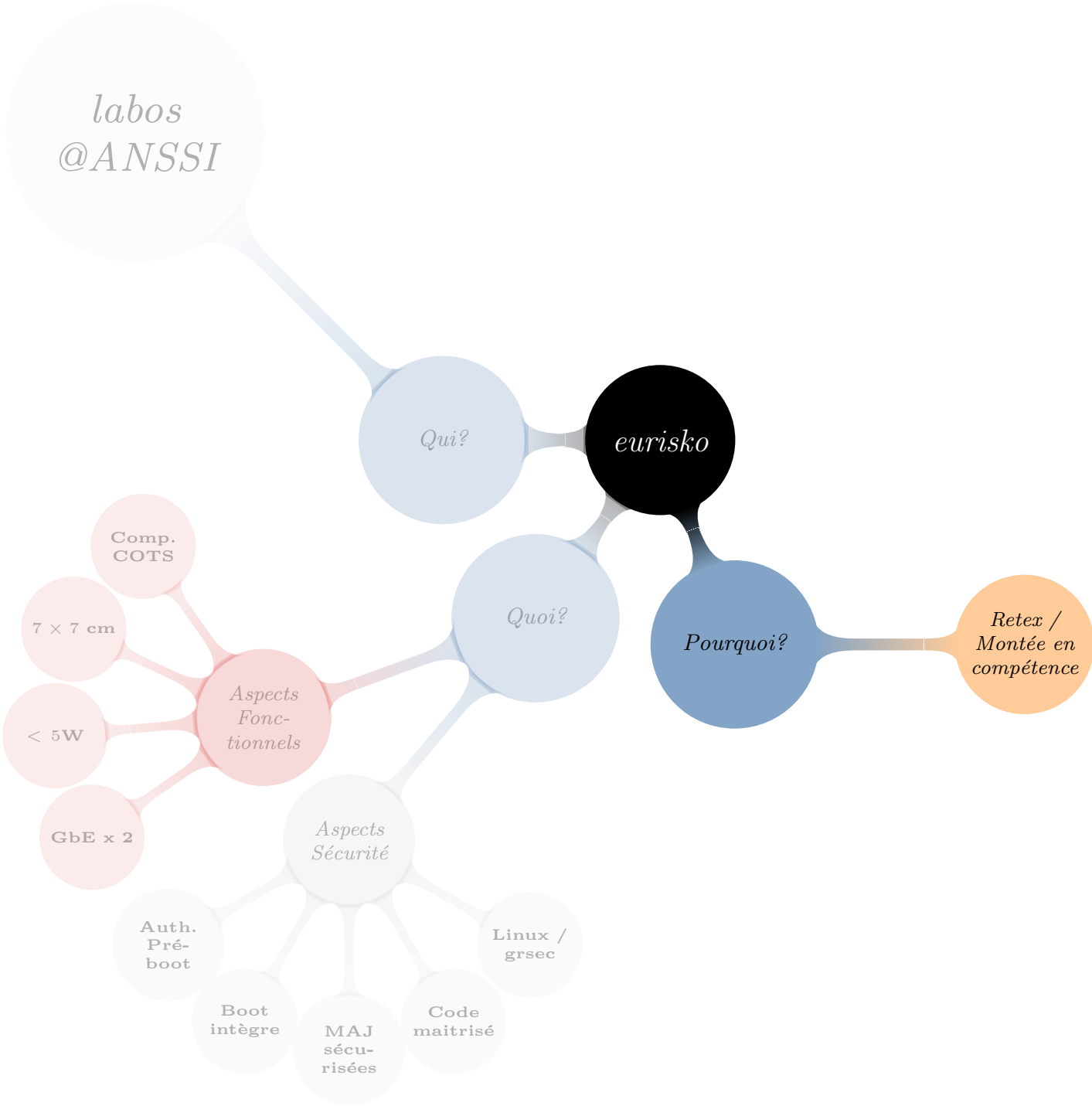

labos
@ANSSI
Qui?
eurisko
Quoi?
Comp.
COTS
7 × 7 cm
Aspects
Fonc-
tionnels
< 5W
GbE x 2
Aspects
Sécurité
Linux /
grsec
Code
maitrisé

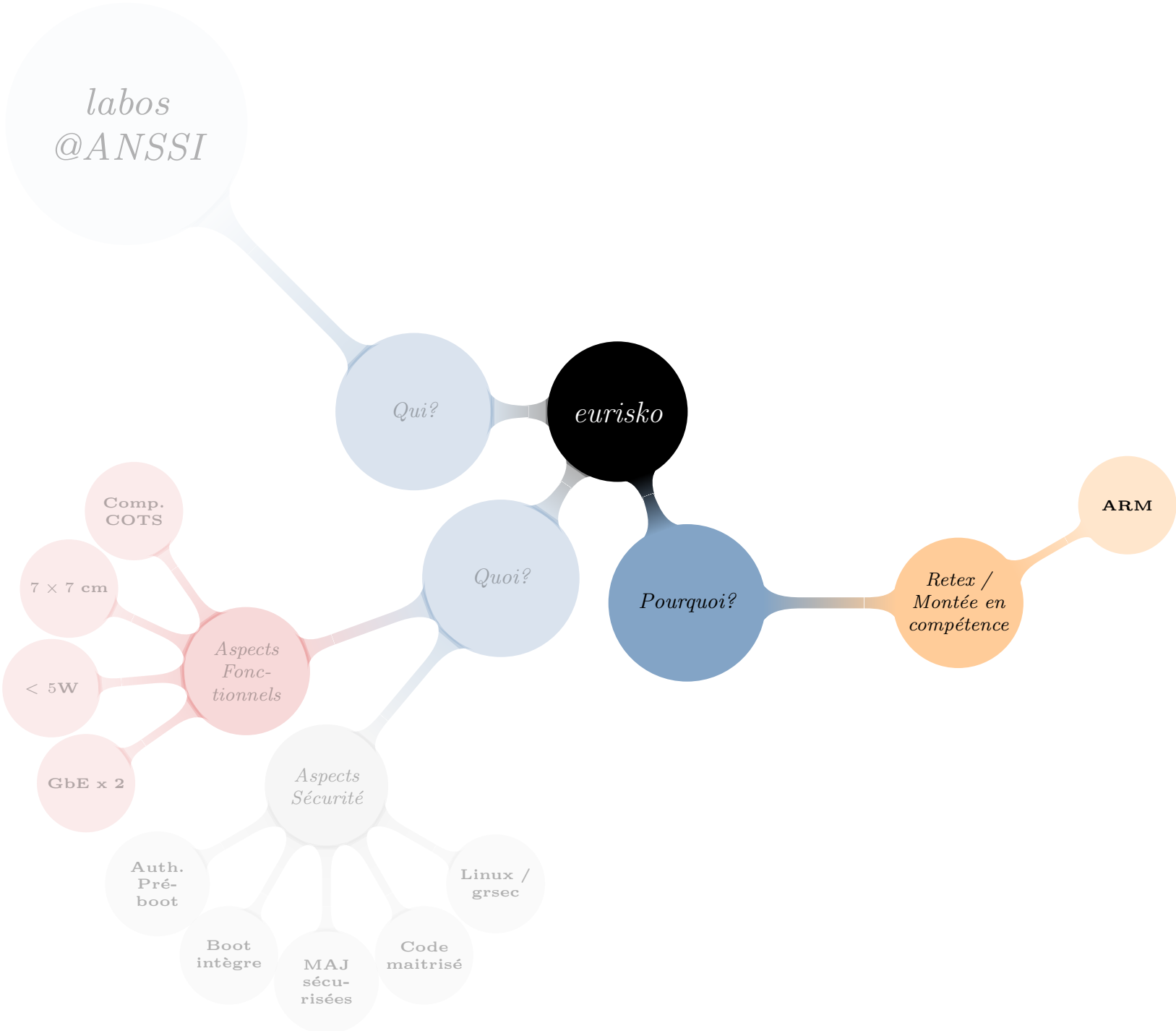

labos
@ANSSI
Qui?
eurisko
Quoi?
Comp.
COTS
7 × 7 cm
Aspects
Fonc-
tionnels
< 5W
GbE x 2
Aspects
Sécurité
Linux /
grsec
Code
maitrisé
MAJ
sécu-
risées

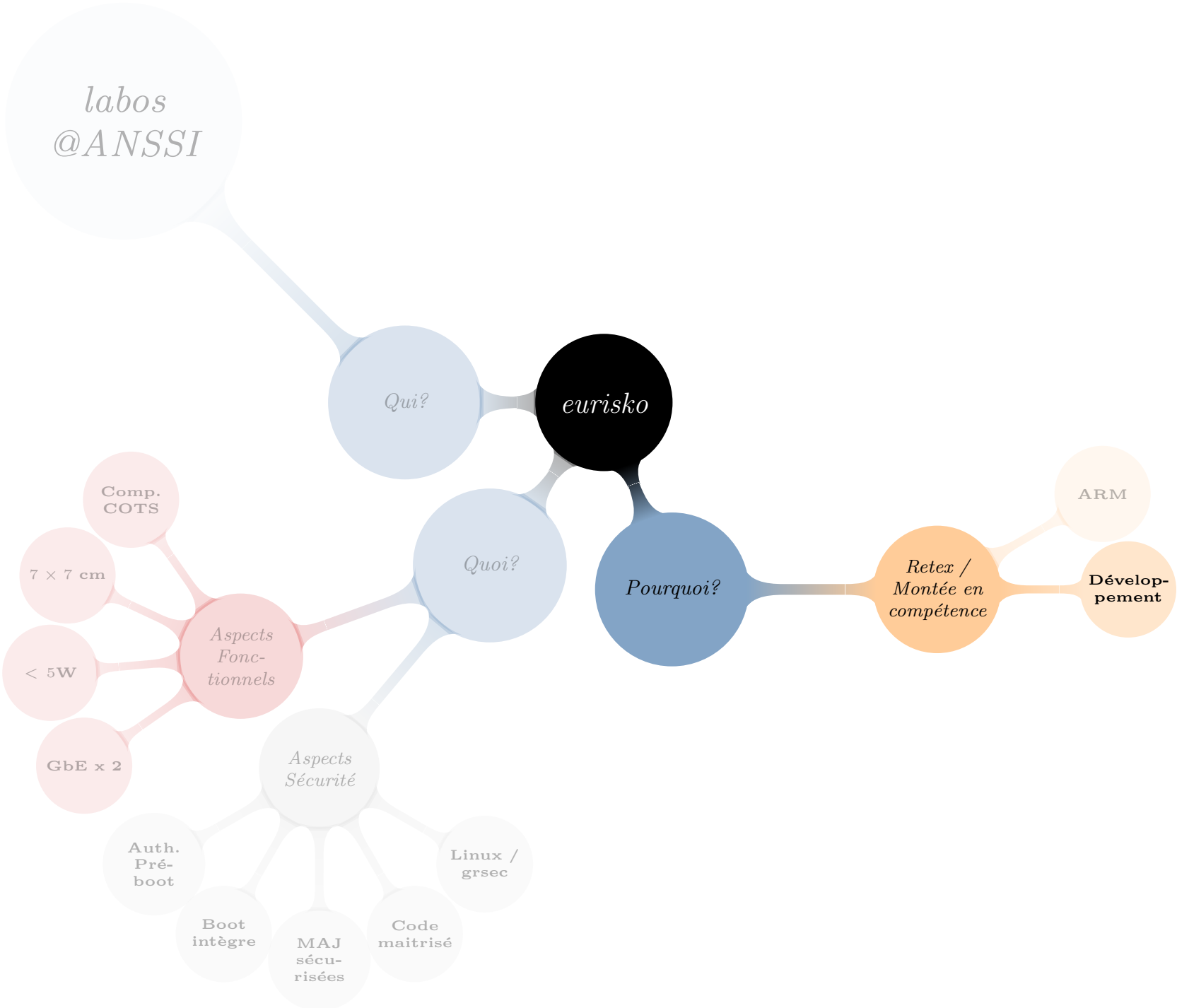

labos
@ANSSI
Qui?
eurisko
Quoi?
Comp.
COTS
7 × 7 cm
Aspects
Fonc-
tionnels
< 5W
GbE x 2
Aspects
Sécurité
Linux /
grsec
Boot
intègre
MAJ
sécu-
risées
Code
maitrisé

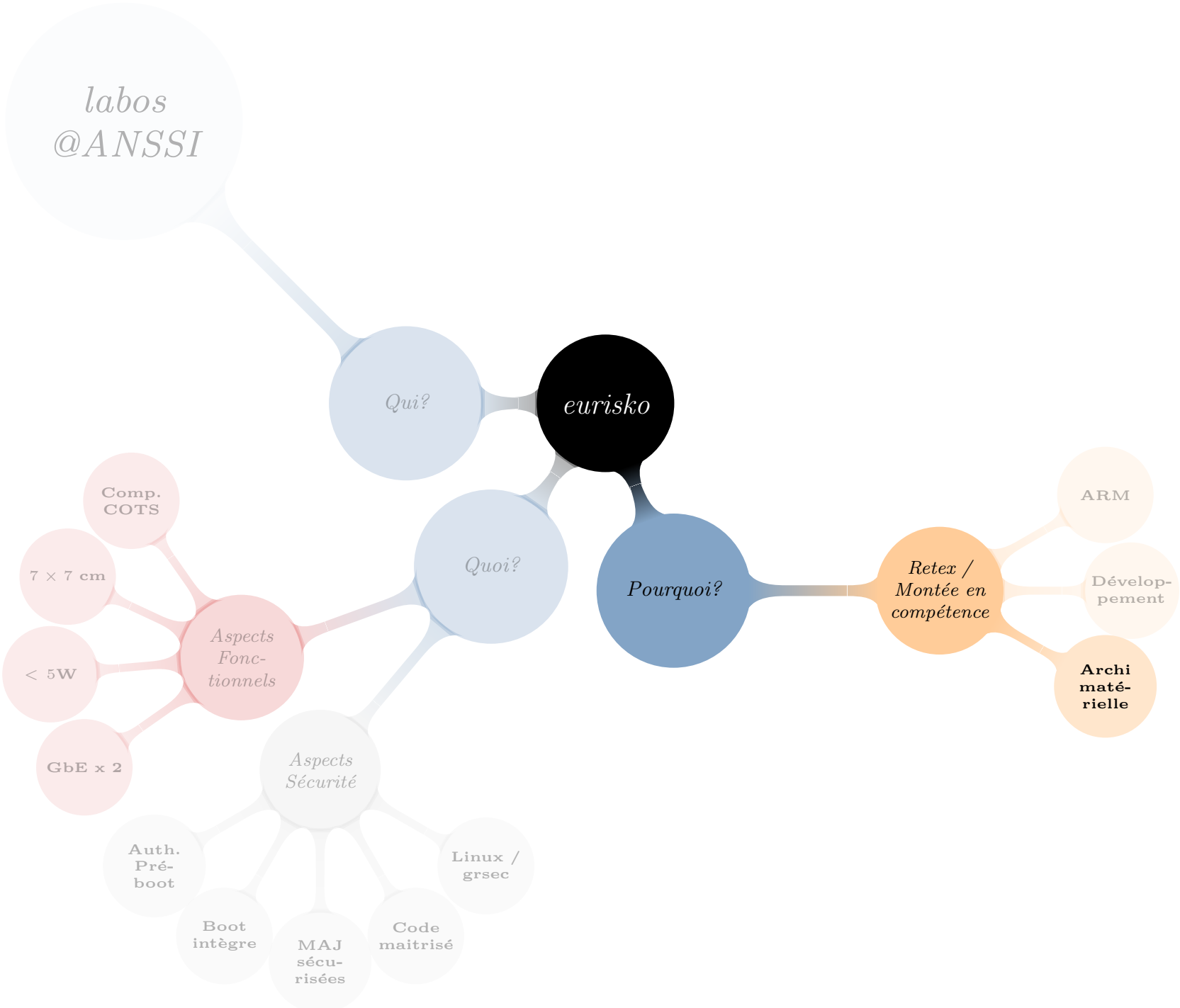

labos
@ANSSI
Qui?
eurisko
Quoi?
Comp.
COTS
7 × 7 cm
< 5W
GbE x 2
Aspects
Fonc-
tionnels
Aspects
Sécurité
Auth.
Pré-
boot
Boot
intègre
MAJ
sécu-
risées
Code
maitrisé
Linux /
grsec

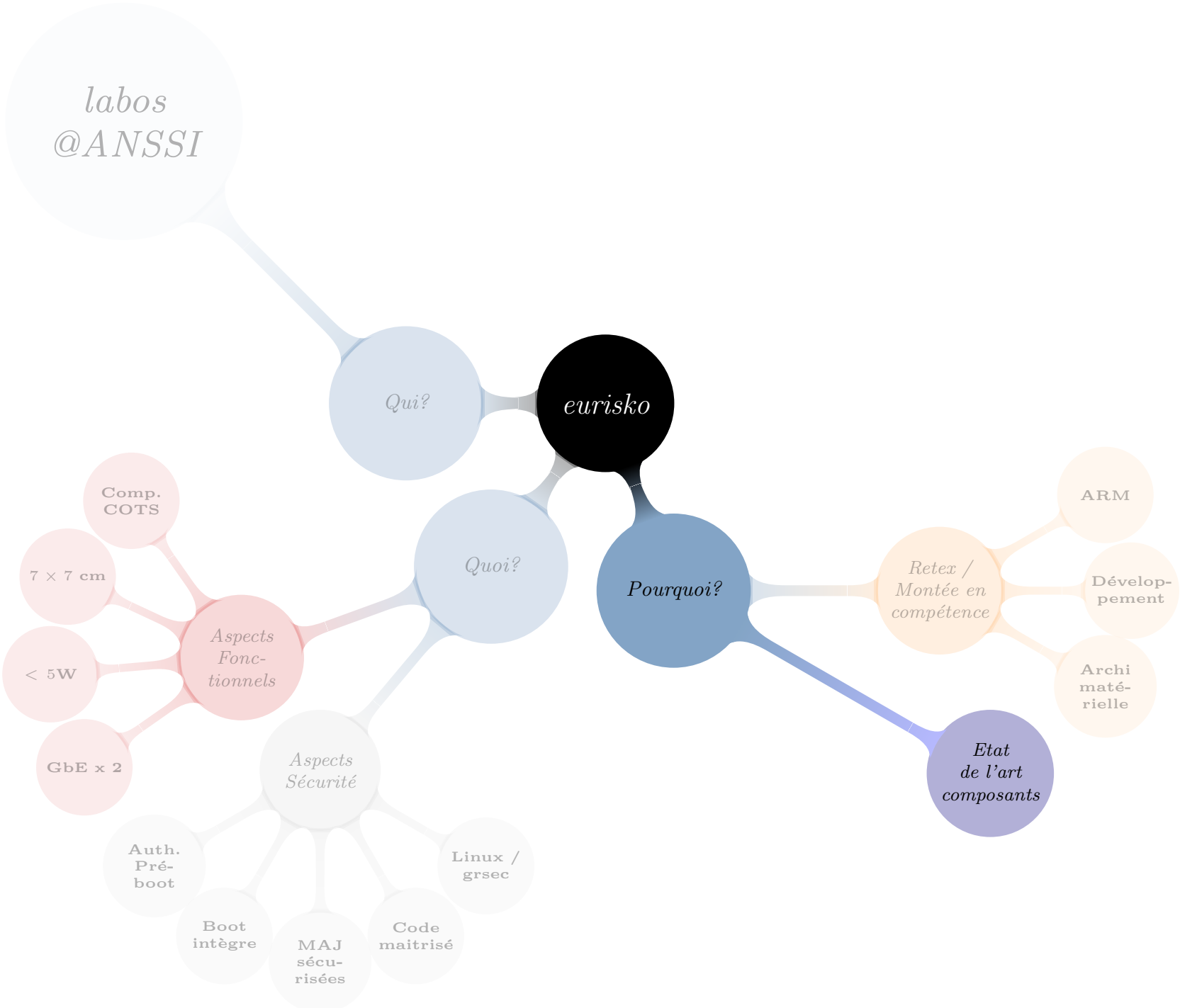

labos
@ANSSI
Qui?
eurisko
Quoi?
Pourquoi?
Comp.
COTS
7 × 7 cm
< 5W
GbE x 2
Aspects
Fonc-
tionnels
Aspects
Sécurité
Auth.
Pré-
boot
Boot
intègre
MAJ
sécu-
risées
Code
maitrisé
Linux /
grsec

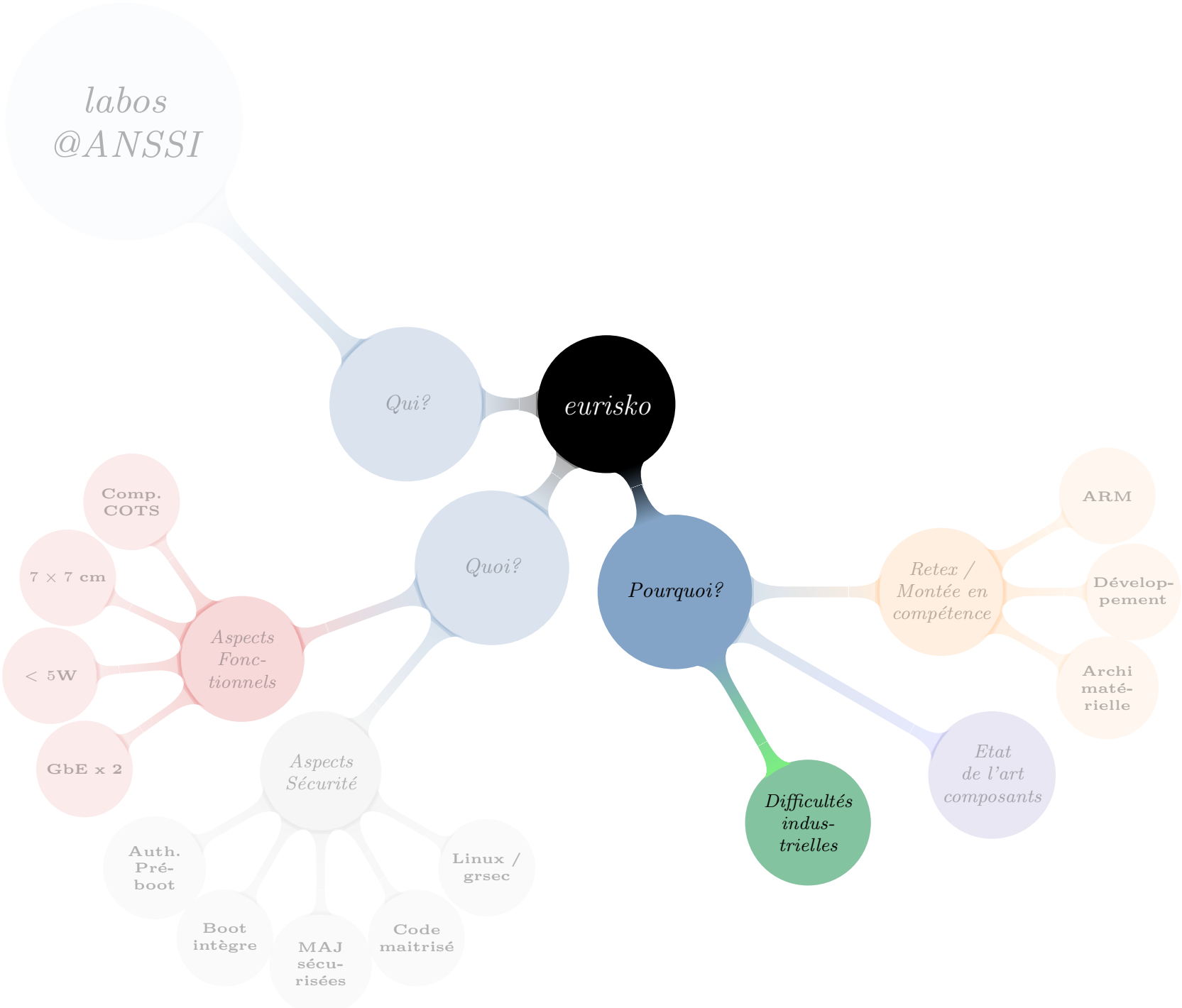

labos
@ANSSI
Qui?
eurisko
Quoi?
Pourquoi?
Retex /
Montée en
compétence
Comp.
COTS
7 × 7 cm
< 5W
GbE x 2
Aspects
Fonc-
tionnels
Aspects
Sécurité
Auth.
Pré-
boot
Boot
intègre
MAJ
sécu-
risées
Code
maitrisé
Linux /
grsec

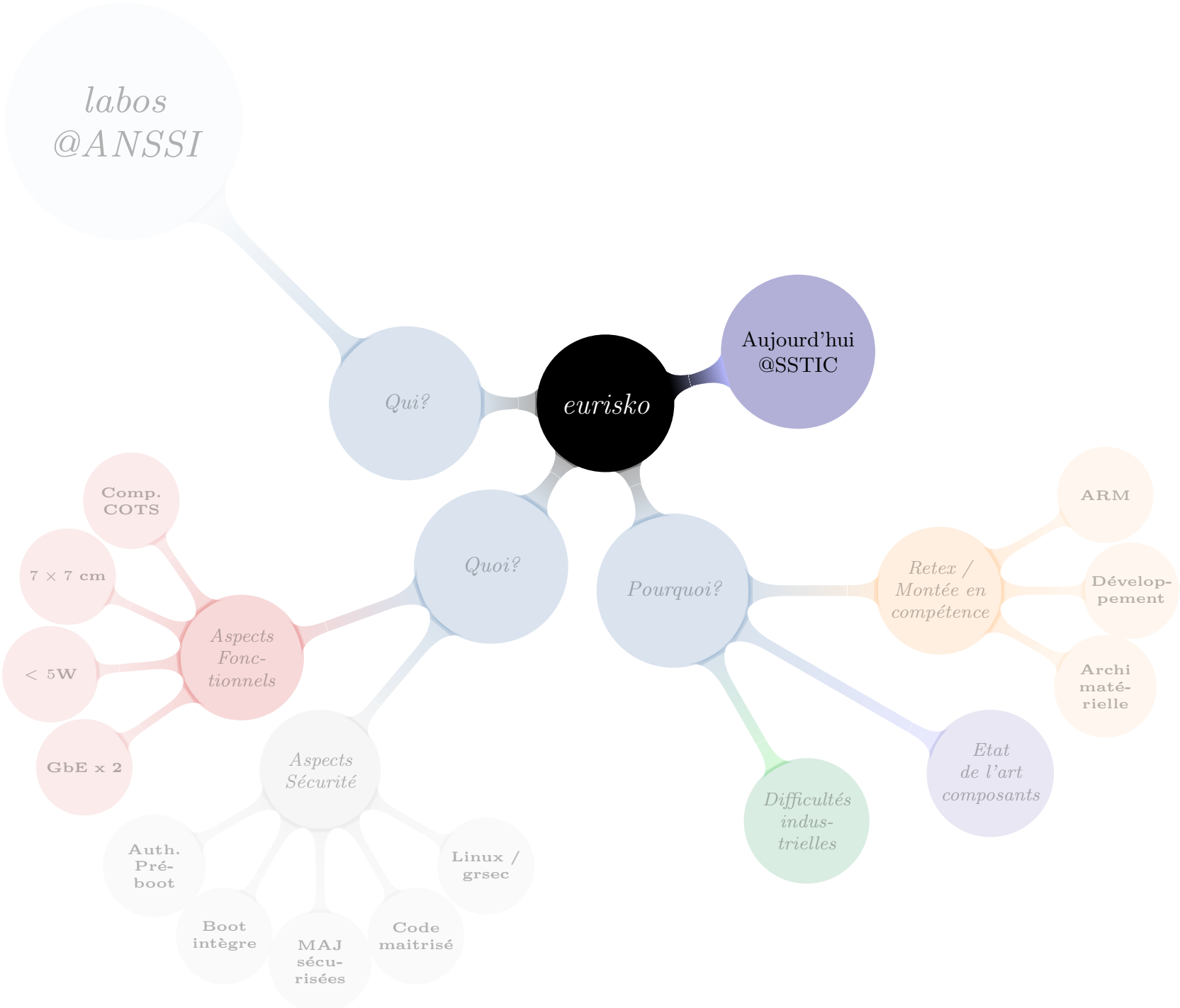

labos @ANSSI
Qui?
eurisko
Quoi?
Pourquoi?
Retex / Montée en compétence
ARM
Aspects Fonc-tionnels
Comp. COTS
7 × 7 cm
< 5W
GbE x 2
Aspects Sécurité
Auth. Pré-boot
Boot intègre
MAJ sécu-risées
Code maitrisé
Linux / grsec

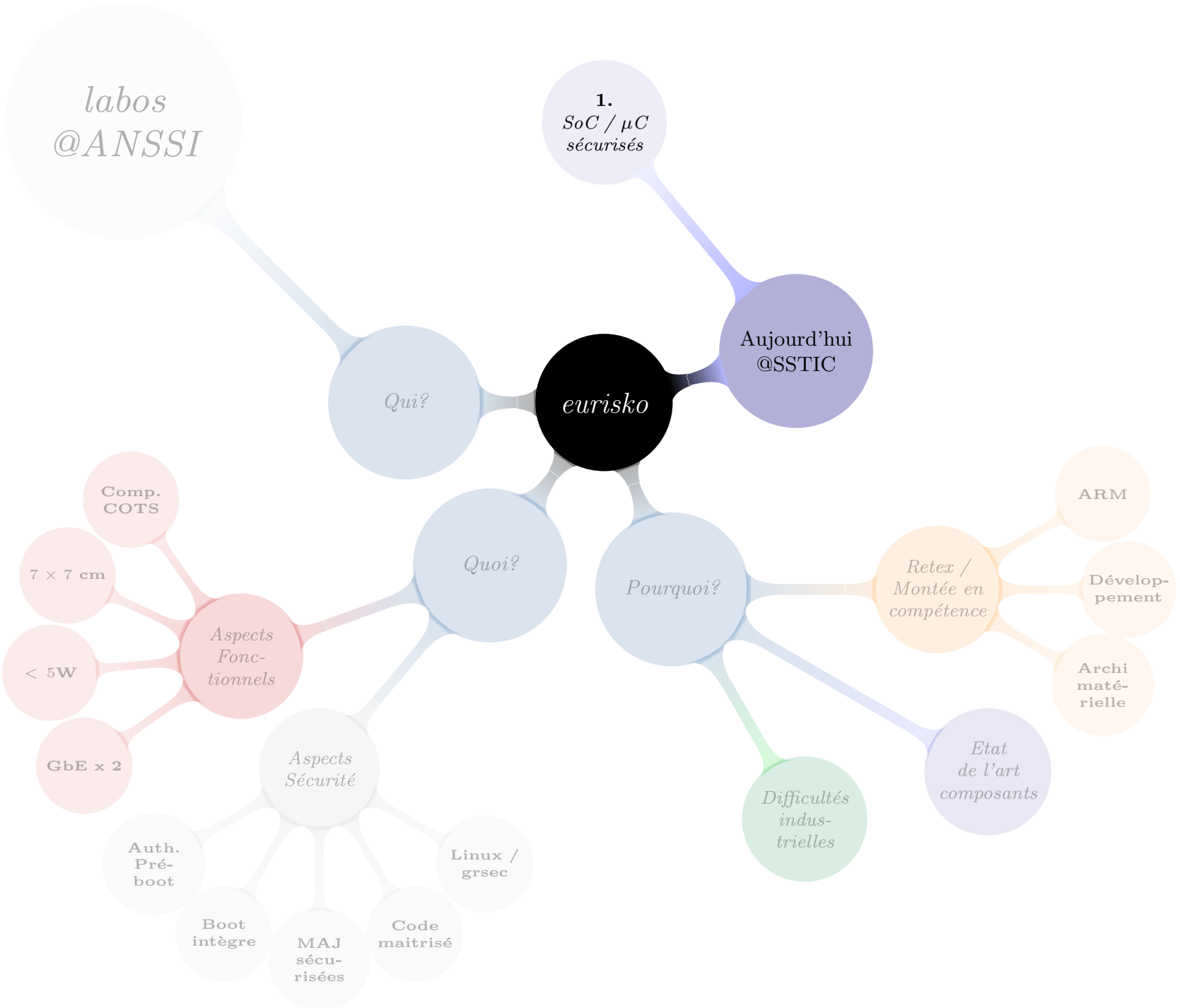

labos @ANSSI
Qui?
eurisko
Quoi?
Pourquoi?
Comp. COTS
7 × 7 cm
< 5W
GbE x 2
Aspects Fonc-tionnels
Aspects Sécurité
Auth. Pré-boot
Boot intègre
MAJ sécu-risées
Code maitrisé
Linux / grsec
Retex / Montée en compétence
ARM
Dévelop-pement

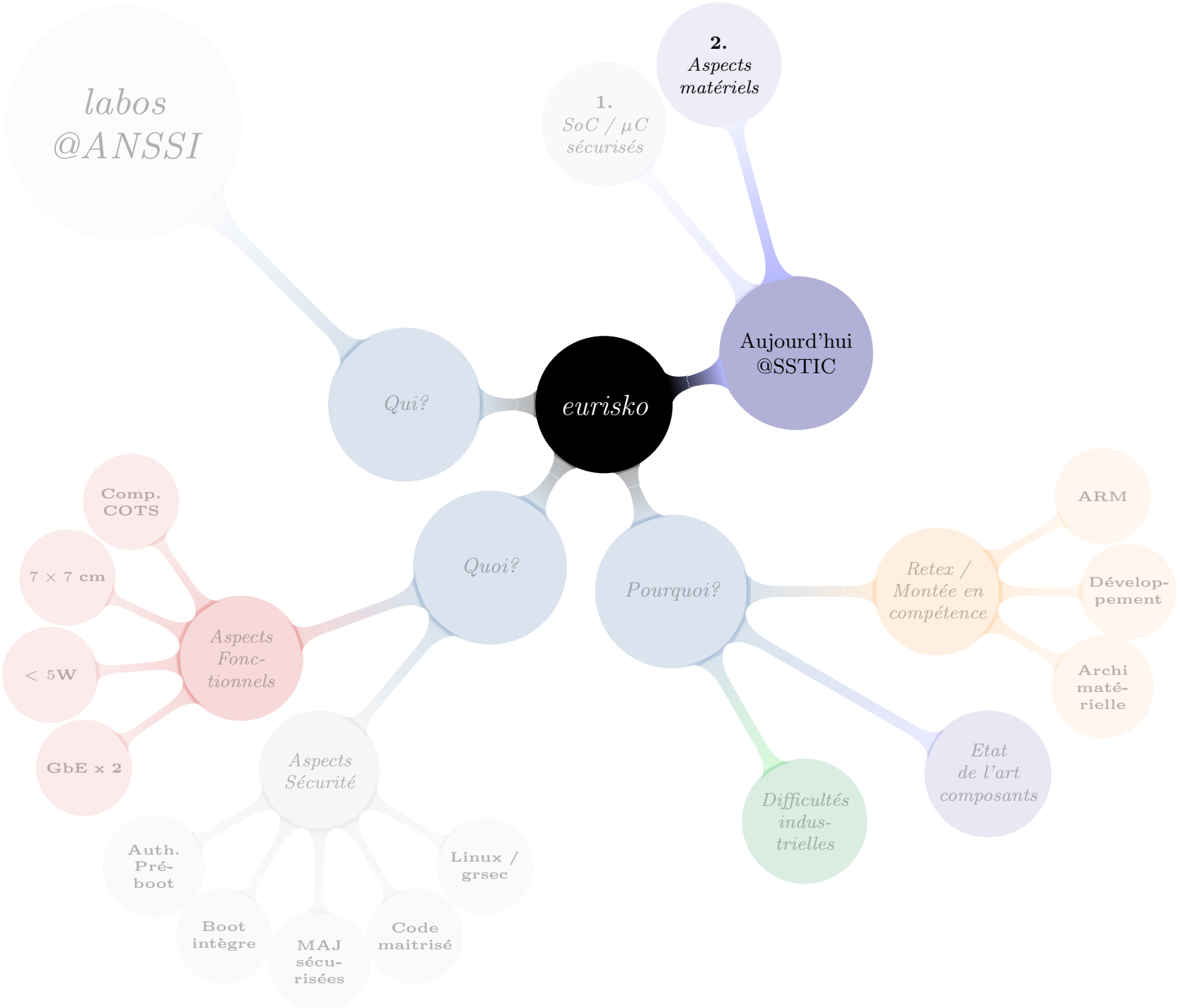

labos @ANSSI
Qui?
eurisko
Quoi?
Pourquoi?
Comp. COTS
7 × 7 cm
< 5W
GbE x 2
Aspects Fonc-tionnels
Aspects Sécurité
Auth. Pré-boot
Boot intègre
MAJ sécu-risées
Code maitrisé
Linux / grsec
Retex / Montée en compétence
ARM
Dévelop-pement
Archi maté-rielle

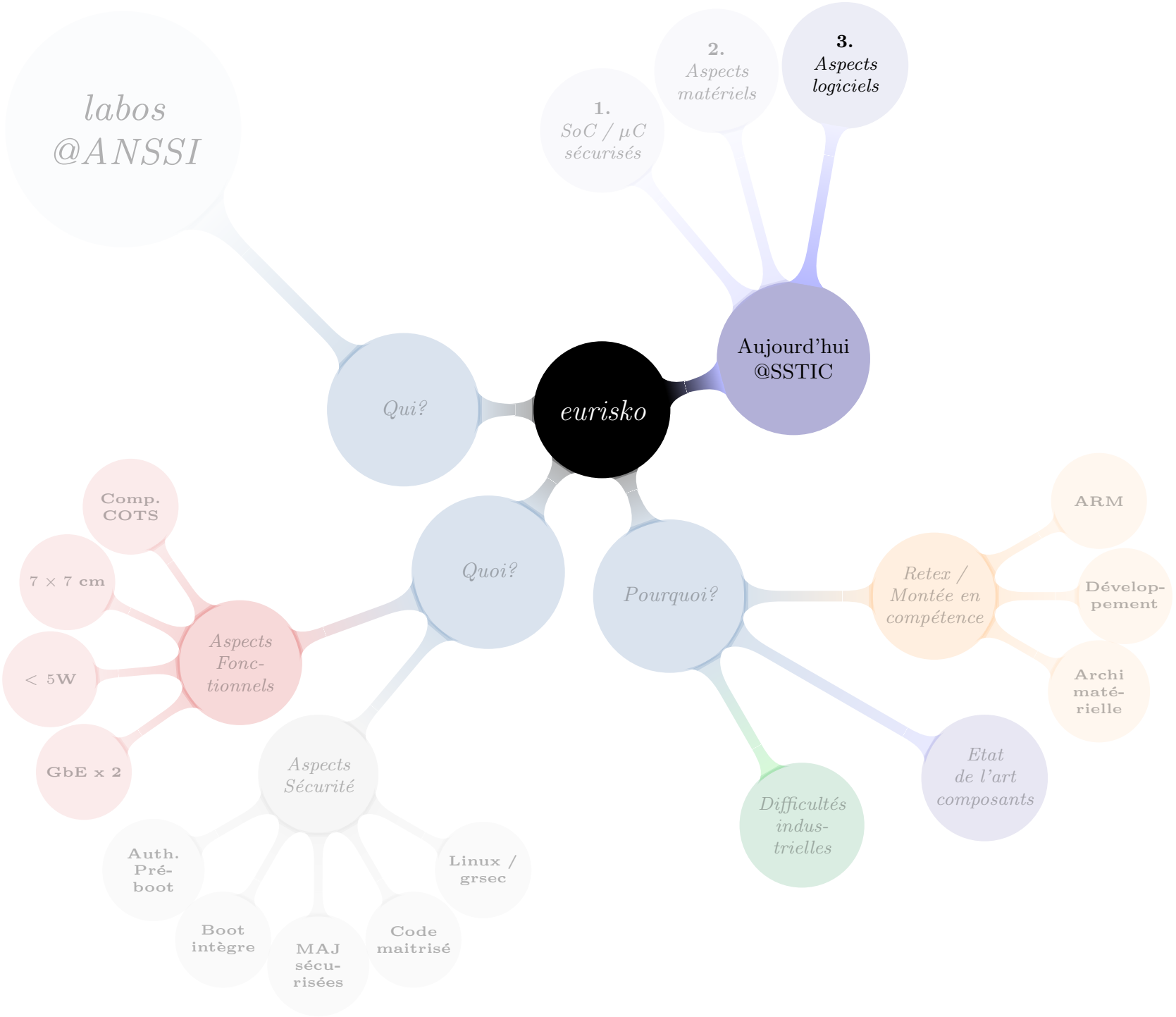

labos @ANSSI
Qui?
eurisko
Quoi?
Pourquoi?
Comp. COTS
7 × 7 cm
< 5W
GbE x 2
Aspects Fonc-tionnels
Aspects Sécurité
Auth. Pré-boot
Boot intègre
MAJ sécu-risées
Code maitrisé
Linux / grsec
Retex / Montée en compétence
ARM
Dévelop-pement
Archi maté-rielle
Etat de l'art composants

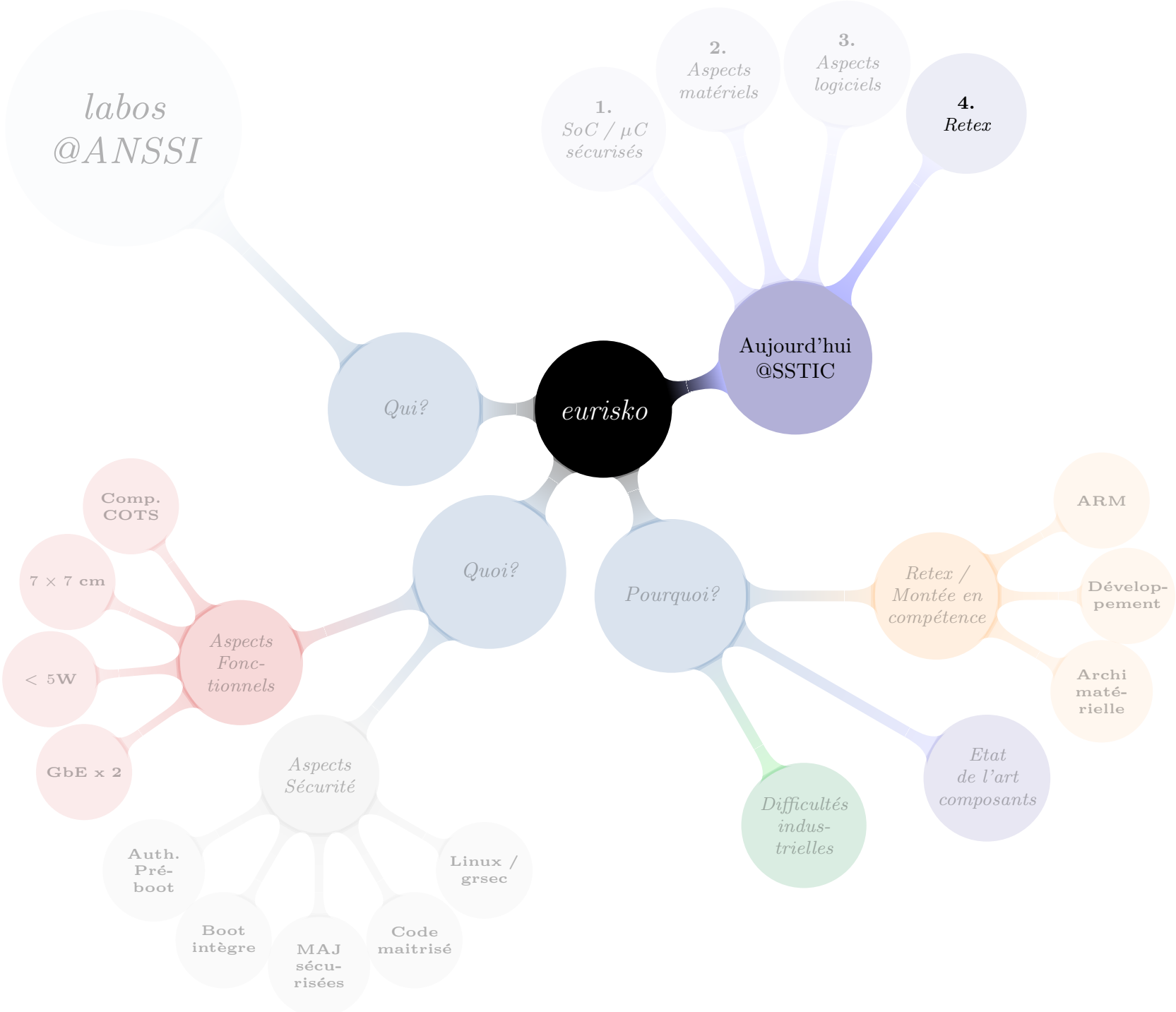

labos @ANSSI
Qui?
eurisko
Quoi?
Pourquoi?
Comp. COTS
7 × 7 cm
< 5W
GbE x 2
Aspects Fonc-tionnels
Aspects Sécurité
Auth. Pré-boot
Boot intègre
MAJ sécu-risées
Code maitrisé
Linux / grsec
Retex / Montée en compétence
ARM
Dévelop-pement
Archi maté-rielle
Etat de l'art composants
Difficultés indus-trielles

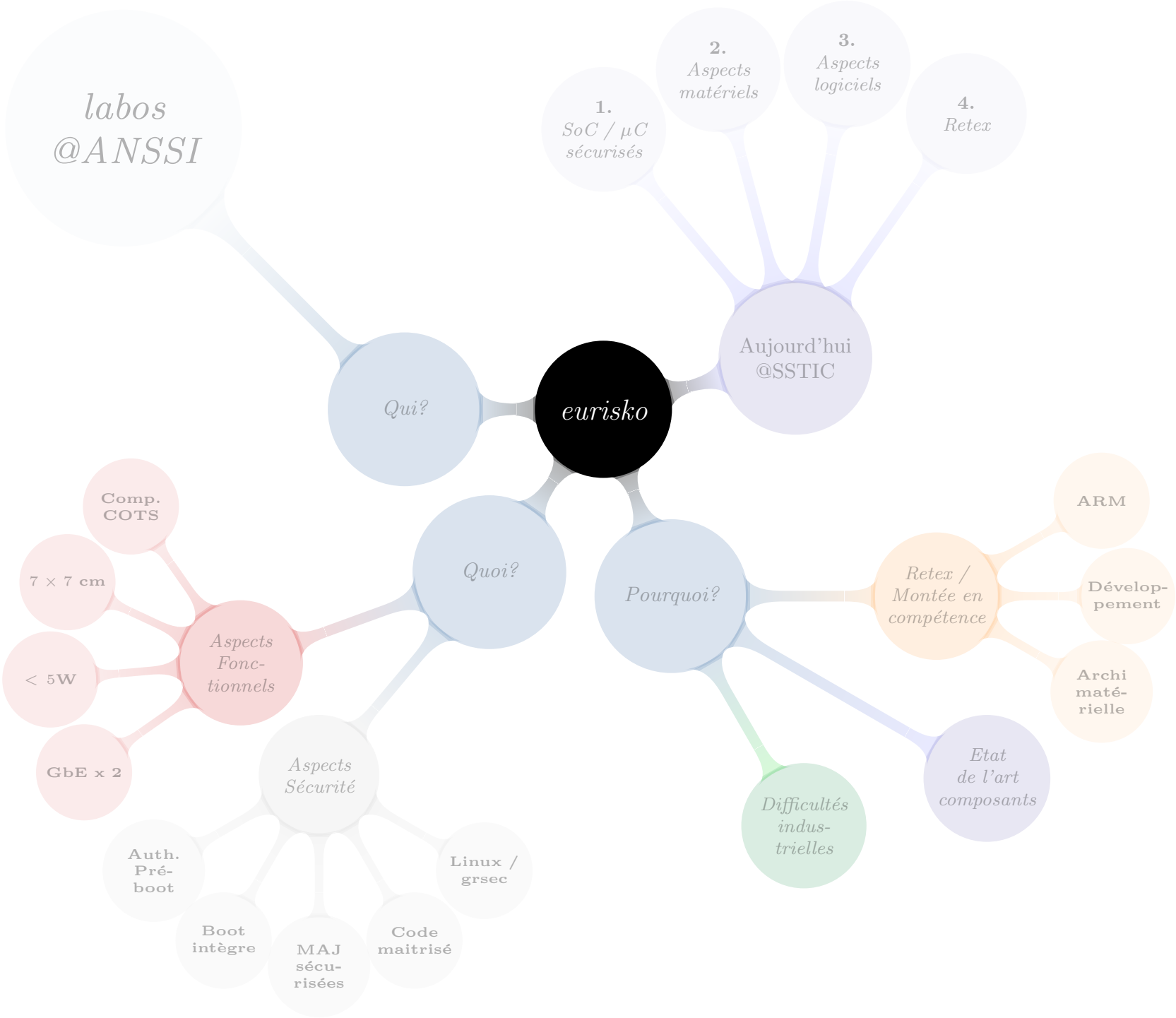

labos @ANSSI
Qui?
eurisko
Aujourd'hui @SSTIC
Quoi?
Pourquoi?
Comp. COTS
7 × 7 cm
< 5W
GbE x 2
Aspects Fonc-tionnels
Aspects Sécurité
Auth. Pré-boot
Boot intègre
MAJ sécu-risées
Code maitrisé
Linux / grsec
Retex / Montée en compétence
ARM
Dévelop-pement
Archi maté-rielle
Etat de l'art composants
Difficultés indus-trielles

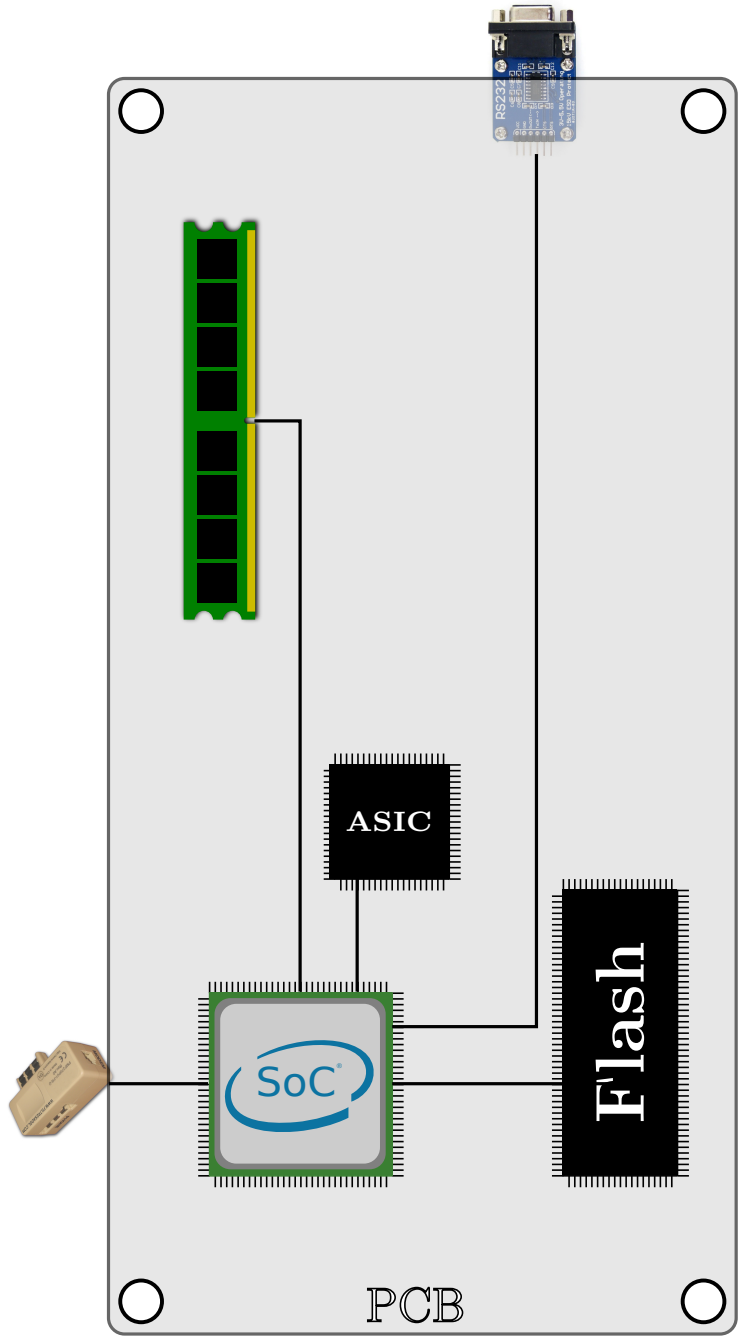

labos @ANSSI
1. SoC / µC sécurisés
Aujourd'hui @SSTIC
eurisko
Qui?
Quoi?
Pourquoi?
Comp. COTS
7 × 7 cm
< 5W
GbE x 2
Aspects Fonc-tionnels
Aspects Sécurité
Auth. Pré-boot
Boot intègre
MAJ sécu-risées
Code maitrisé
Linux / grsec
ARM
Dévelop-pement
Archi maté-rielle
Retex / Montée en compétence
Etat de l'art composants
Difficultés indus-trielles

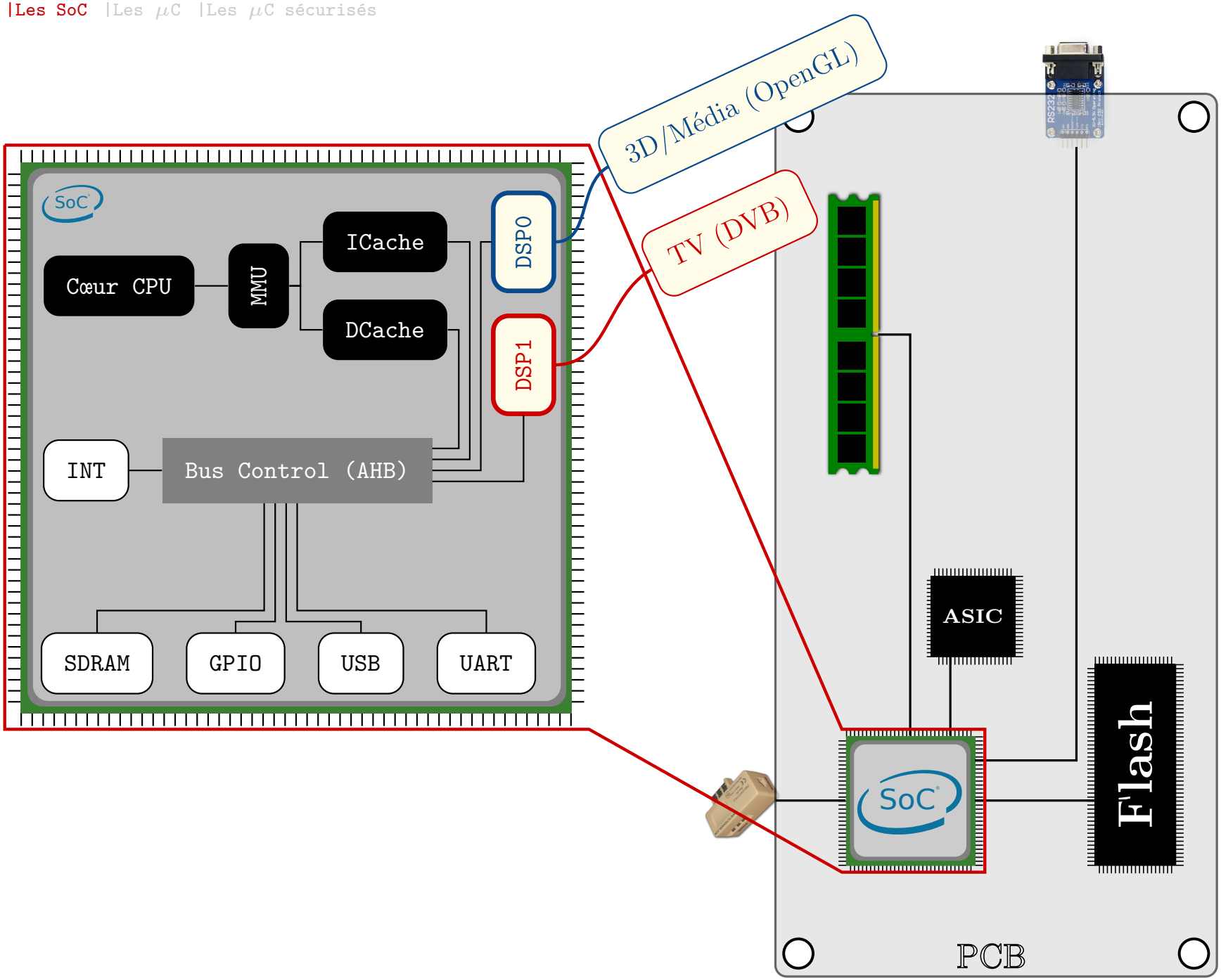

labos @ANSSI
1. SoC / µC sécurisés
2. Aspects matériels
Aujourd'hui @SSTIC
Qui?
eurisko
Quoi?
Pourquoi?
Comp. COTS
7 × 7 cm
< 5W
GbE x 2
Aspects Fonc-tionnels
Aspects Sécurité
Auth. Pré-boot
Boot intègre
MAJ sécu-risées
Code maitrisé
Linux / grsec
ARM
Dévelop-pement
Archi maté-rielle
Retex / Montée en compétence
Etat de l'art composants
Difficultés indus-trielles


labos @ANSSI
1. SoC / µC sécurisés
2. Aspects matériels
3. Aspects logiciels
Aujourd'hui @SSTIC
eurisko
Qui?
Quoi?
Pourquoi?
Comp. COTS
7 × 7 cm
< 5W
GbE x 2
Aspects Fonc-tionnels
Aspects Sécurité
Auth. Pré-boot
Boot intègre
MAJ sécu-risées
Code maitrisé
Linux / grsec
Retex / Montée en compétence
ARM
Dévelop-pement
Archi maté-rielle
Etat de l'art composants
Difficultés indus-trielles

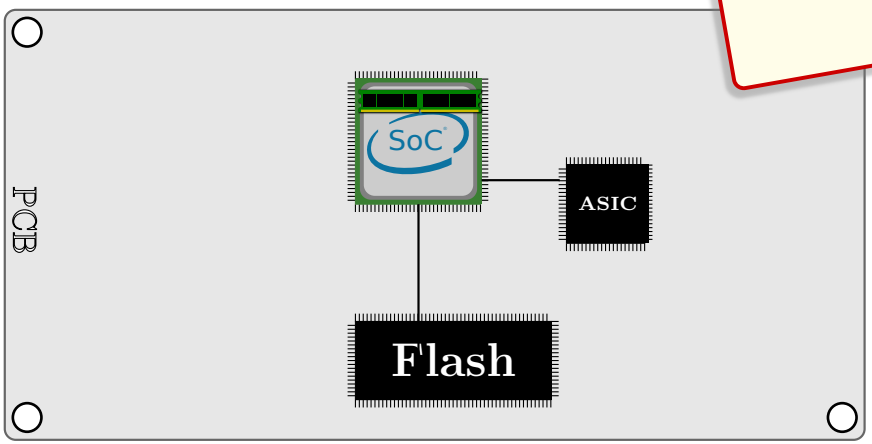

labos @ANSSI
Qui?
eurisko
Aujourd'hui @SSTIC
1. SoC / µC sécurisés
2. Aspects matériels
3. Aspects logiciels
4. Retex
Quoi?
Aspects Fonc-tionnels
Comp. COTS
7 × 7 cm
< 5W
GbE x 2
Aspects Sécurité
Auth. Pré-boot
Boot intègre
MAJ sécu-risées
Code maitrisé
Linux / grsec
Pourquoi?
Retex / Montée en compétence
ARM
Dévelop-pement
Archi maté-rielle
Etat de l'art composants
Difficultés indus-trielles

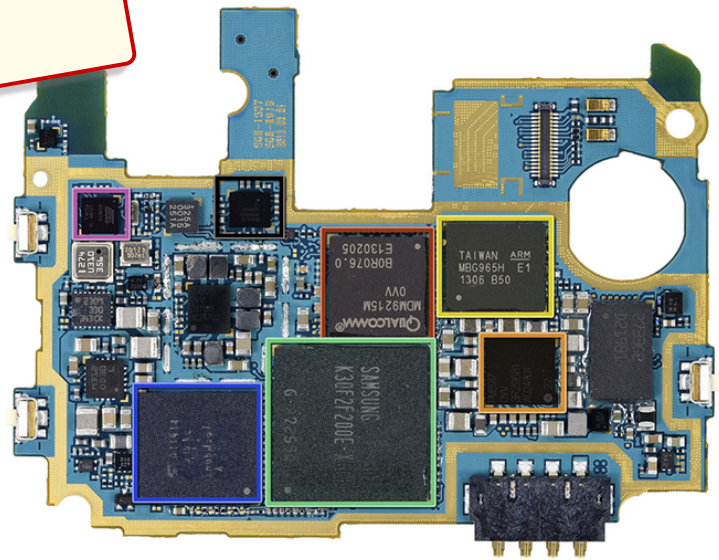

labos @ANSSI
Qui?
eurisko
Aujourd'hui @SSTIC
1. SoC / µC sécurisés
2. Aspects matériels
3. Aspects logiciels
4. Retex
Quoi?
Aspects Fonc-tionnels
Comp. COTS
7 × 7 cm
< 5W
GbE x 2
Aspects Sécurité
Auth. Pré-boot
Boot intègre
MAJ sécu-risées
Code maitrisé
Linux / grsec
Pourquoi?
Retex / Montée en compétence
ARM
Dévelop-pement
Archi maté-rielle
Etat de l'art composants
Difficultés indus-trielles

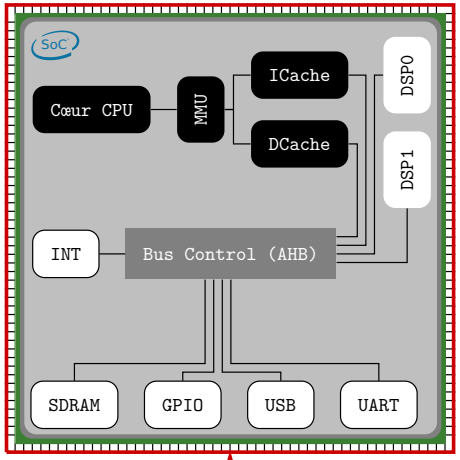

ASIC
SoC
Flash
PCB


SoC
Cœur CPU
MMU
ICache
DCache
DSP0
DSP1
INT
Bus Control (AHB)
SDRAM
GPIO
USB
UART
3D/Média (OpenGL)
TV (DVB)
ASIC
SoC
Flash
PCB

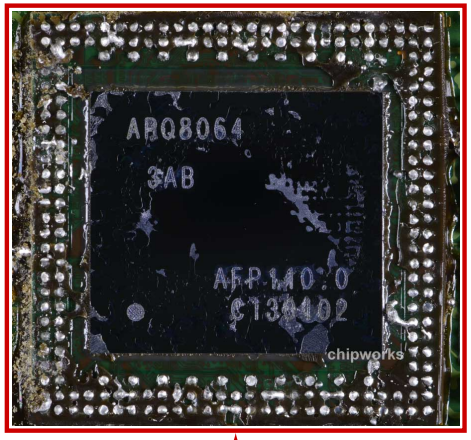
OEM
Samsung
Galaxy S4



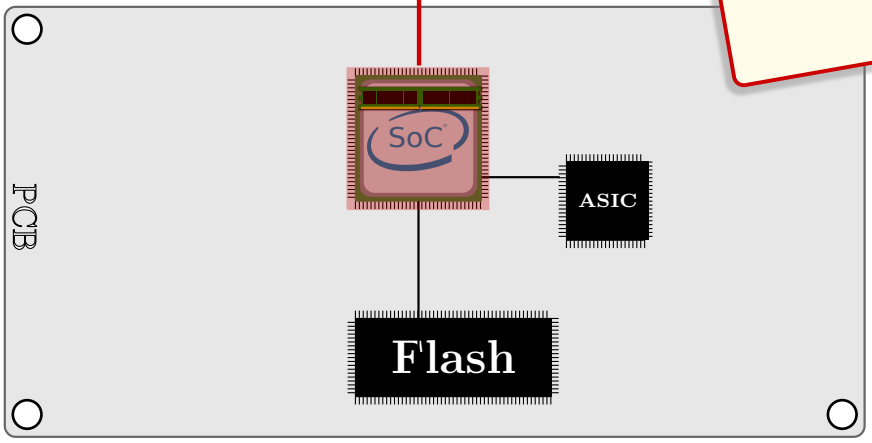


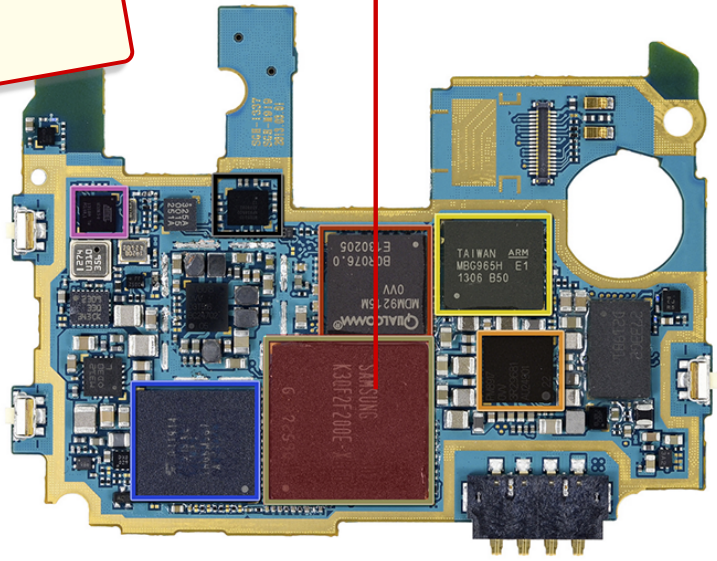


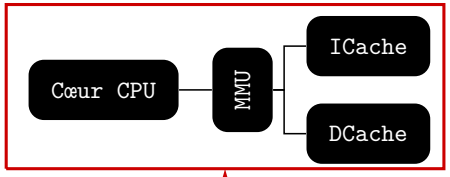
Fabriquant SoC
Qualcomm
Snapdragon 600



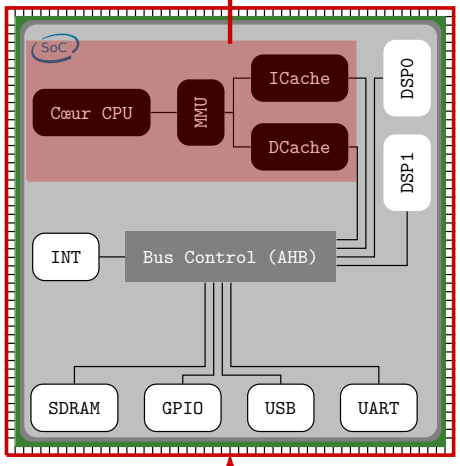
OEM
Samsung
Galaxy S4



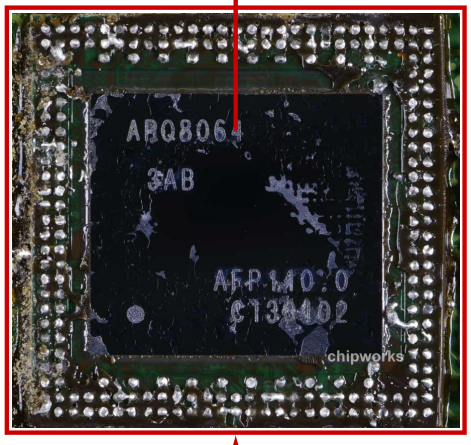




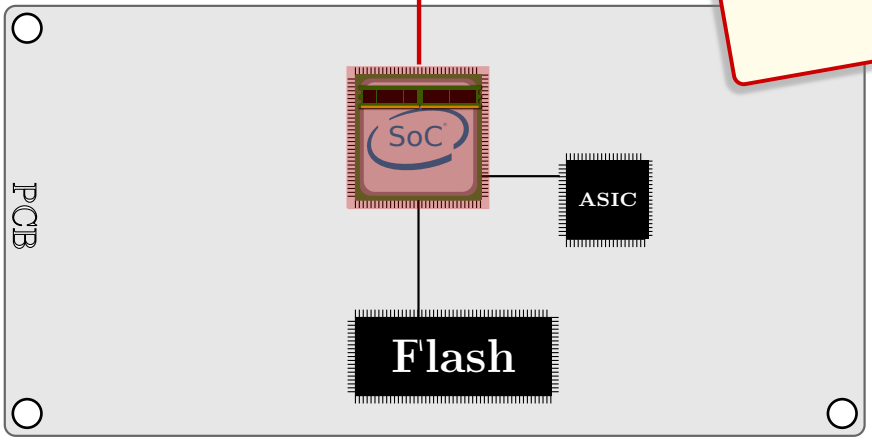
IP Cœur
ARM/Qualcomm
Krait 300

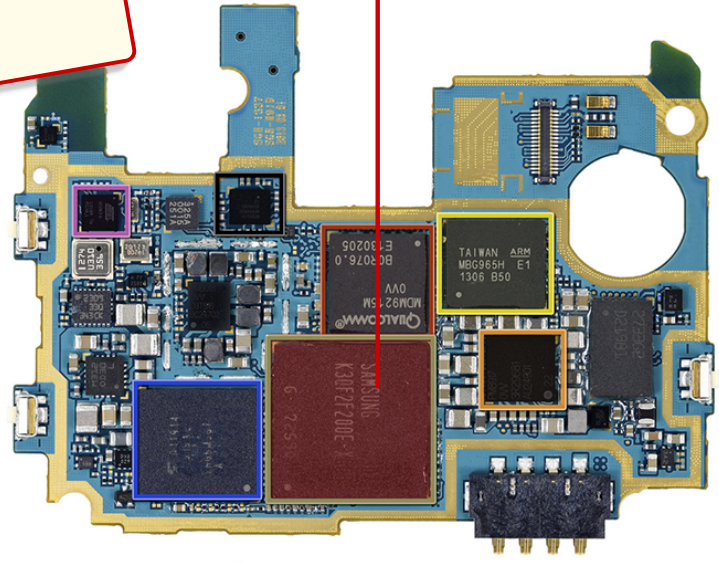


Fabriquant SoC
Qualcomm
Snapdragon 600

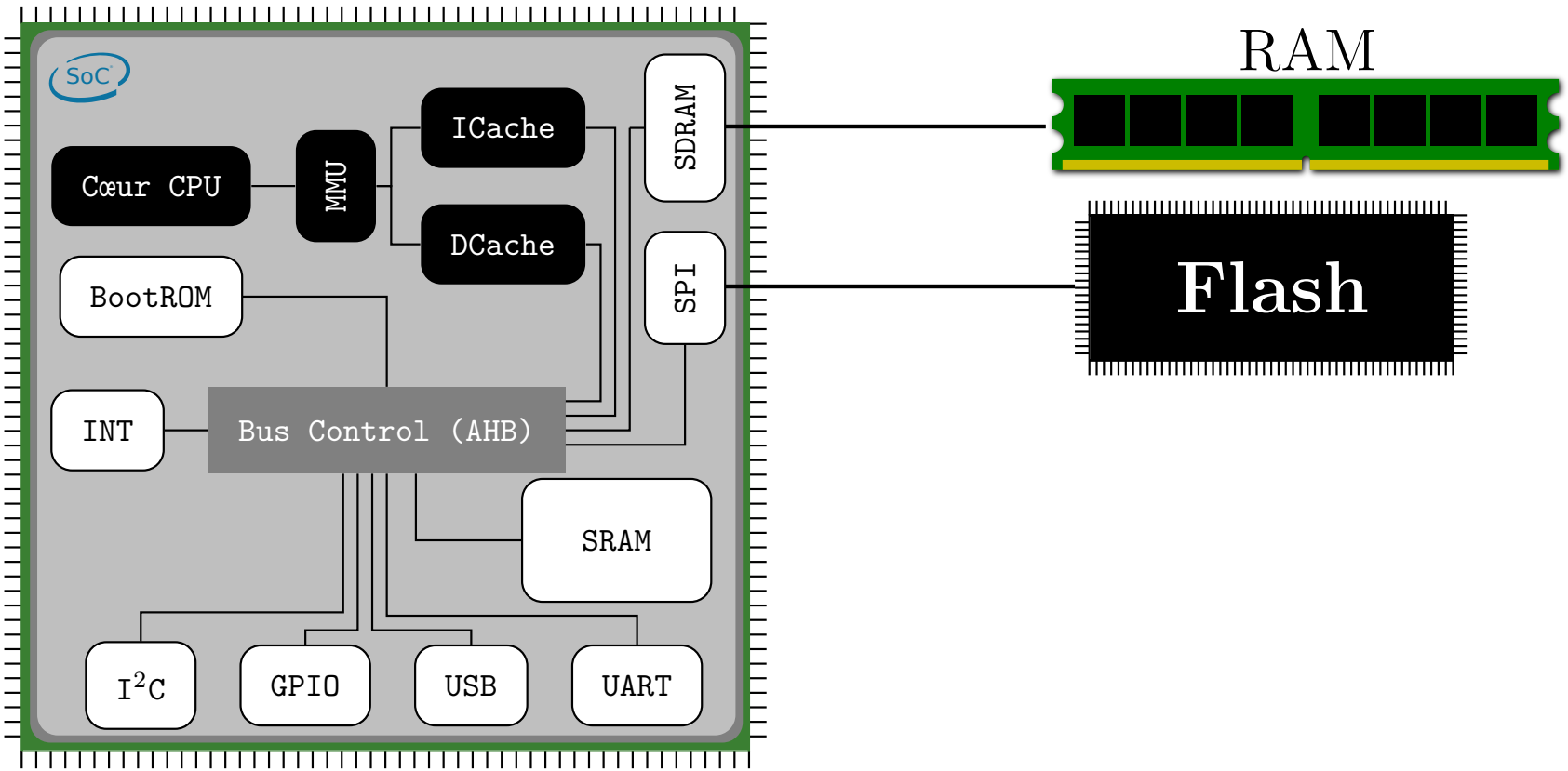


OEM
Samsung
Galaxy S4

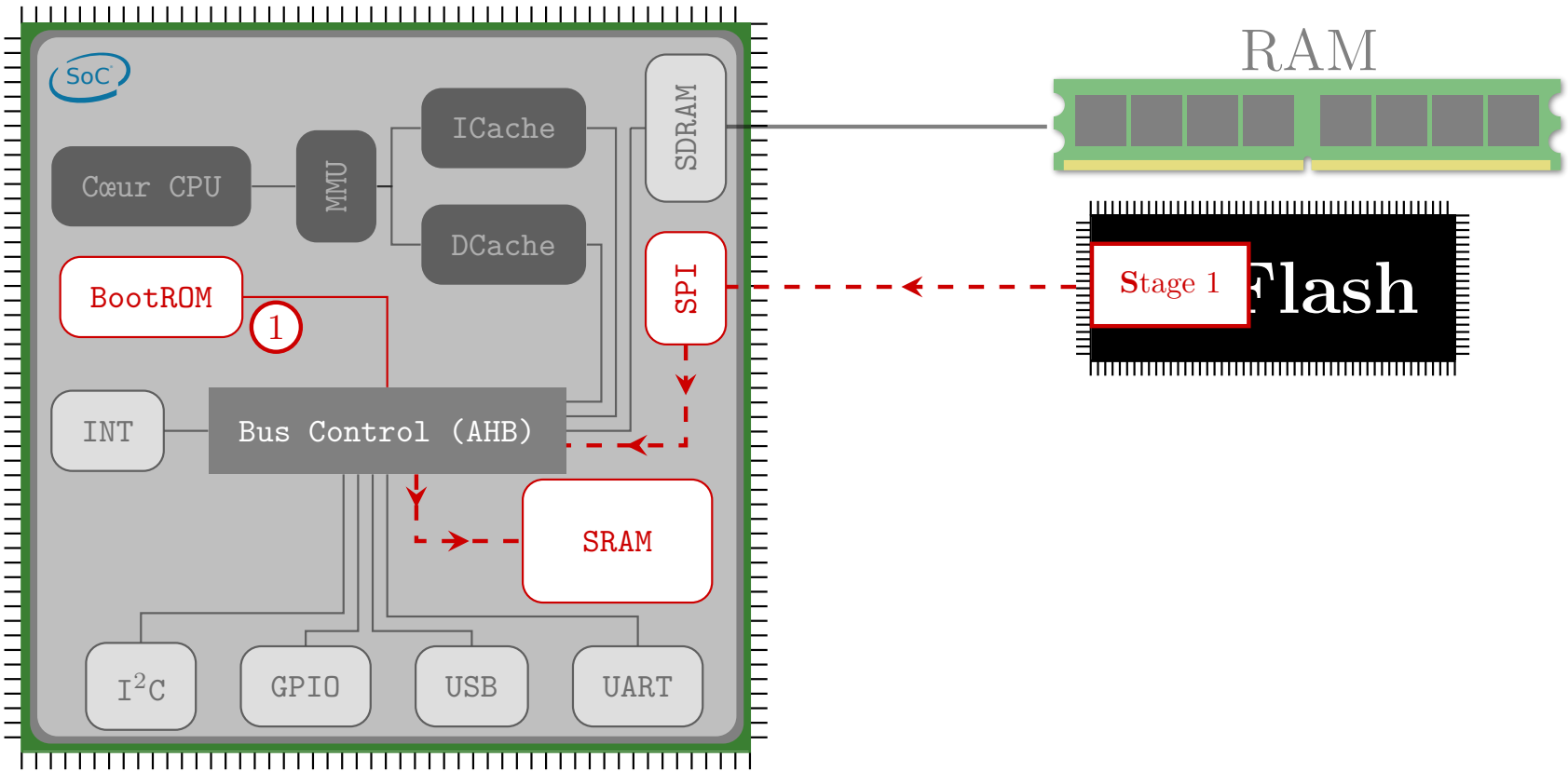




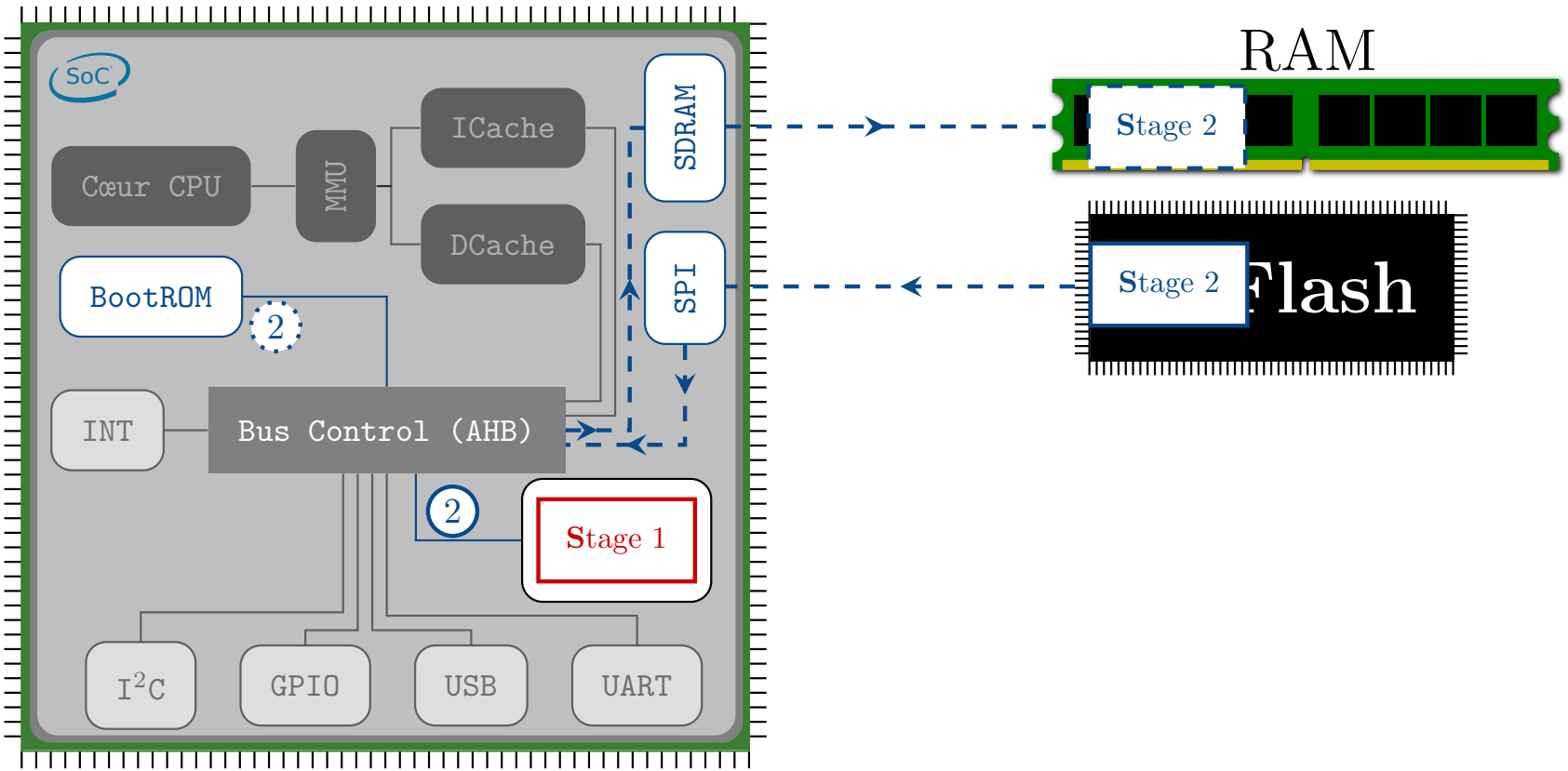
Chaîne de démarrage des SoC



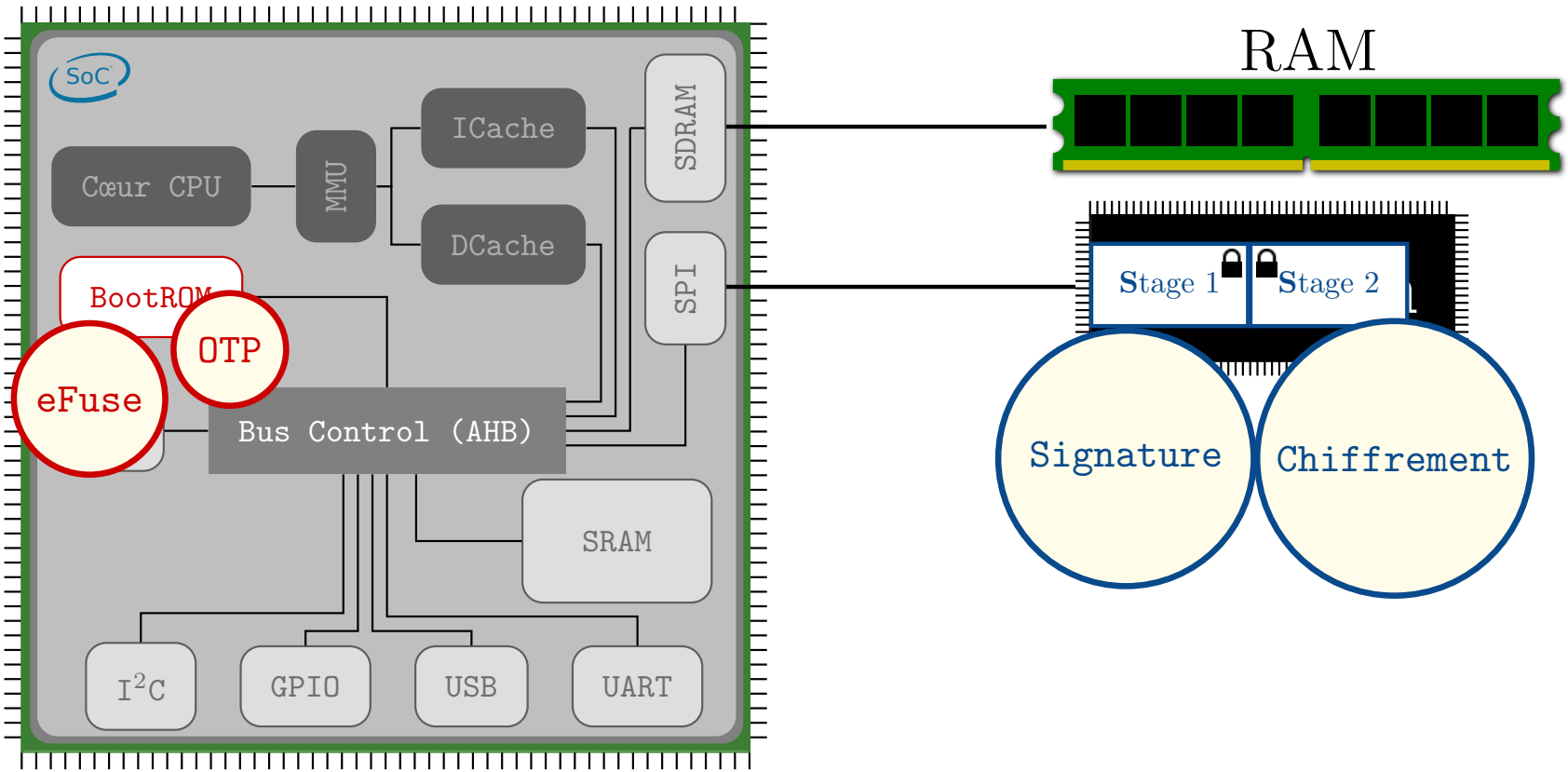
Chaîne de démarrage des SoC



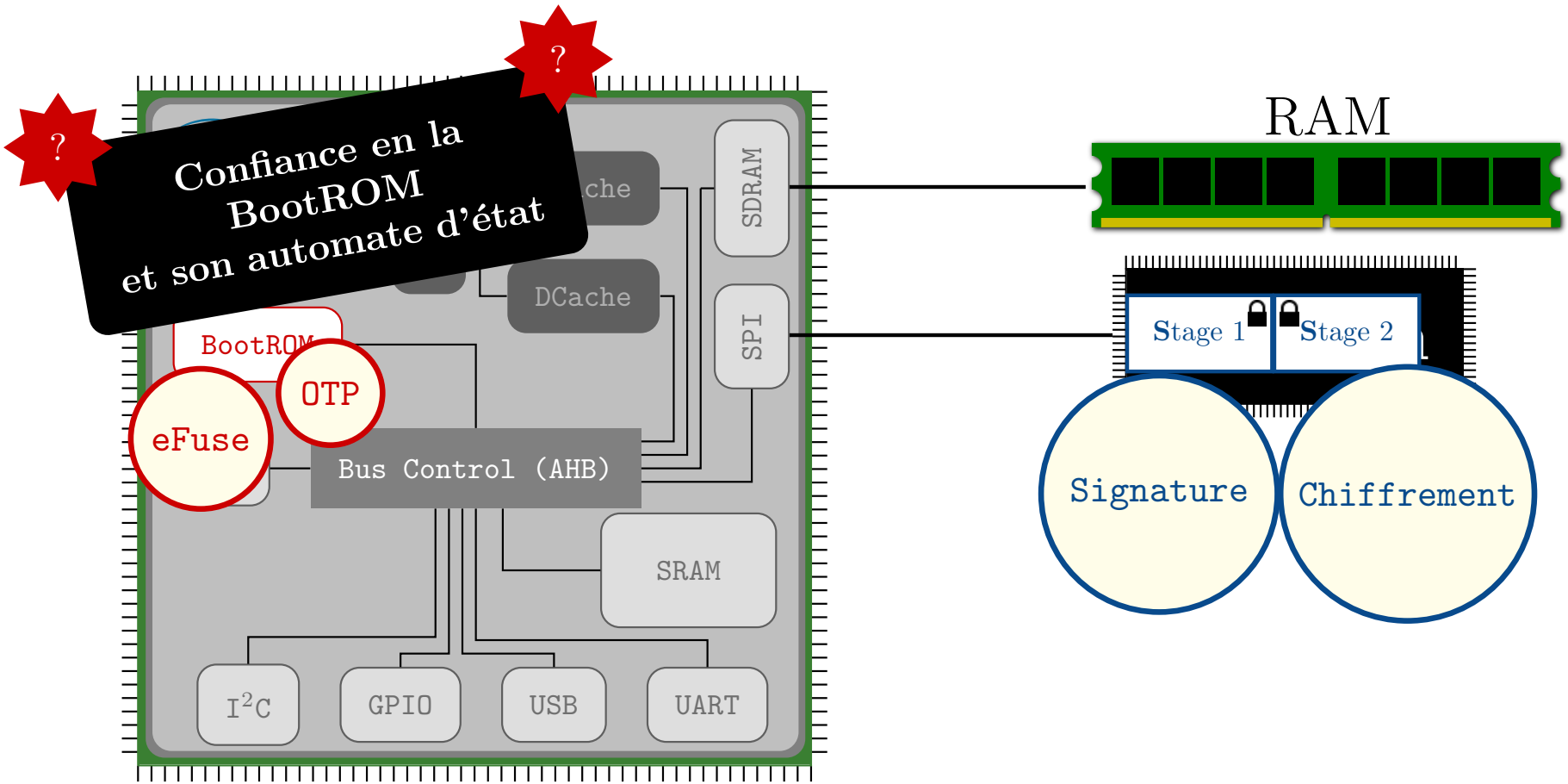
Chaîne de démarrage des SoC



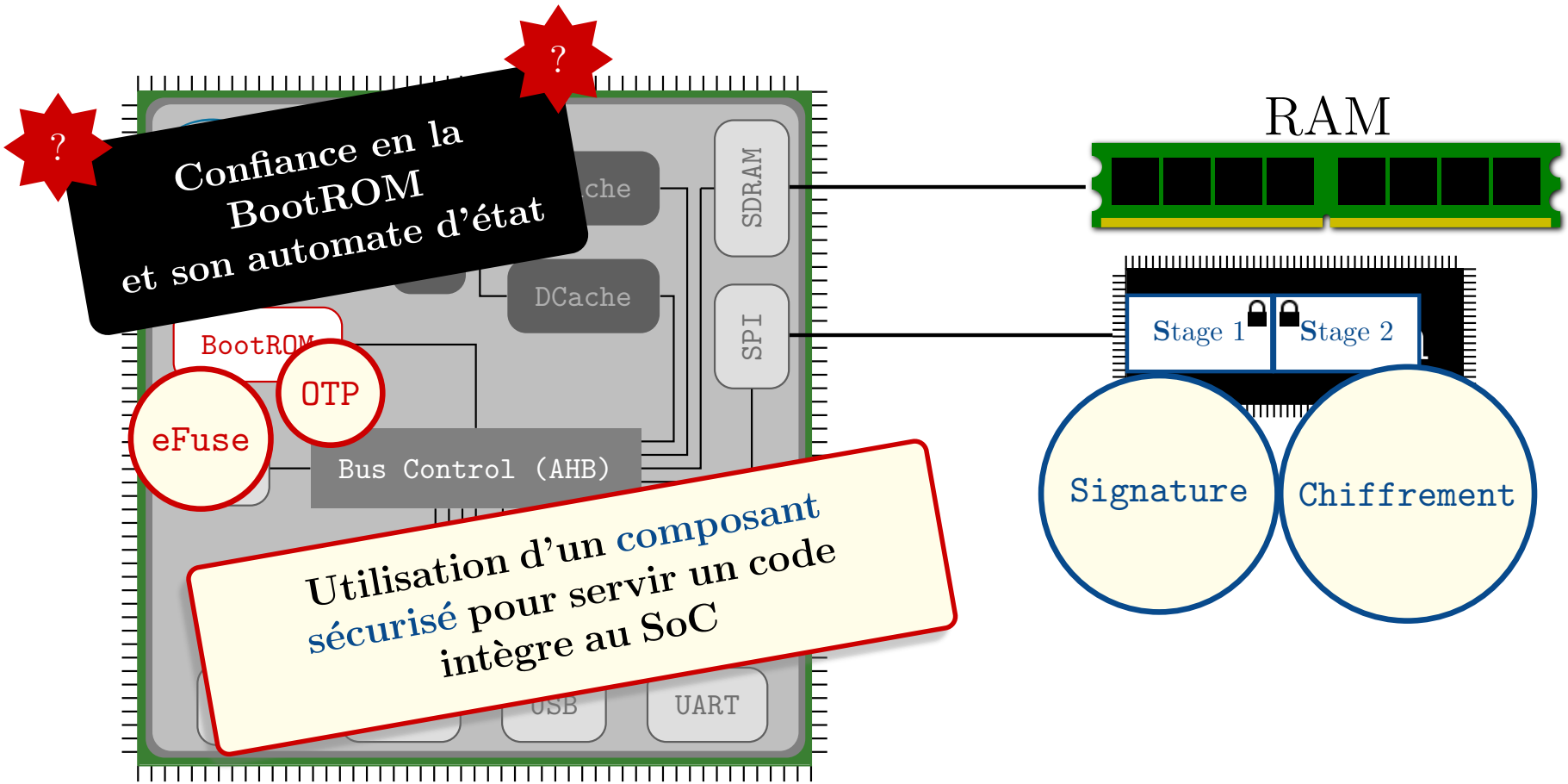
Chaîne de démarrage des SoC

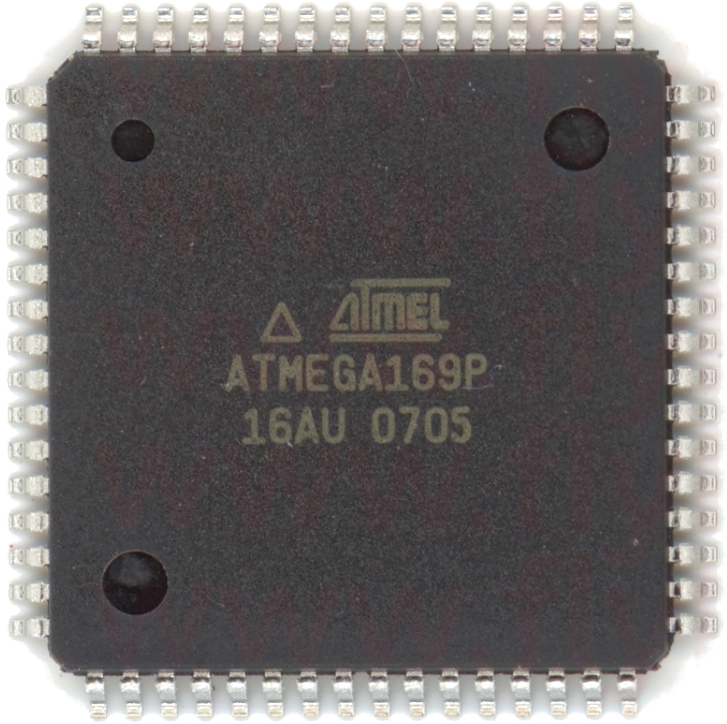


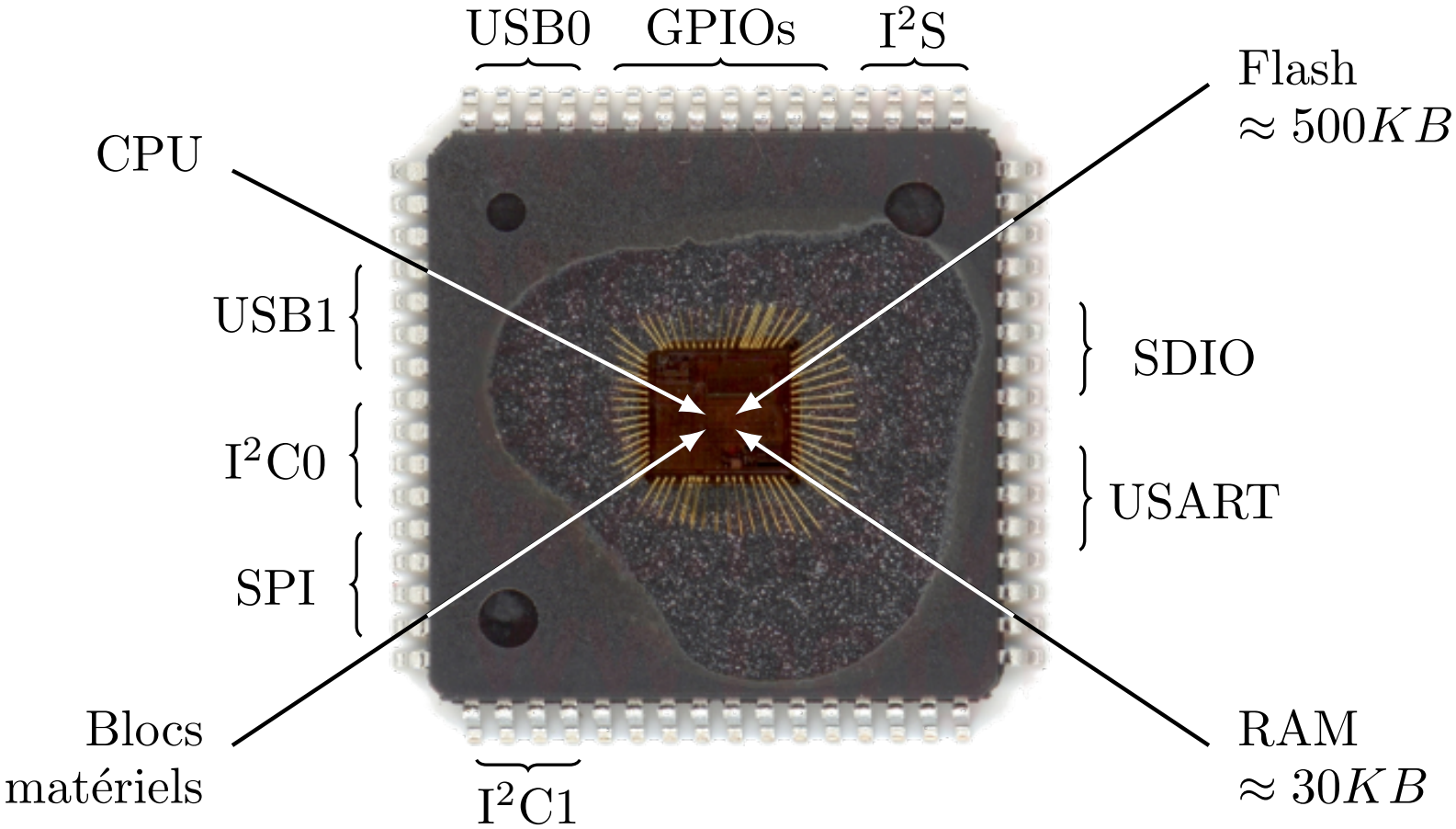
Chaîne de démarrage des SoC

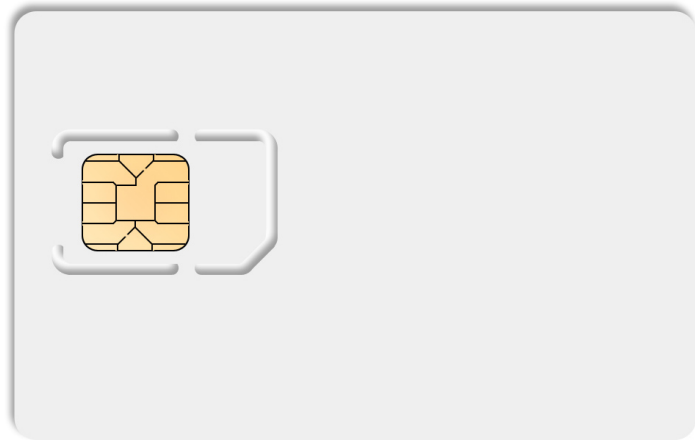


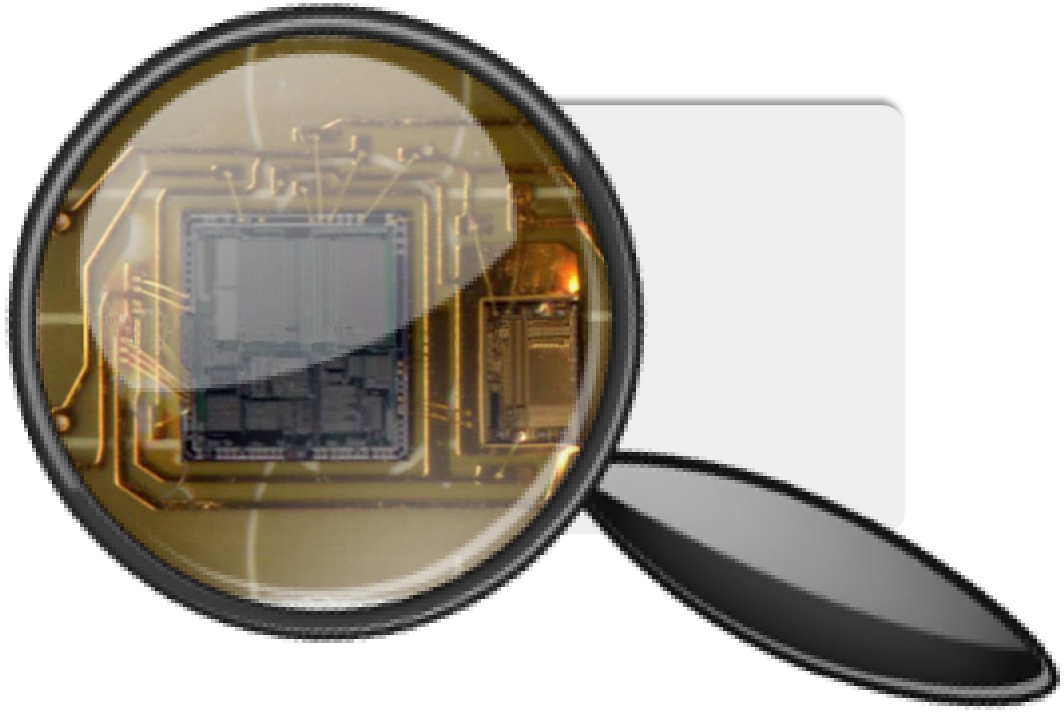
Chaîne de démarrage des SoC

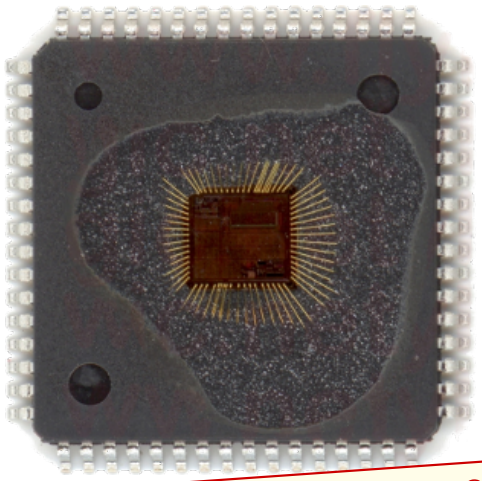


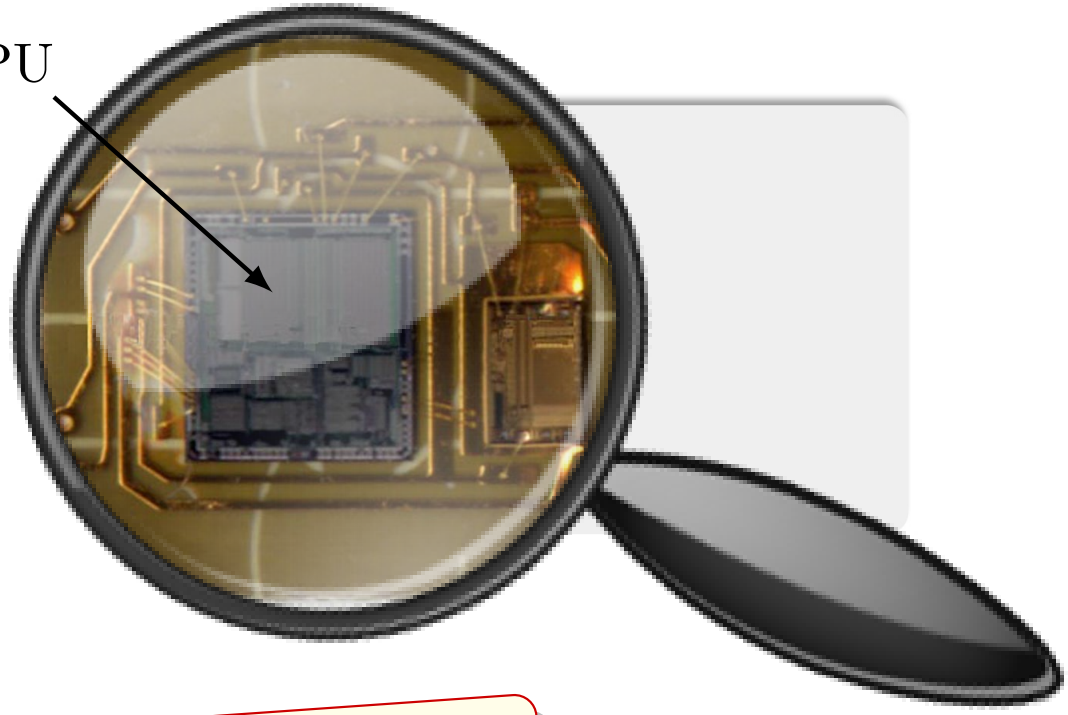

ATMEL
ATMEGA169P
16AU 0705


USB0
GPIOs
I²S
Flash
≈ 500KB
CPU
USB1
SDIO
I²C0
USART
SPI
Blocs
matériels
RAM
≈ 30KB
I²C1

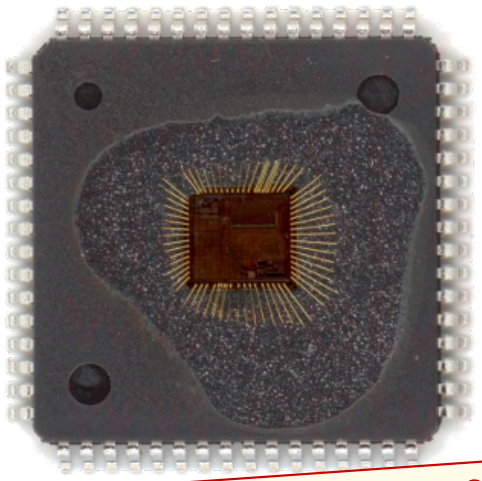


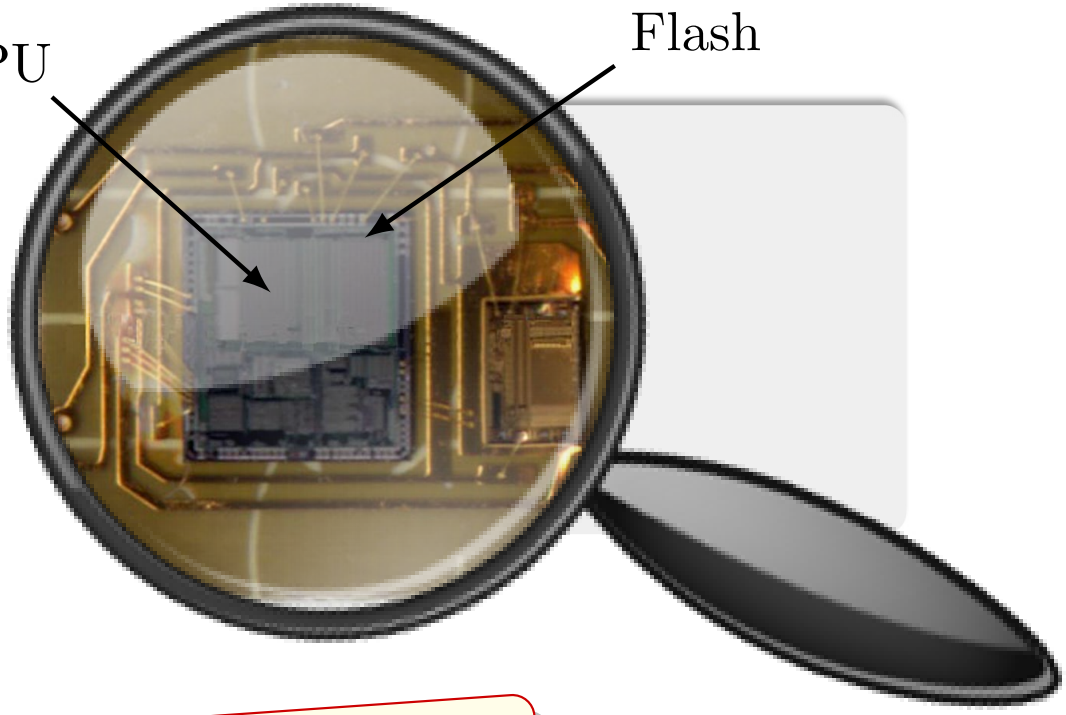






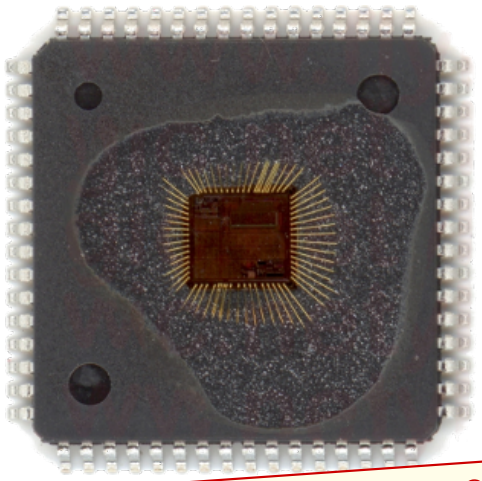
ARM SecurCore SC300

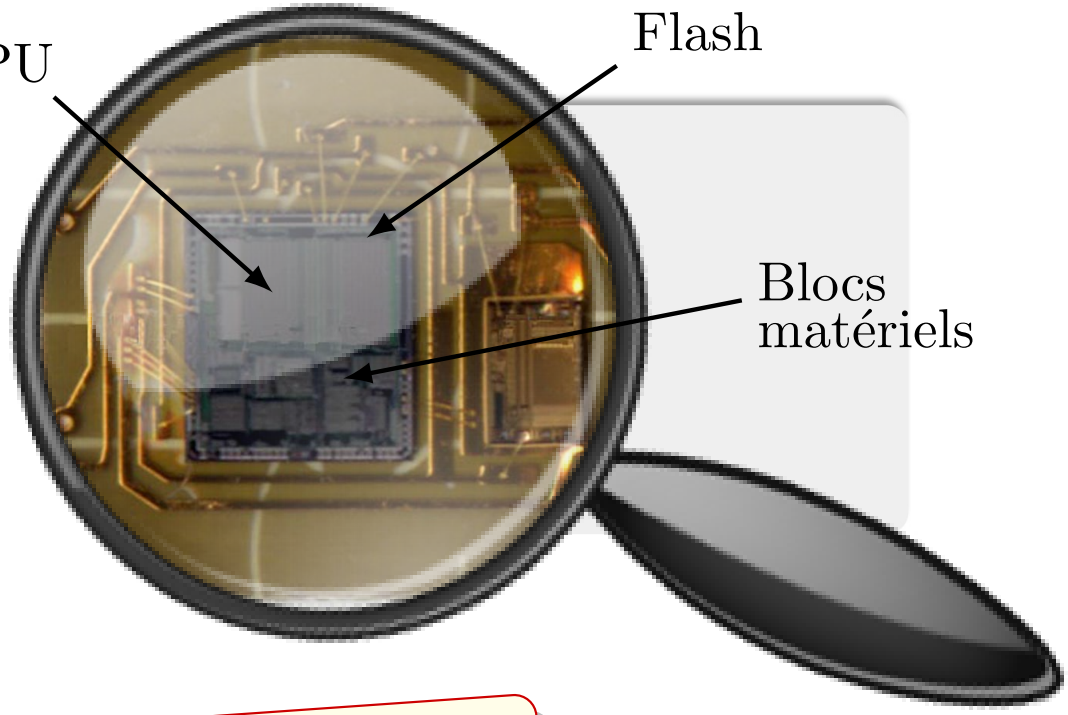




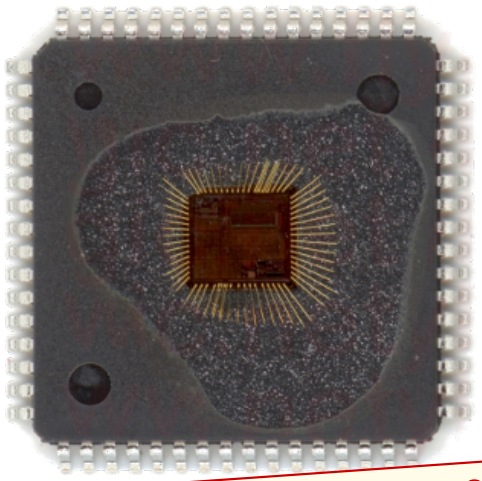
ARM SecurCore SC300

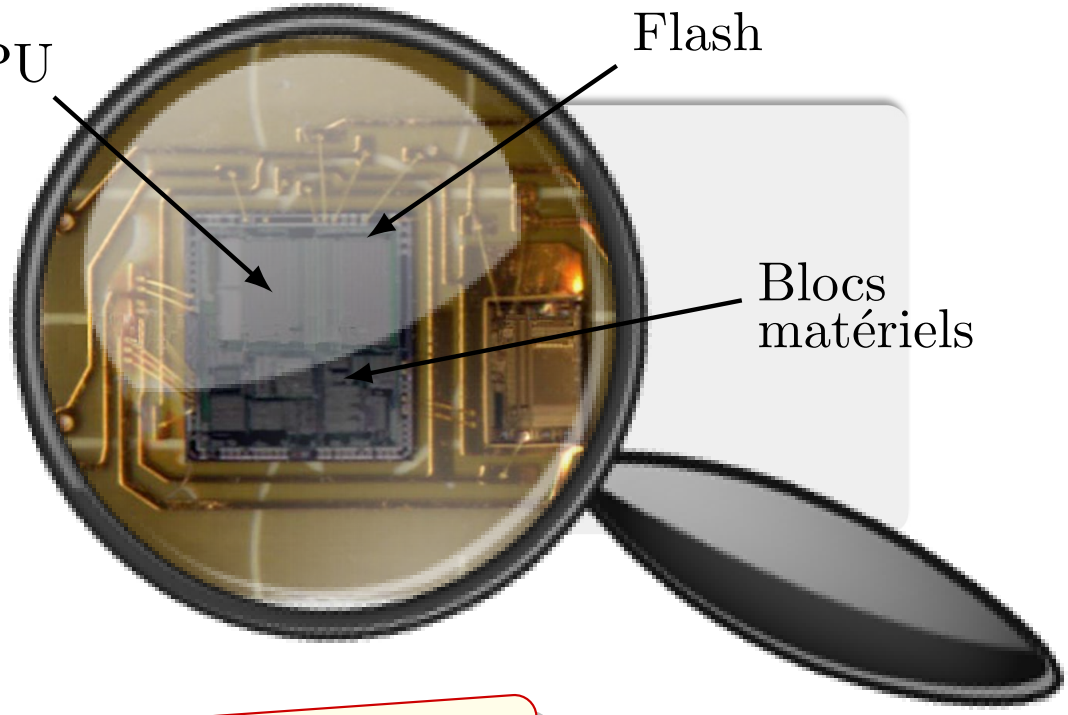
Flash protégée en confidentialité et intégrité



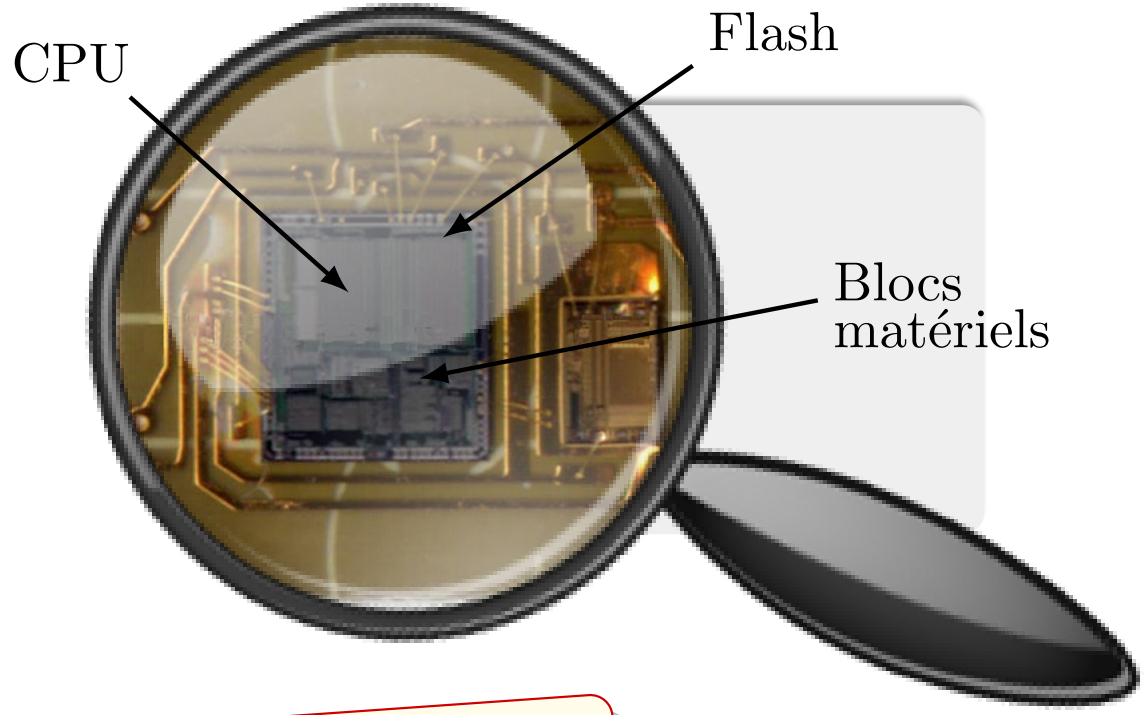


ARM SecurCore SC300
Flash protégée en confidentialité et intégrité
Générateur de nombres aléatoires
Accélérateurs cryptographiques





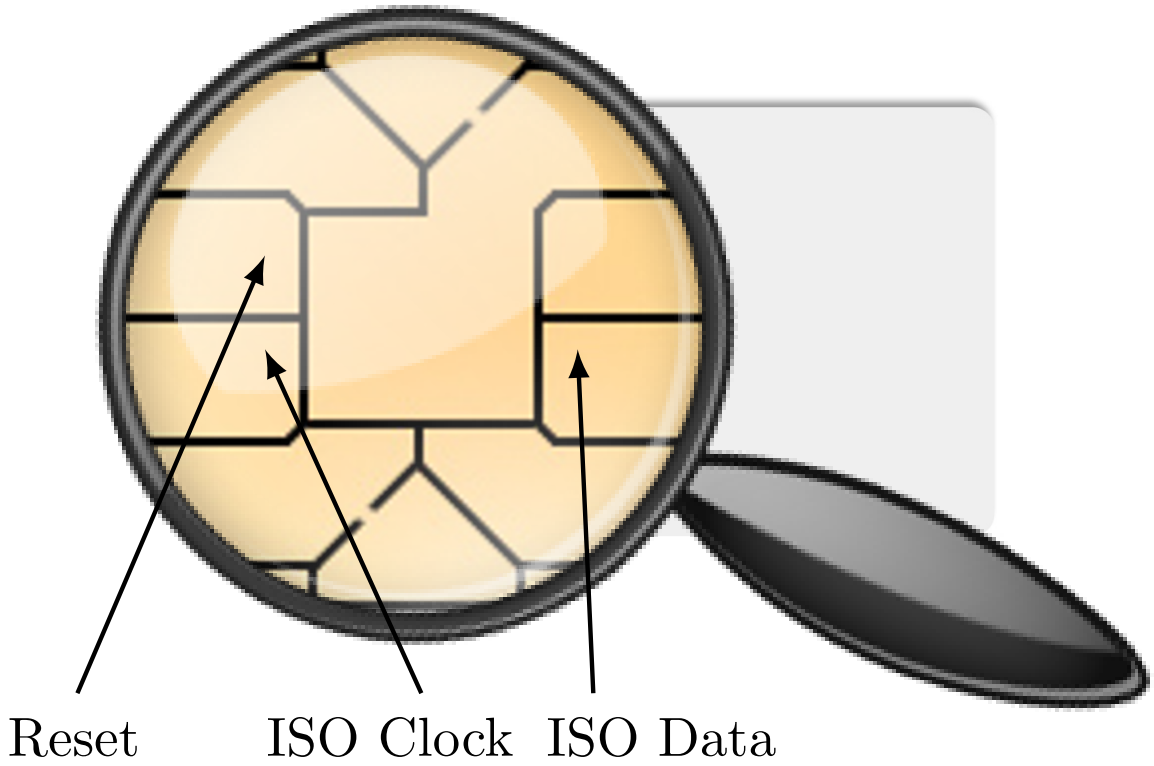
ARM SecurCore SC300
Flash protégée en confidentialité et intégrité
Générateur de nombres aléatoires
Accélérateurs cryptographiques
Détection des attaques par probing et
modification de signaux sur le circuit
Protections anti-DPA et contre les fautes



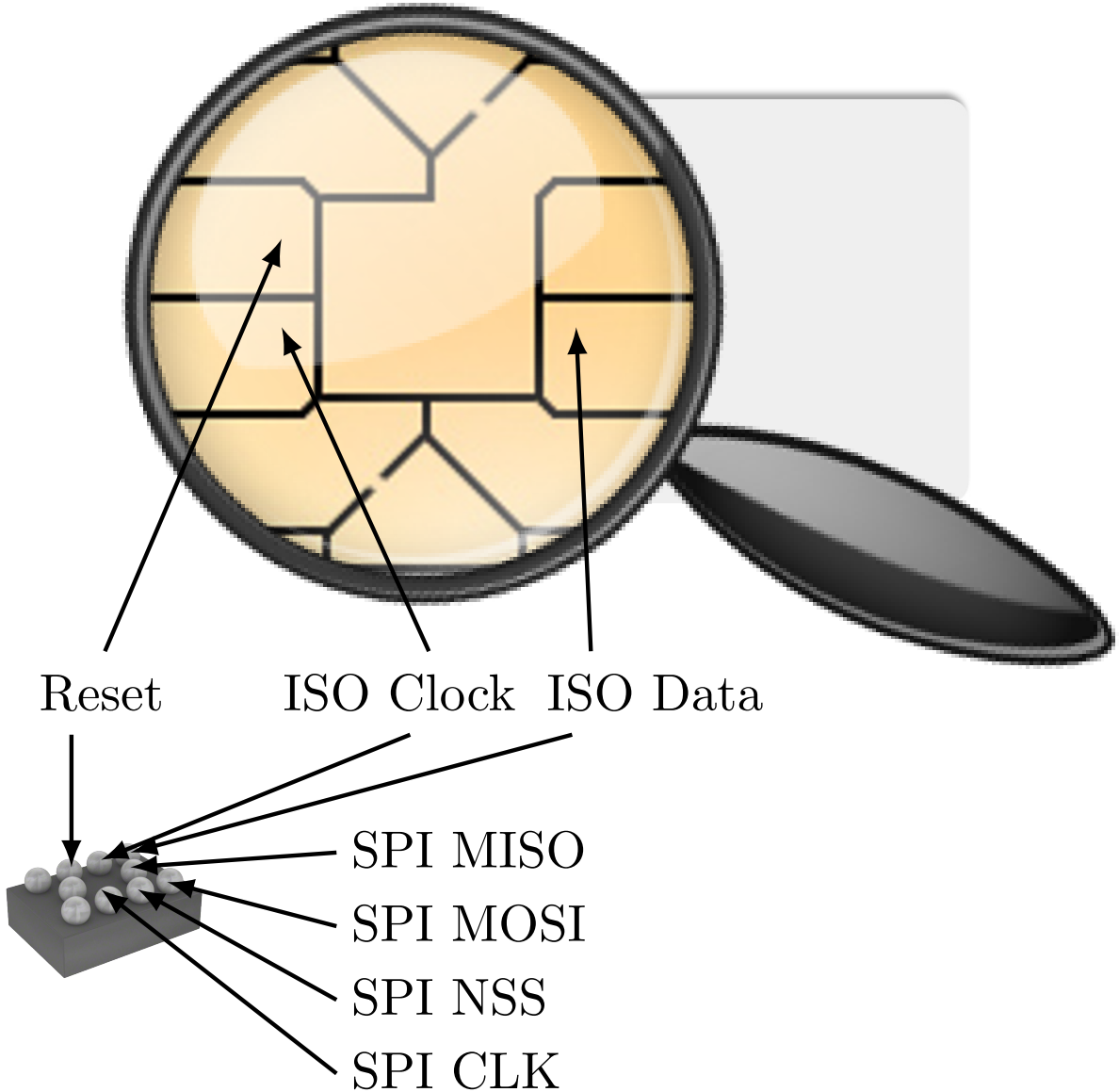
COMMON CRITERIA
CERTIFIED
EAL 5+

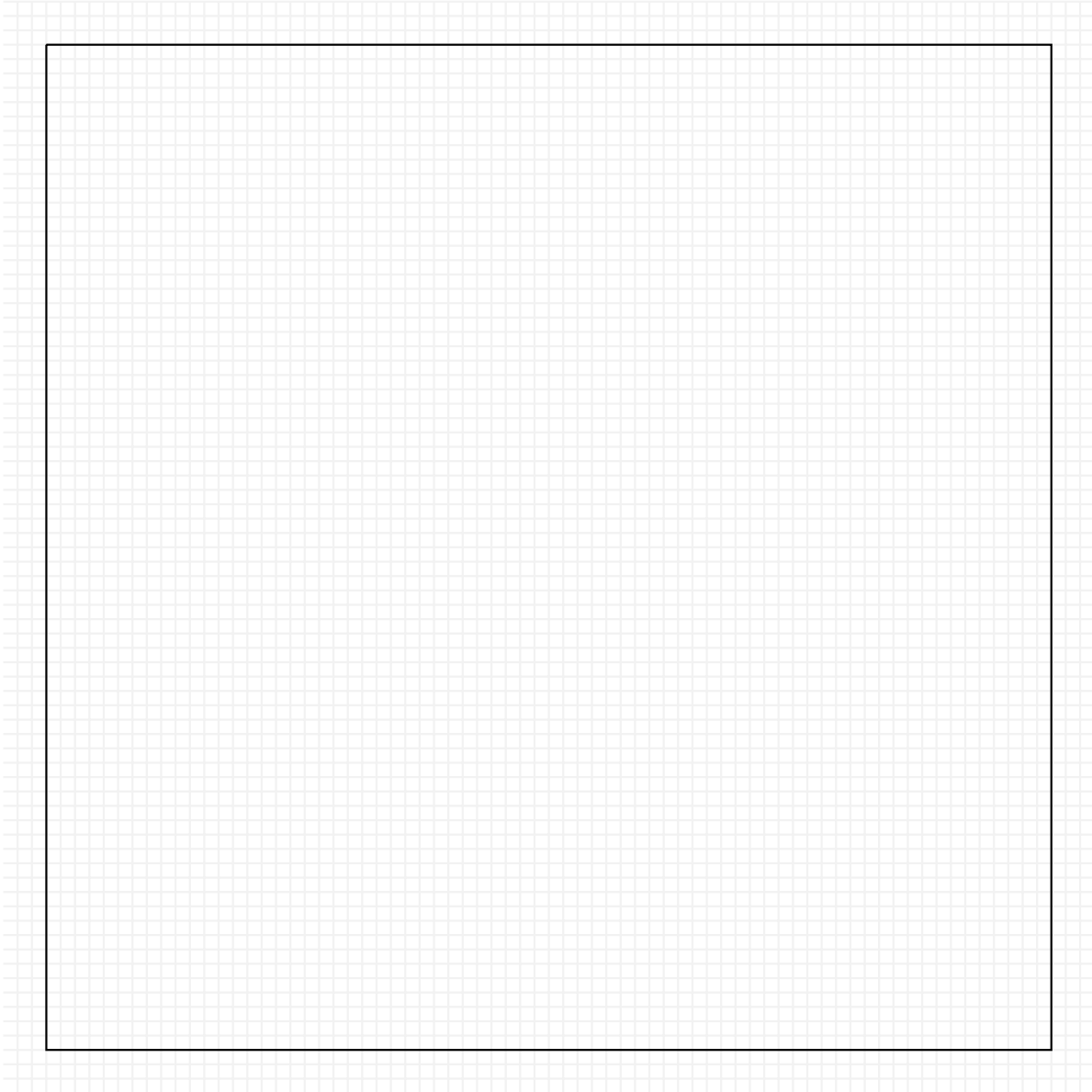
ARM SecurCore SC300
Flash protégée en confidentialité et intégrité
Générateur de nombres aléatoires
Accélérateurs cryptographiques
Détection des attaques par probing et
modification de signaux sur le circuit
Protections anti-DPA et contre les fautes

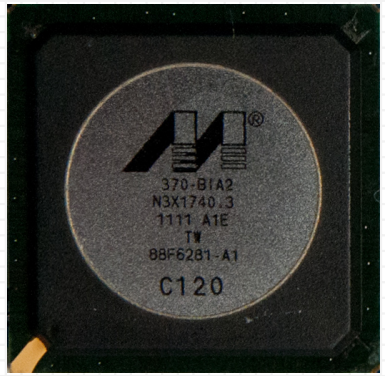

ATMEL
ATMEGA169P
16AU 0705

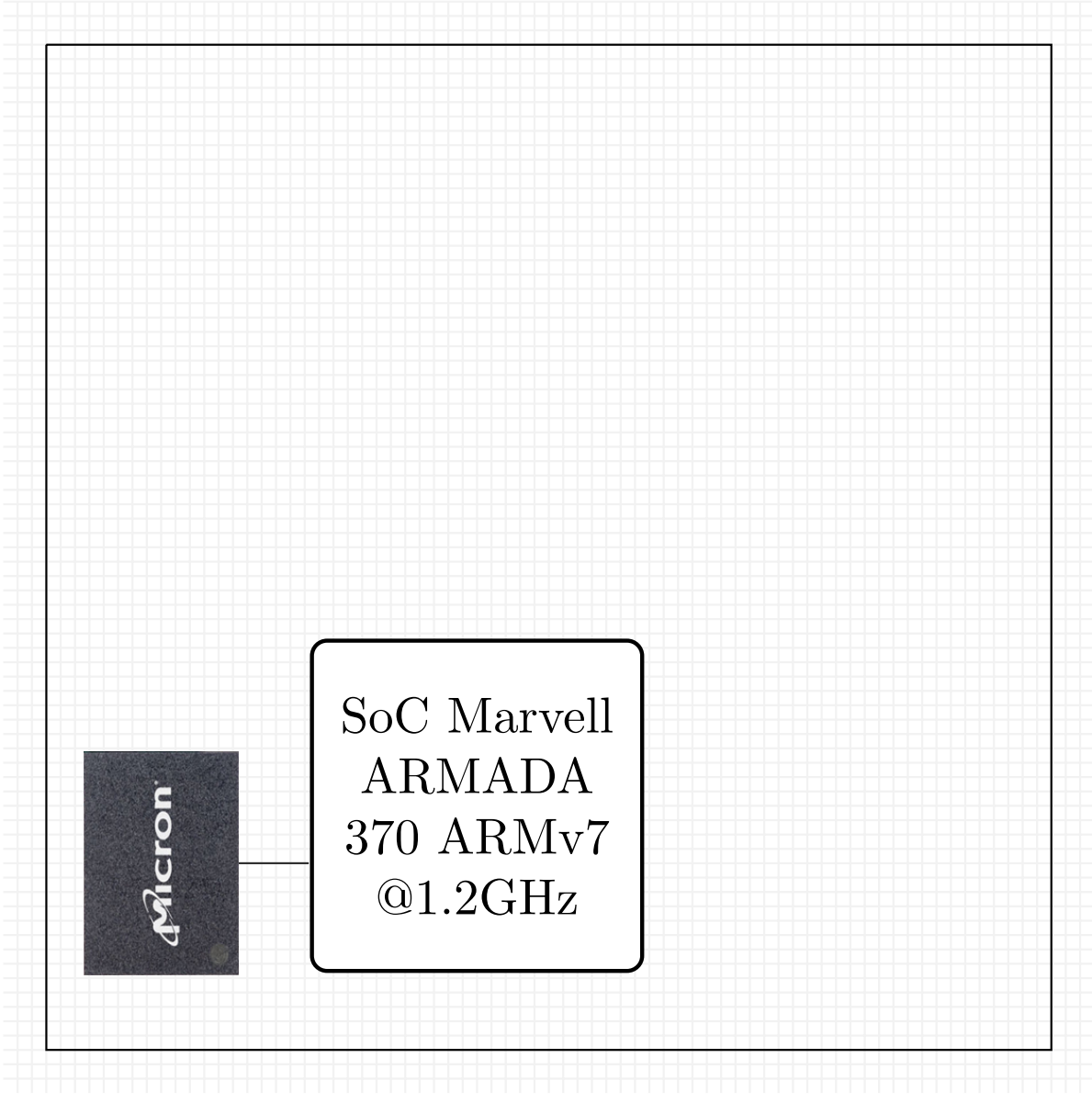

Reset
ISO Clock
ISO Data

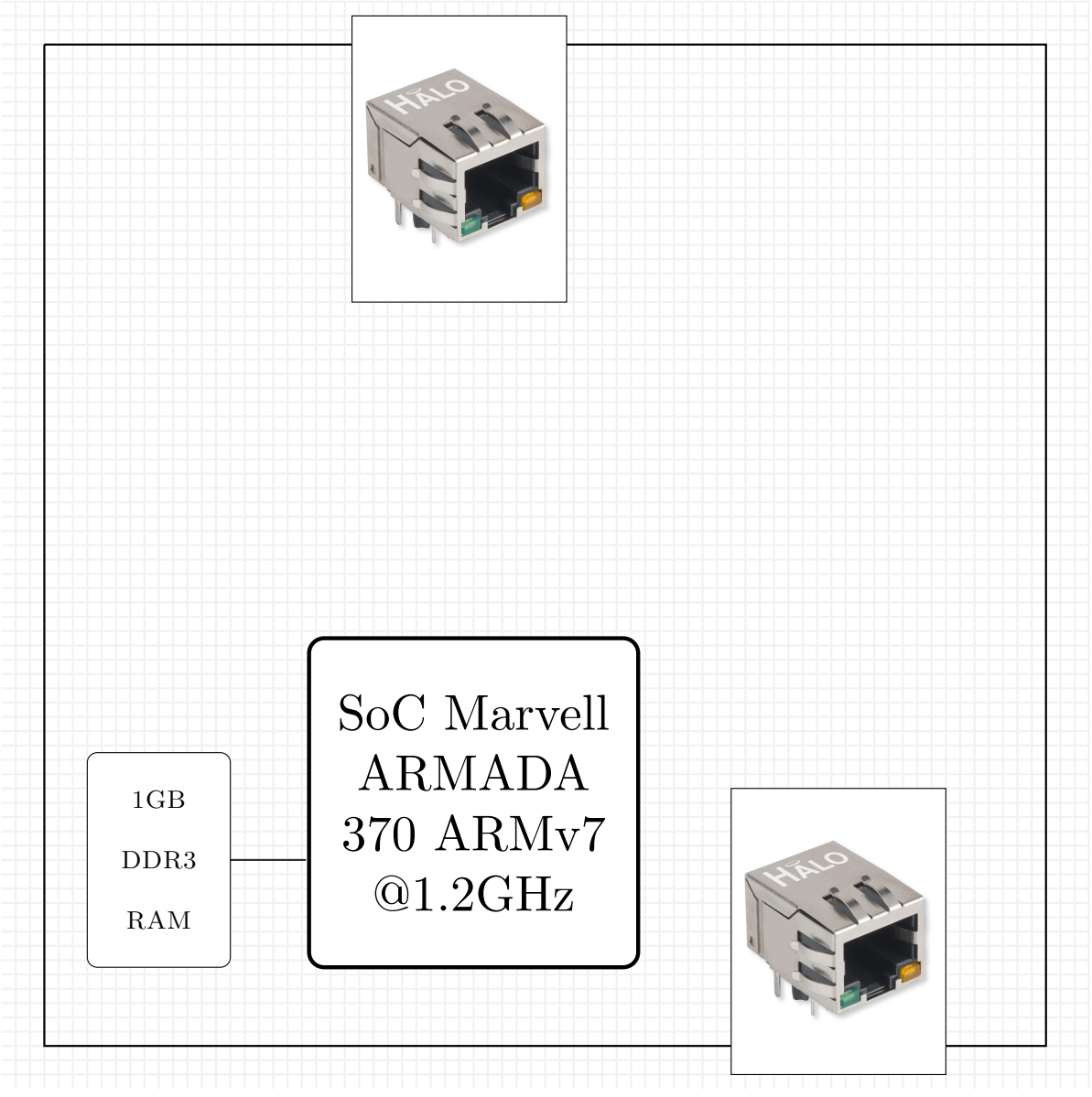

ATMEL
ATMEGA169P
16AU 0705

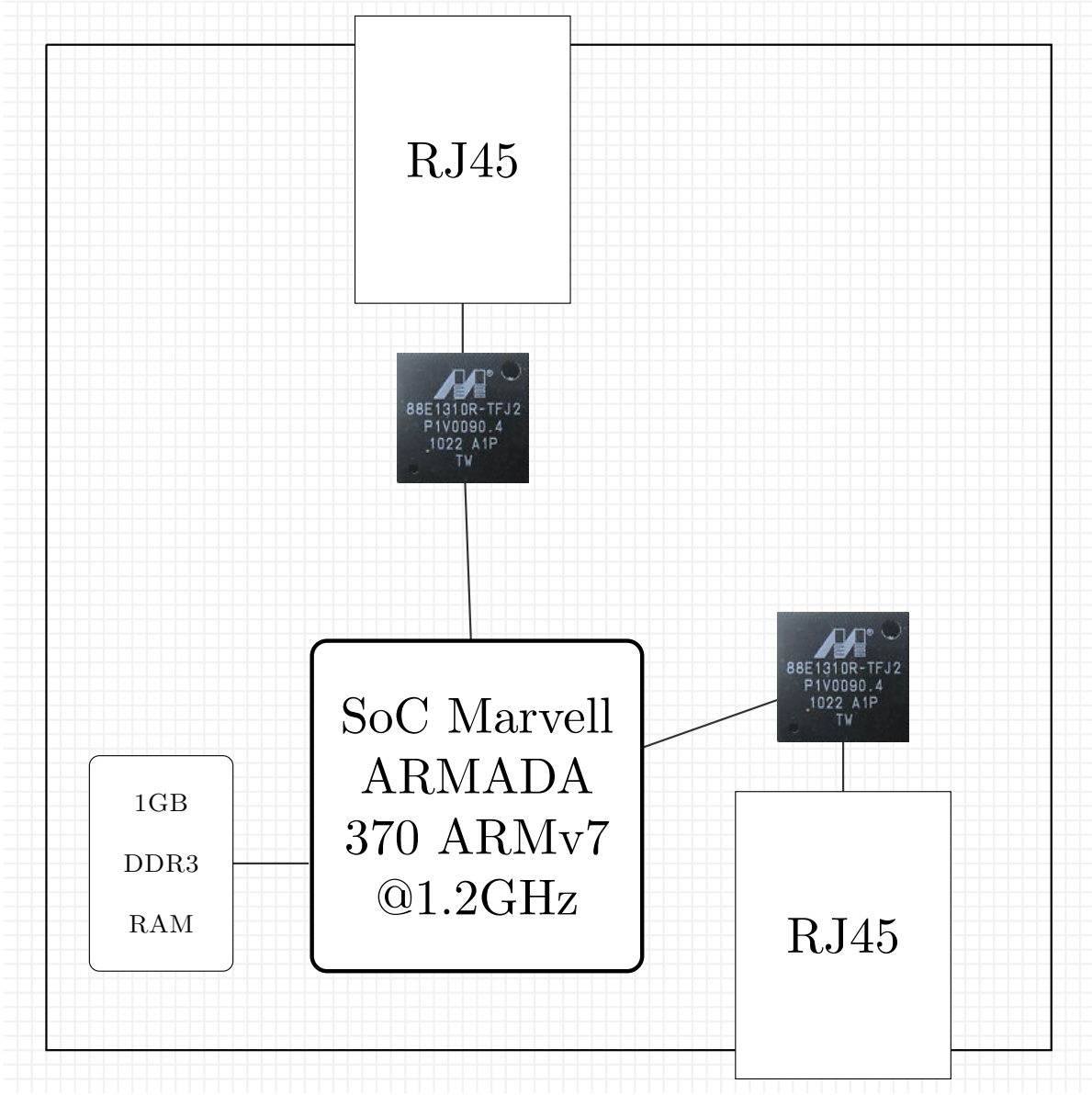

Reset
ISO Clock
ISO Data
SPI MISO
SPI MOSI
SPI NSS
SPI CLK

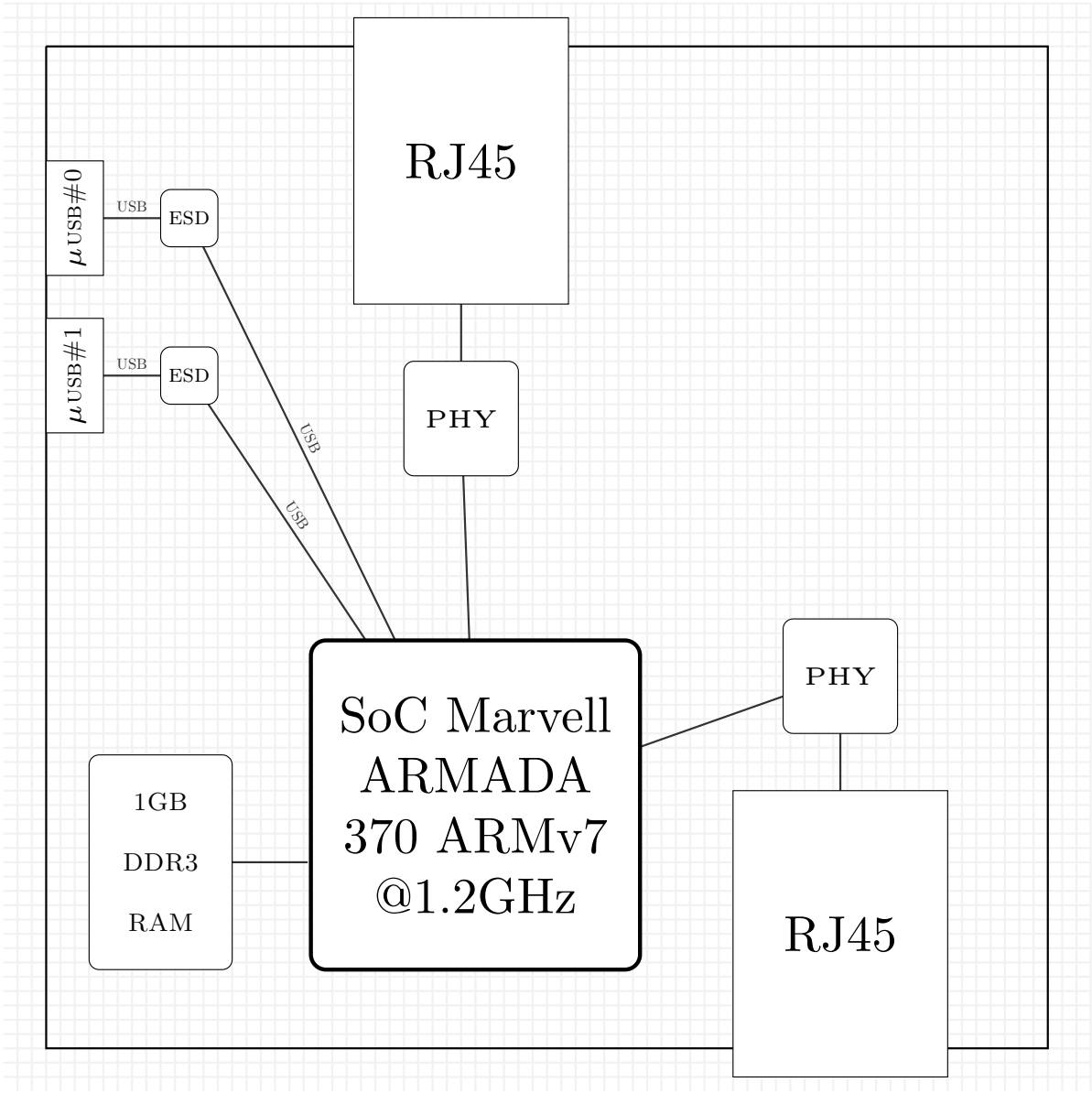


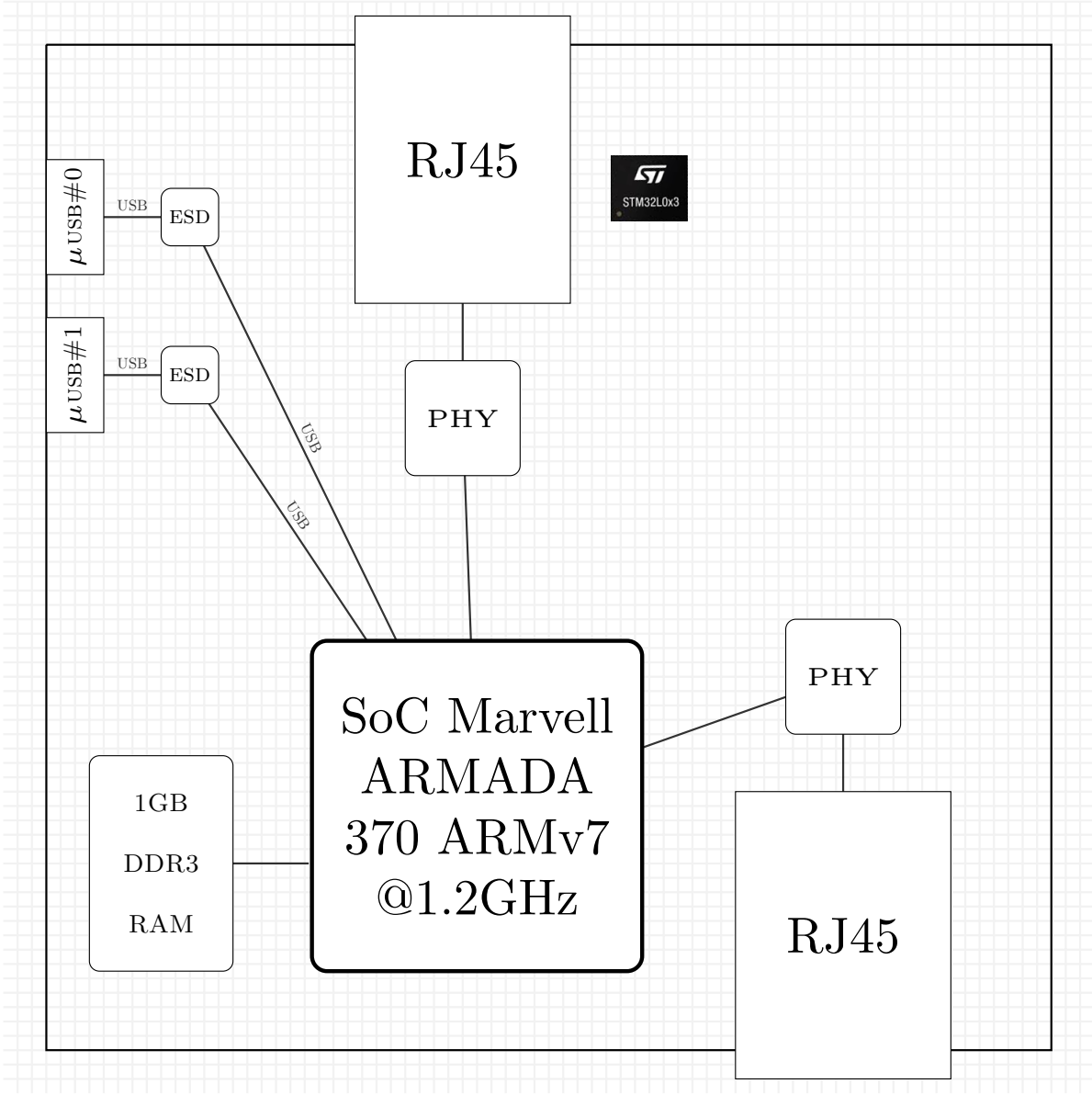

370-BIA2
N3X1740.3
1111 A1E
TW
88F6281-A1
C120

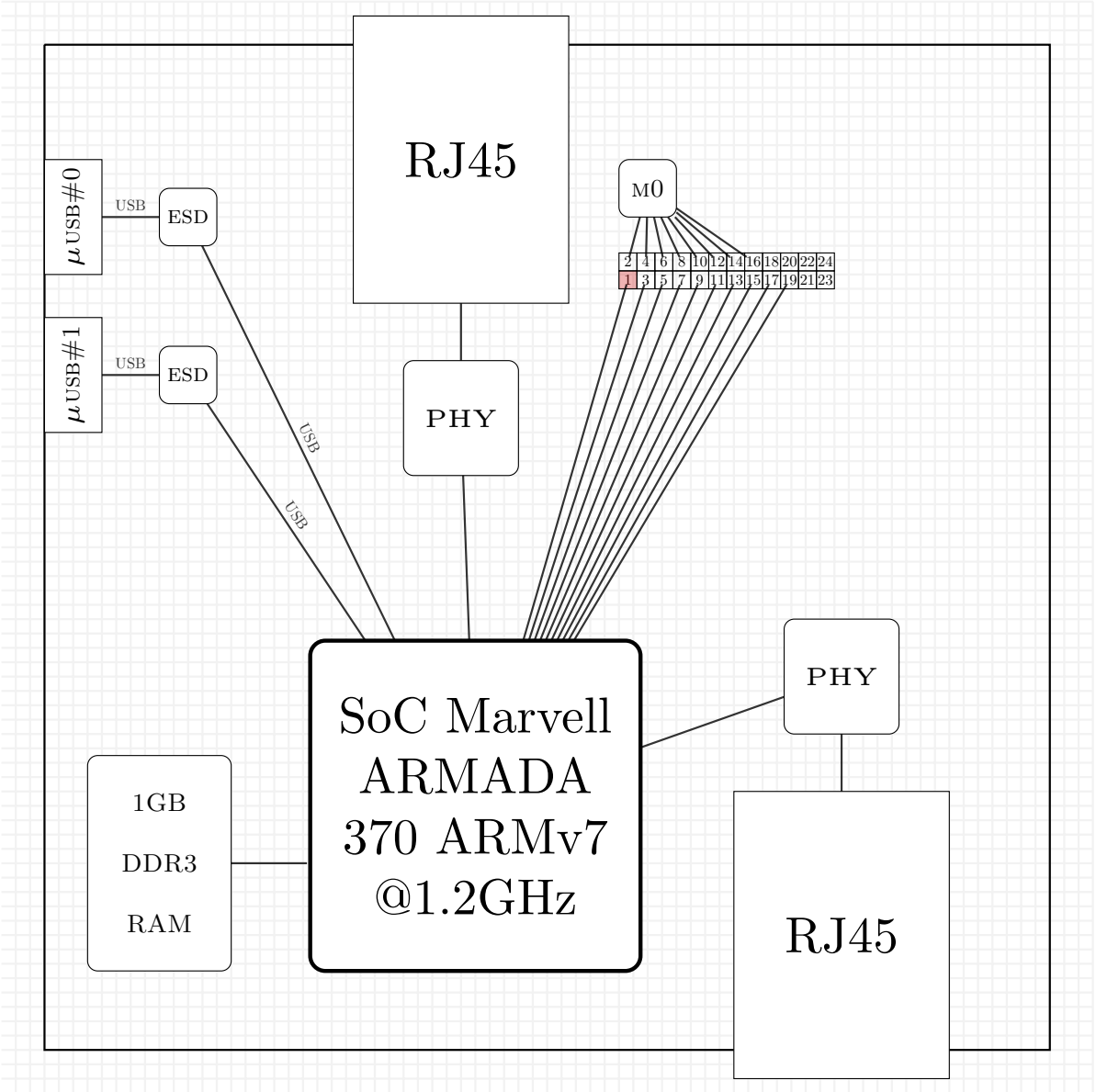

Micron
SoC Marvell
ARMADA
370 ARMv7
@1.2GHz

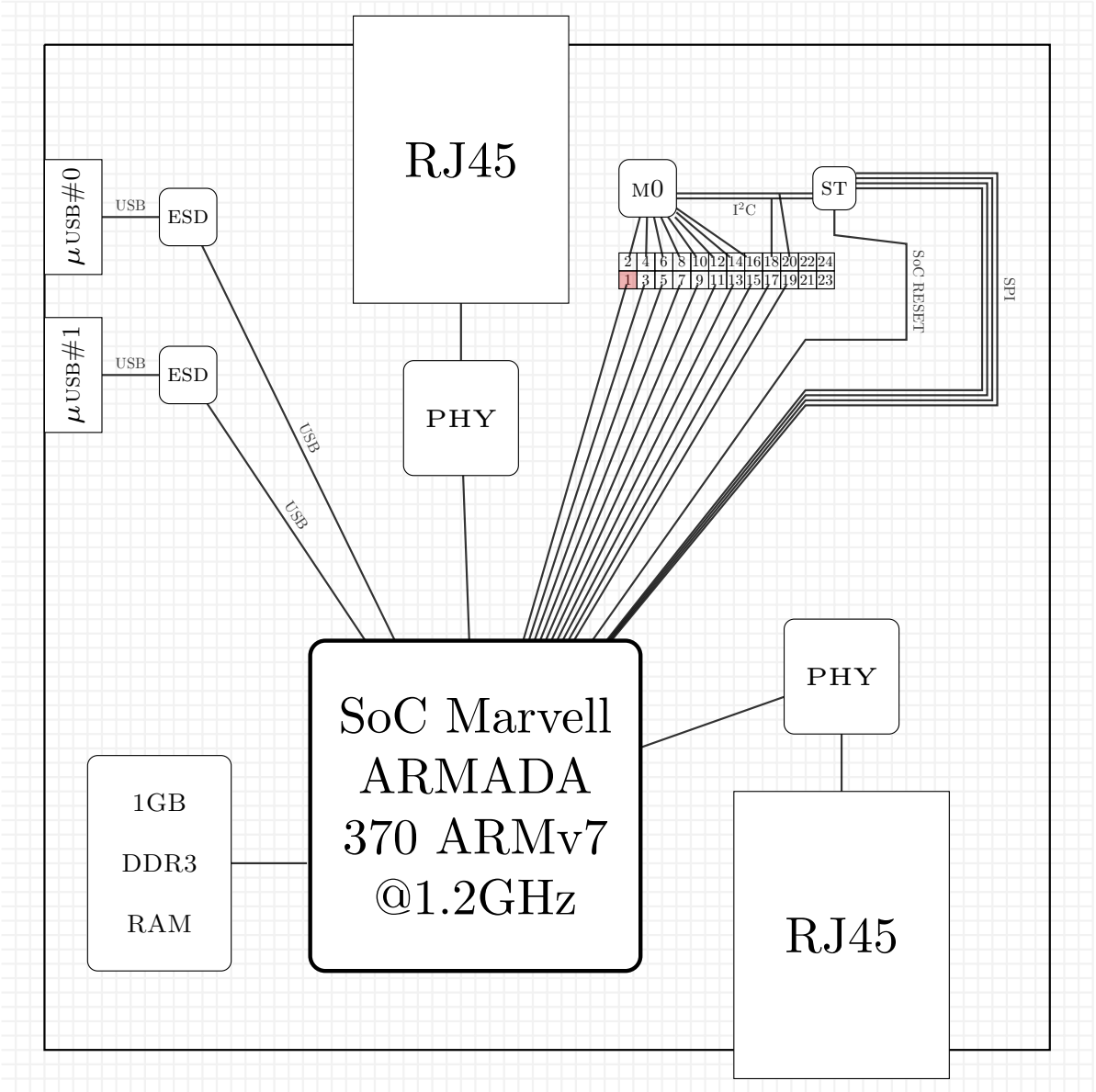

SoC Marvell
ARMADA
370 ARMv7
@1.2GHz
1GB
DDR3
RAM

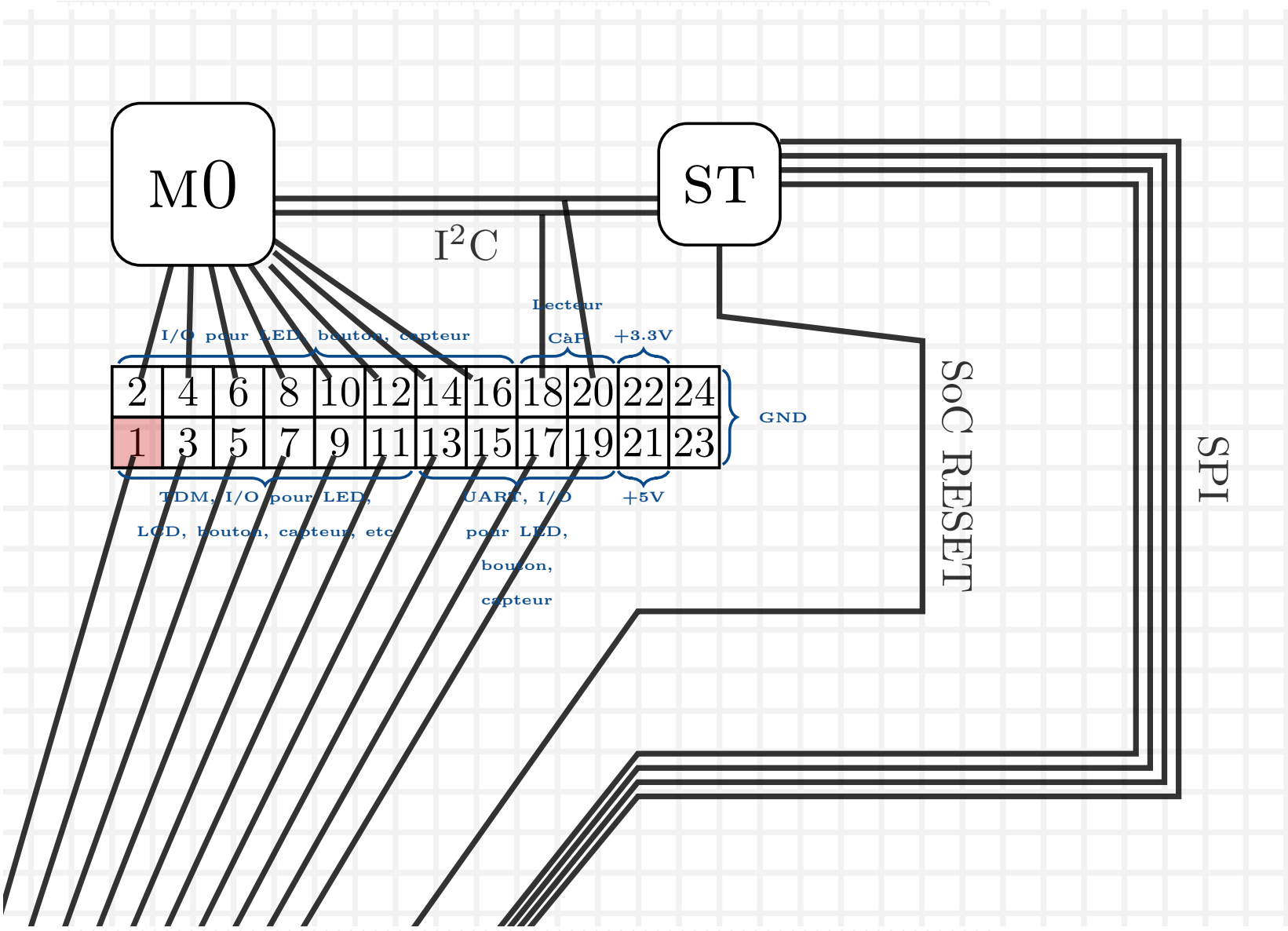

RJ45
88E1310R-TFJ2
P1V0090.4
.1022 A1P
TW
SoC Marvell
ARMADA
370 ARMv7
@1.2GHz
88E1310R-TFJ2
P1V0090.4
.1022 A1P
TW
1GB
DDR3
RAM
RJ45

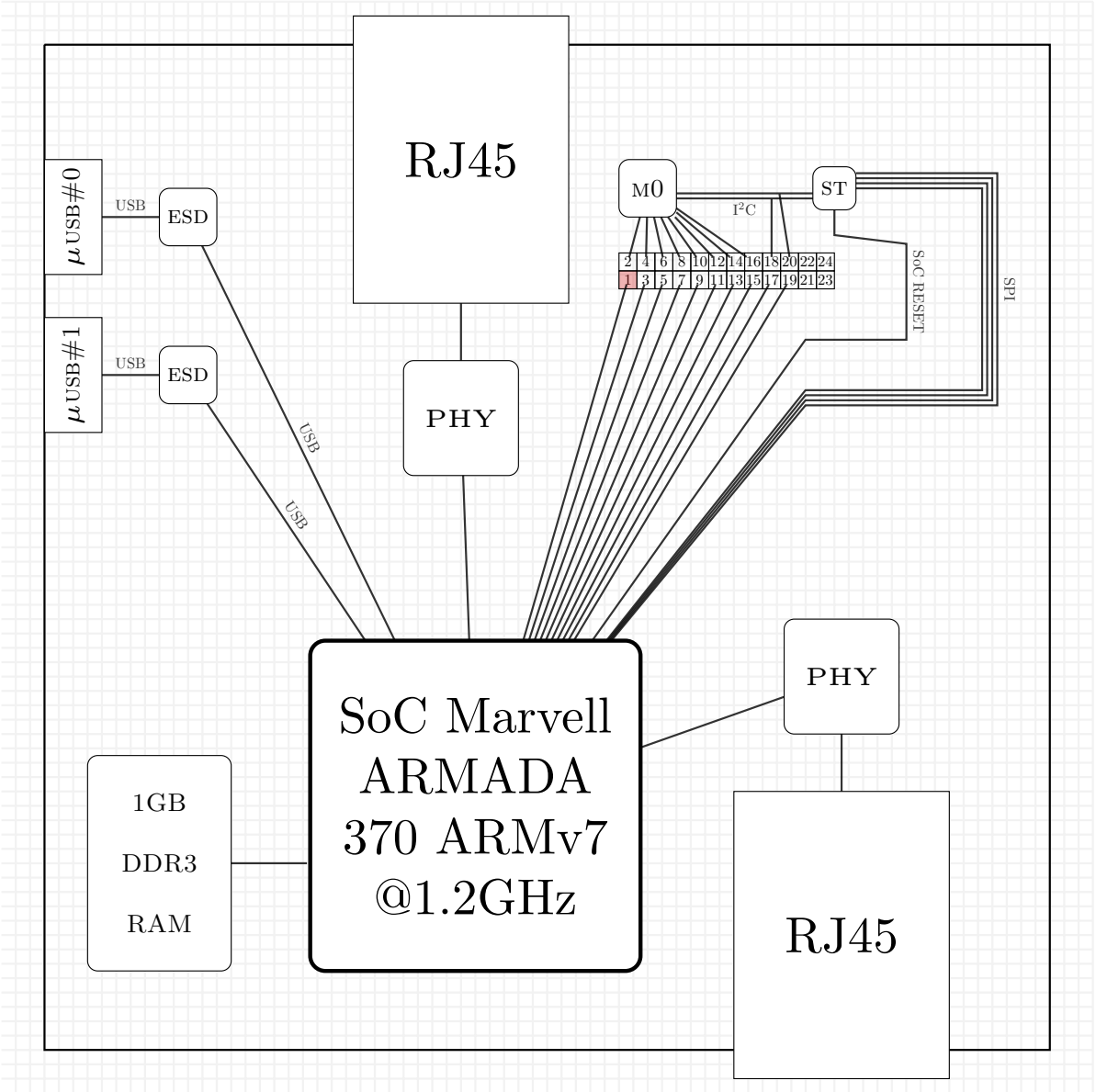

RJ45
µUSB#0
USB
ESD
µUSB#1
USB
ESD
PHY
USB
USB
SoC Marvell
ARMADA
370 ARMv7
@1.2GHz
1GB
DDR3
RAM
PHY
RJ45

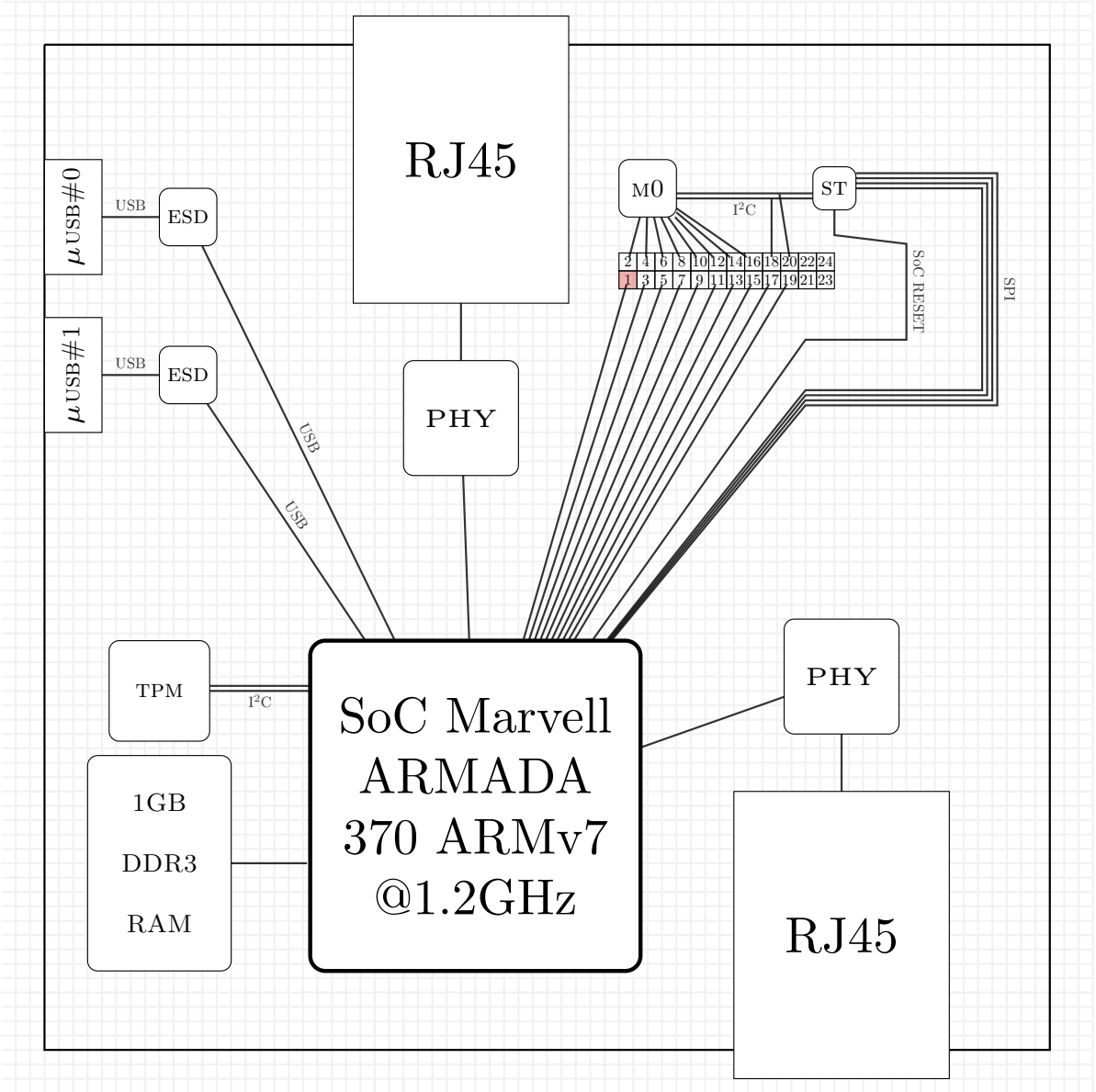

RJ45
STM32L0x3
µUSB#0
USB
ESD
µUSB#1
USB
ESD
PHY
USB
USB
SoC Marvell
ARMADA
370 ARMv7
@1.2GHz
PHY
1GB
DDR3
RAM
RJ45

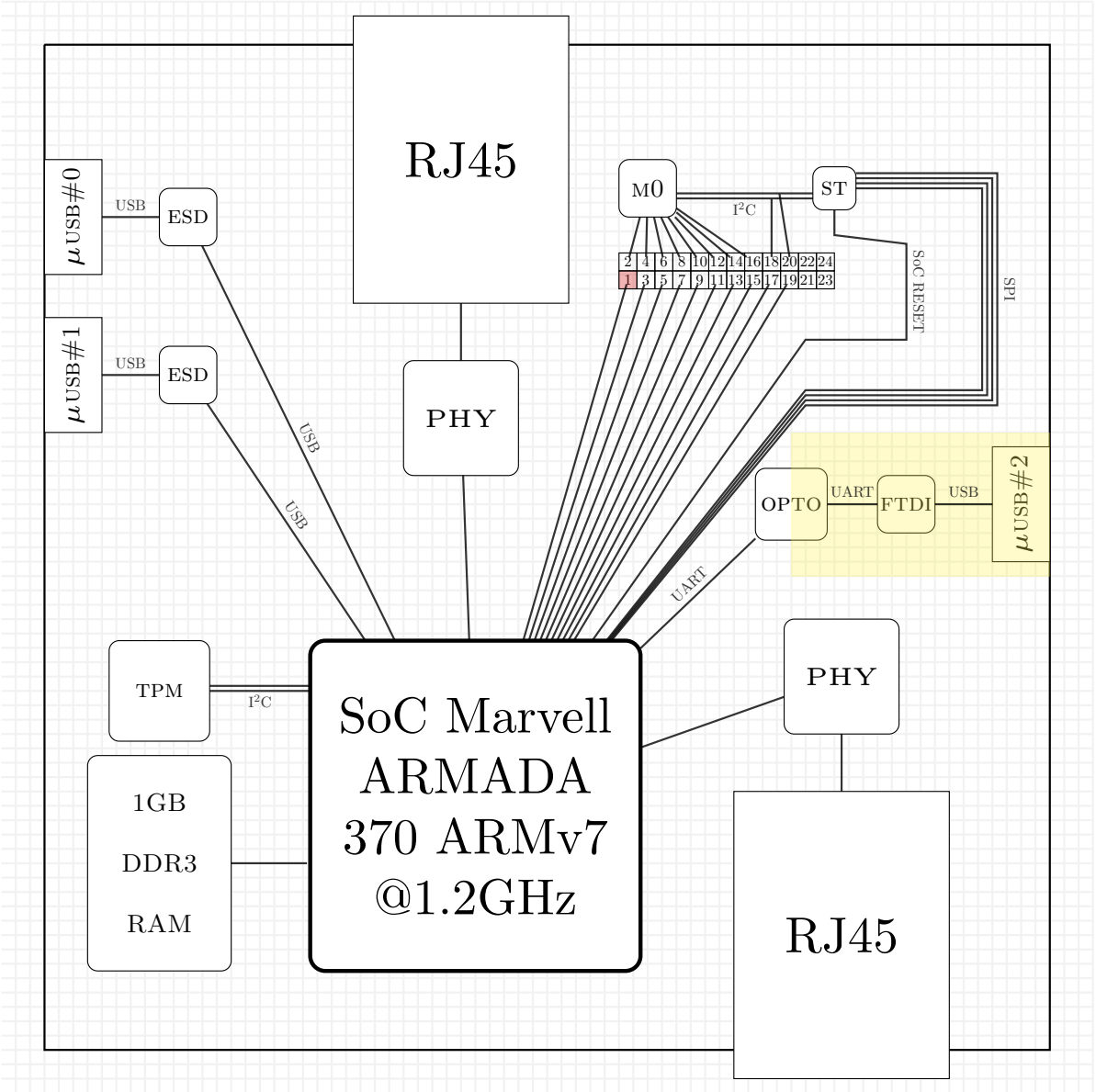

RJ45
µUSB#0
USB
ESD
µUSB#1
USB
ESD
USB
USB
PHY
M0
2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23
SoC Marvell
ARMADA
370 ARMv7
@1.2GHz
1GB
DDR3
RAM
PHY
RJ45

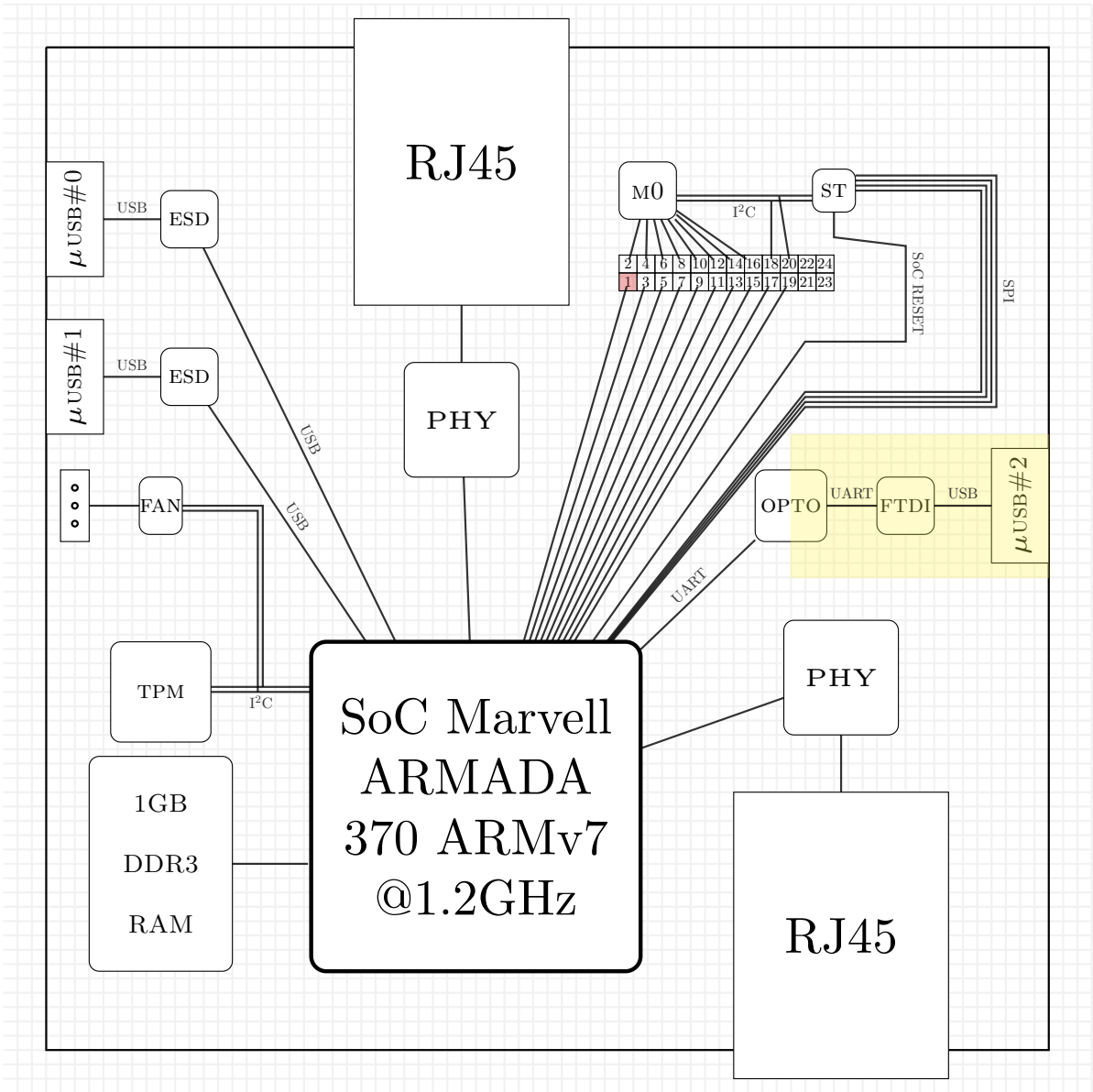

RJ45
µUSB#0
USB
ESD
µUSB#1
USB
ESD
USB
USB
PHY
M0
I²C
ST
SoC RESET
SPI
2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23
SoC Marvell
ARMADA
370 ARMv7
@1.2GHz
1GB
DDR3
RAM
PHY
RJ45

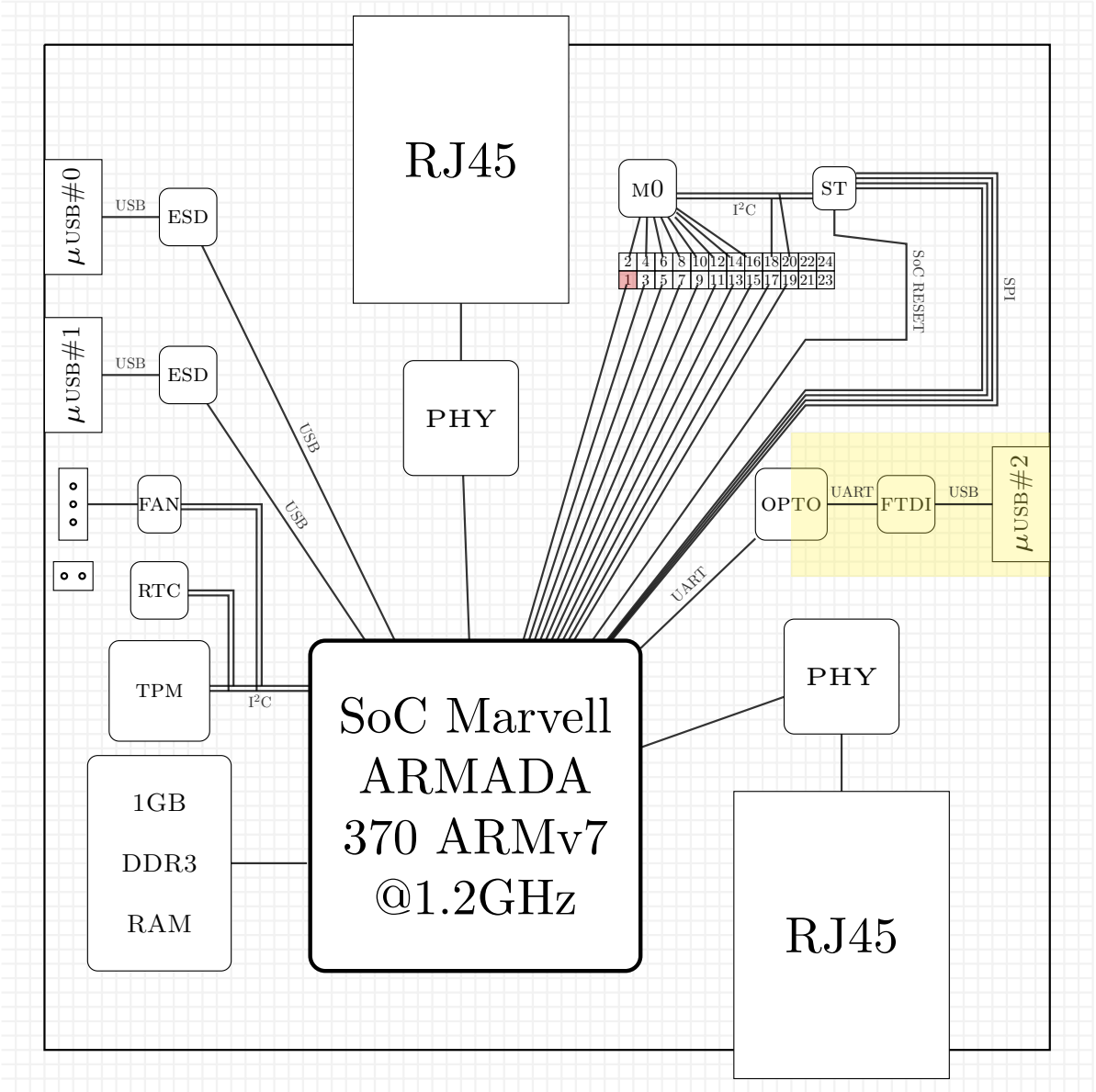

M0
ST
I²C
Lecteur CàP
+3.3V
I/O pour LED, bouton, capteur
2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23
GND
TDM, I/O pour LED, LCD, bouton, capteur, etc
UART, I/O pour LED, bouton, capteur
+5V
SoC RESET
SPI

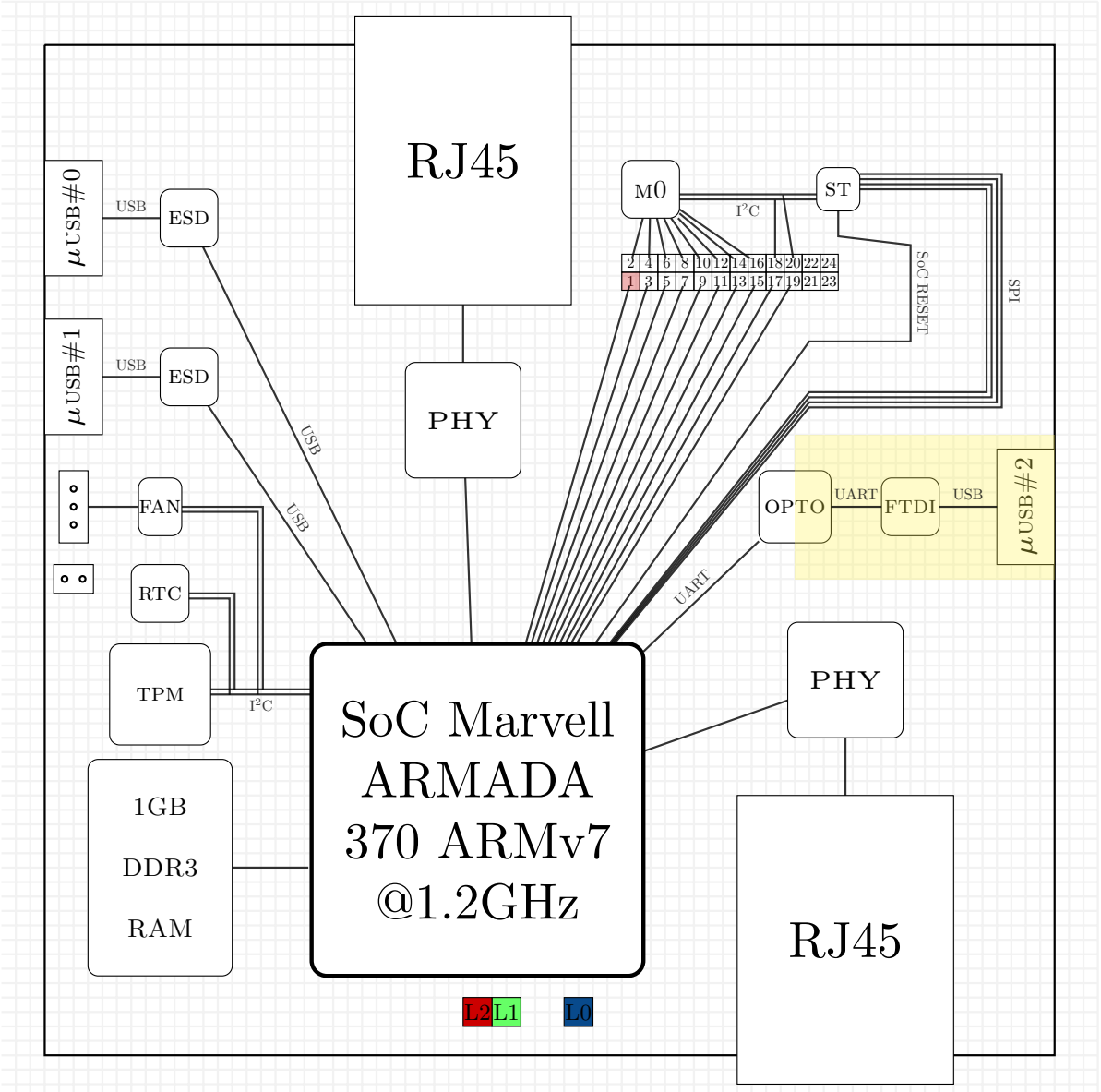

RJ45
µUSB#0
USB
ESD
µUSB#1
USB
ESD
USB
USB
PHY
M0
I²C
ST
SoC RESET
SPI
2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23
SoC Marvell
ARMADA
370 ARMv7
@1.2GHz
1GB
DDR3
RAM
PHY
RJ45

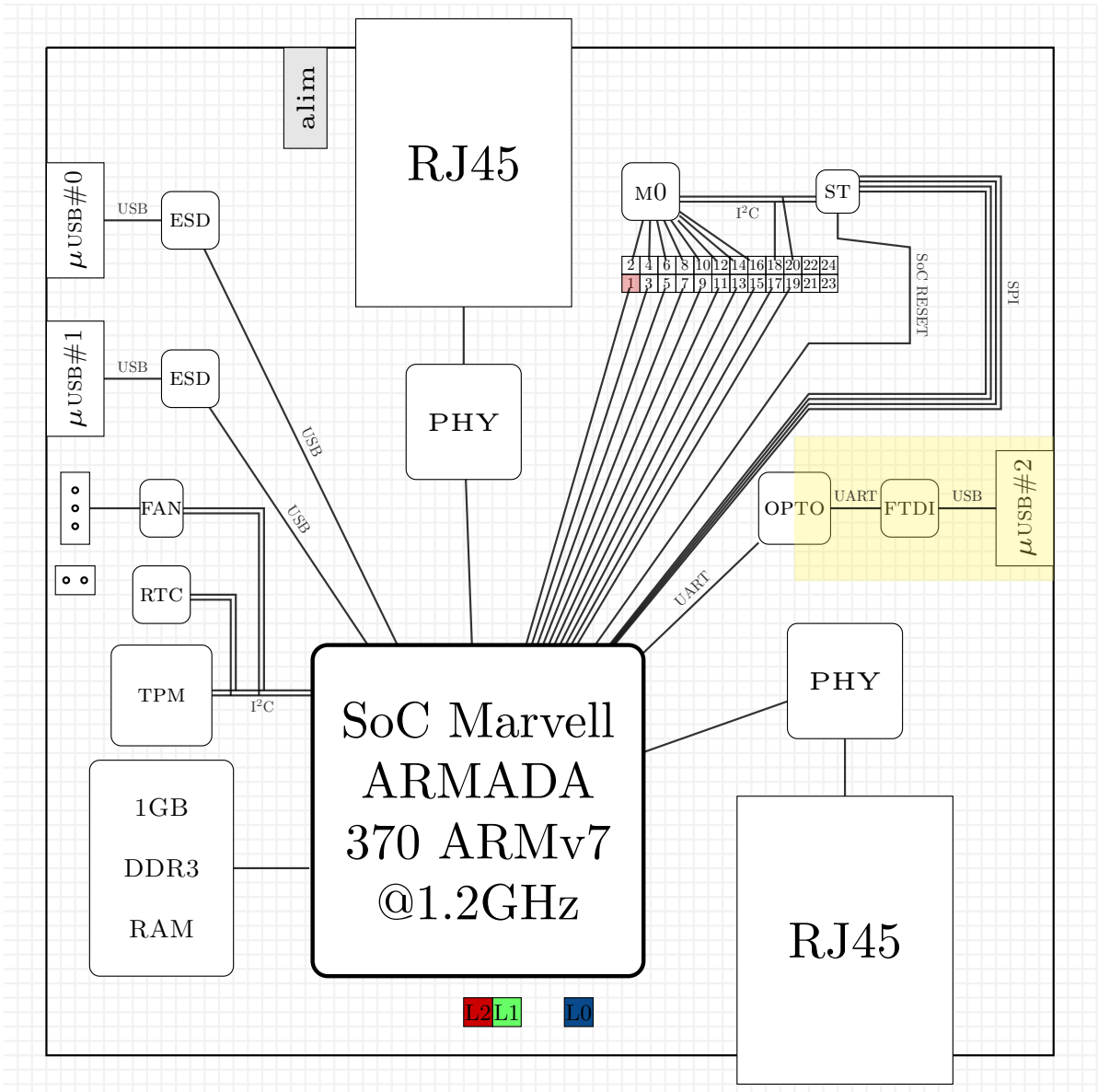

RJ45
µUSB#0
USB
ESD
µUSB#1
USB
ESD
PHY
USB
USB
M0
I²C
ST
SoC RESET
SPI
2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23
TPM
I²C
1GB
DDR3
RAM
SoC Marvell
ARMADA
370 ARMv7
@1.2GHz
PHY
RJ45

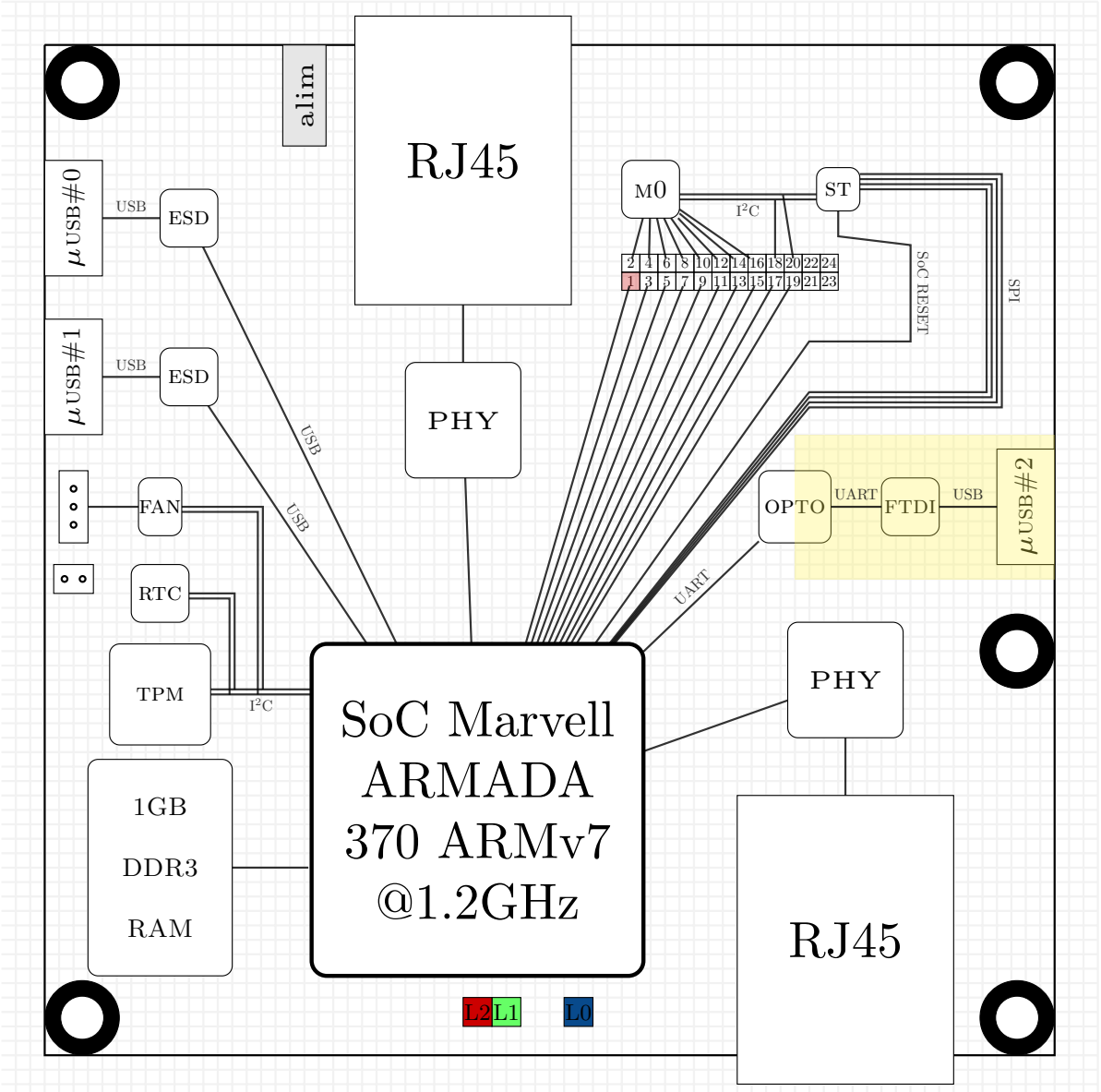

RJ45
µUSB#0
USB
ESD
µUSB#1
USB
ESD
PHY
M0
I²C
ST
SoC RESET
SPI
2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23
USB
USB
OPTO
UART
FTDI
USB
µUSB#2
UART
TPM
I²C
SoC Marvell
ARMADA
370 ARMv7
@1.2GHz
PHY
1GB
DDR3
RAM
RJ45

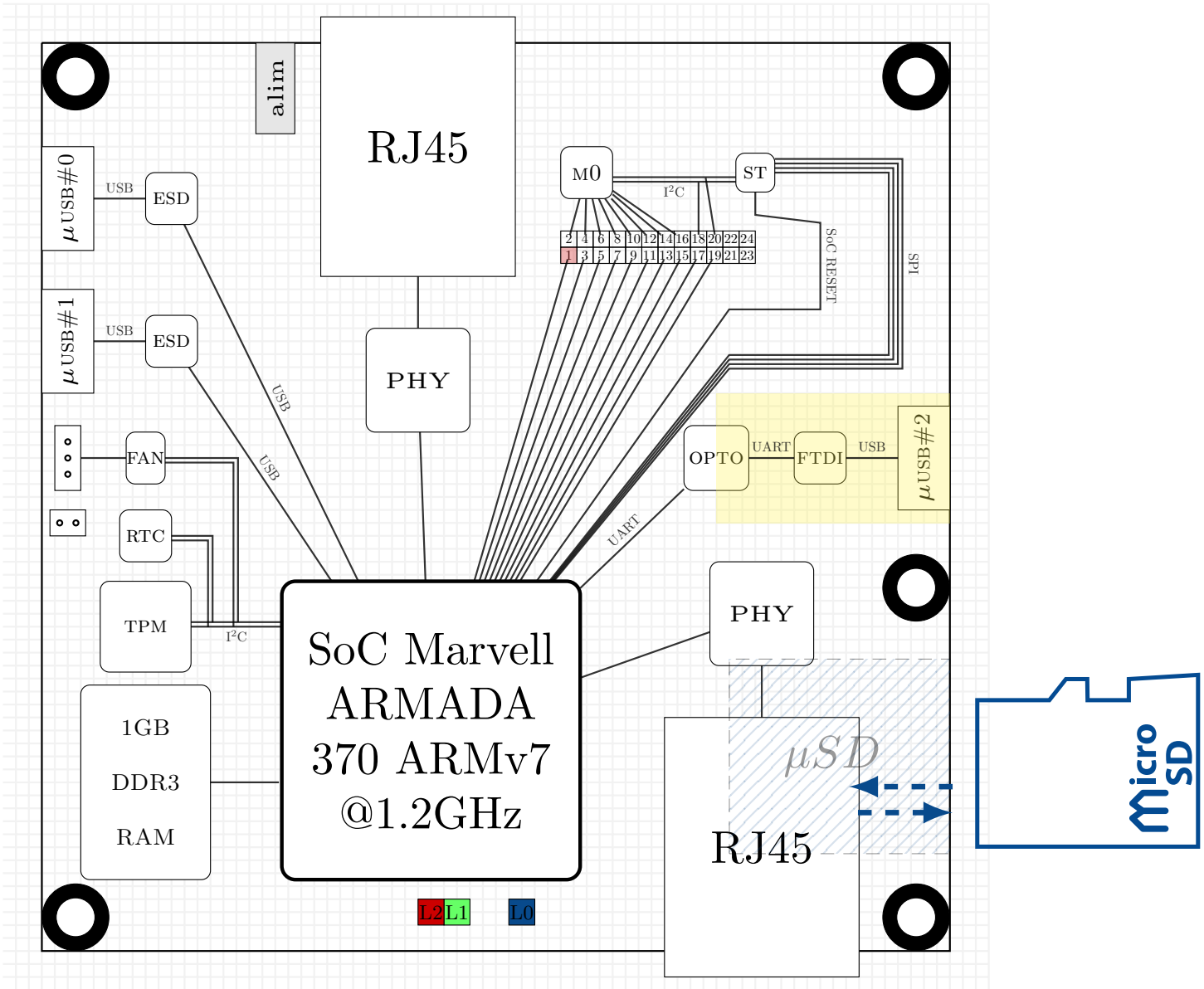

RJ45
µUSB#0
USB
ESD
µUSB#1
USB
ESD
FAN
TPM
I²C
1GB
DDR3
RAM
PHY
USB
USB
M0
I²C
ST
SoC RESET
SPI
2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23
OPTO
UART
FTDI
USB
µUSB#2
UART
SoC Marvell
ARMADA
370 ARMv7
@1.2GHz
PHY
RJ45

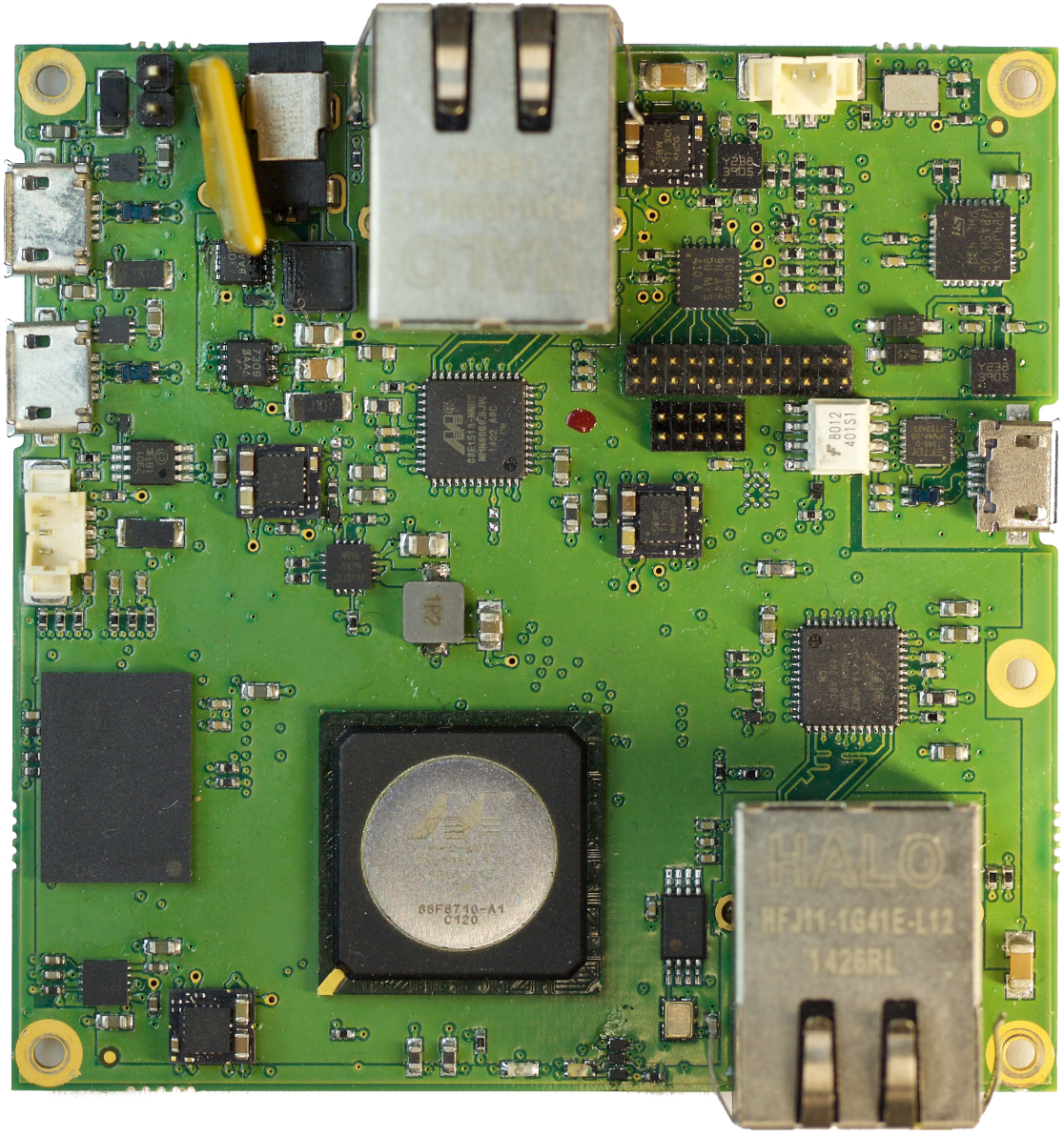

RJ45
µUSB#0
USB
ESD
µUSB#1
USB
ESD
PHY
M0
I²C
ST
SoC RESET
SPI
2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23
USB
USB
FAN
RTC
TPM
I²C
OPTO
UART
FTDI
USB
µUSB#2
UART
PHY
SoC Marvell
ARMADA
370 ARMv7
@1.2GHz
1GB
DDR3
RAM
RJ45

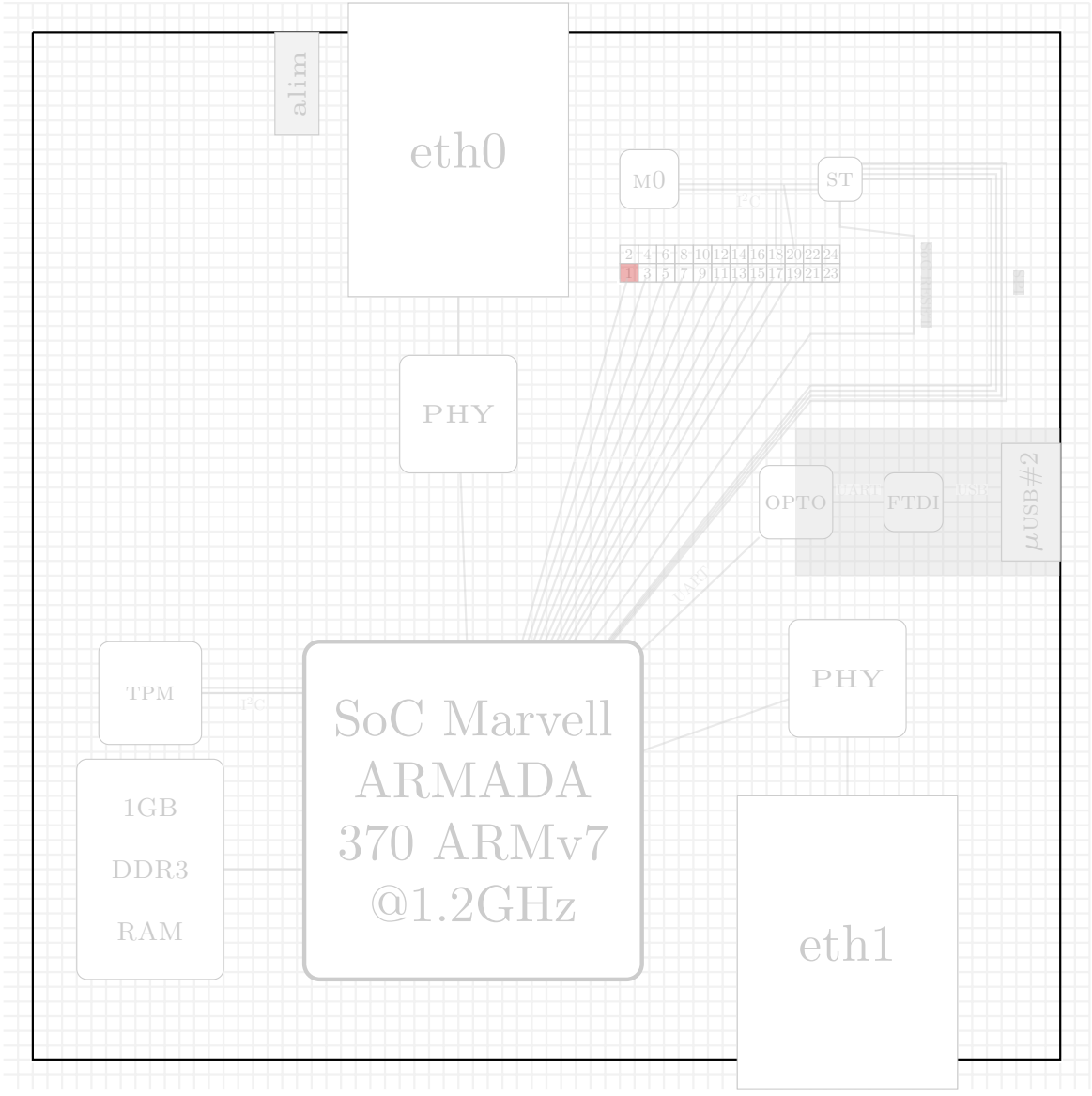

RJ45
µUSB#0
USB
ESD
µUSB#1
USB
ESD
PHY
M0
I²C
ST
SoC RESET
SPI
2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23
USB
USB
FAN
RTC
TPM
I²C
OPTO
UART
FTDI
USB
µUSB#2
UART
PHY
SoC Marvell
ARMADA
370 ARMv7
@1.2GHz
1GB
DDR3
RAM
RJ45
L2 L1
L0

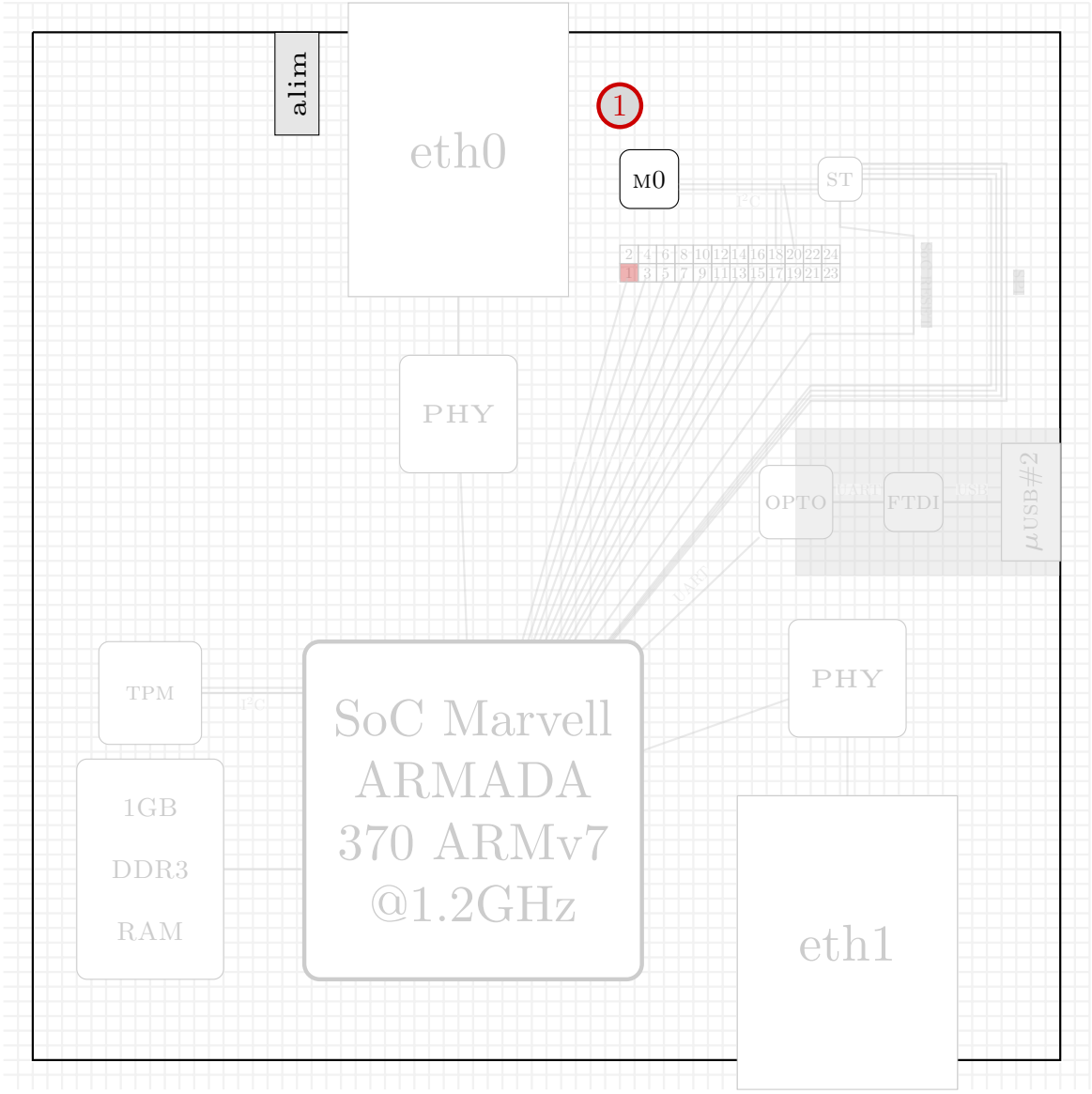

alim
RJ45
µUSB#0
USB
ESD
µUSB#1
USB
ESD
PHY
M0
I²C
ST
SoC RESET
SPI
2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23
USB
USB
FAN
RTC
TPM
I²C
OPTO
UART
FTDI
USB
µUSB#2
UART
SoC Marvell
ARMADA
370 ARMv7
@1.2GHz
PHY
1GB
DDR3
RAM
RJ45
L2 L1
L0


alim
RJ45
µUSB#0
USB
ESD
µUSB#1
USB
ESD
PHY
M0
I²C
ST
SoC RESET
SPI
2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23
USB
USB
FAN
RTC
TPM
I²C
OPTO
UART
FTDI
USB
µUSB#2
UART
PHY
SoC Marvell
ARMADA
370 ARMv7
@1.2GHz
1GB
DDR3
RAM
RJ45
L2 L1
L0


alim
RJ45
µUSB#0
USB
ESD
µUSB#1
USB
ESD
PHY
M0
I²C
ST
SoC RESET
SPI
2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23
FAN
RTC
TPM
I²C
USB
USB
UART
OPTO
UART
FTDI
USB
µUSB#2
SoC Marvell
ARMADA
370 ARMv7
@1.2GHz
1GB
DDR3
RAM
PHY
µSD
RJ45
Micro SD
L2 L1
L0

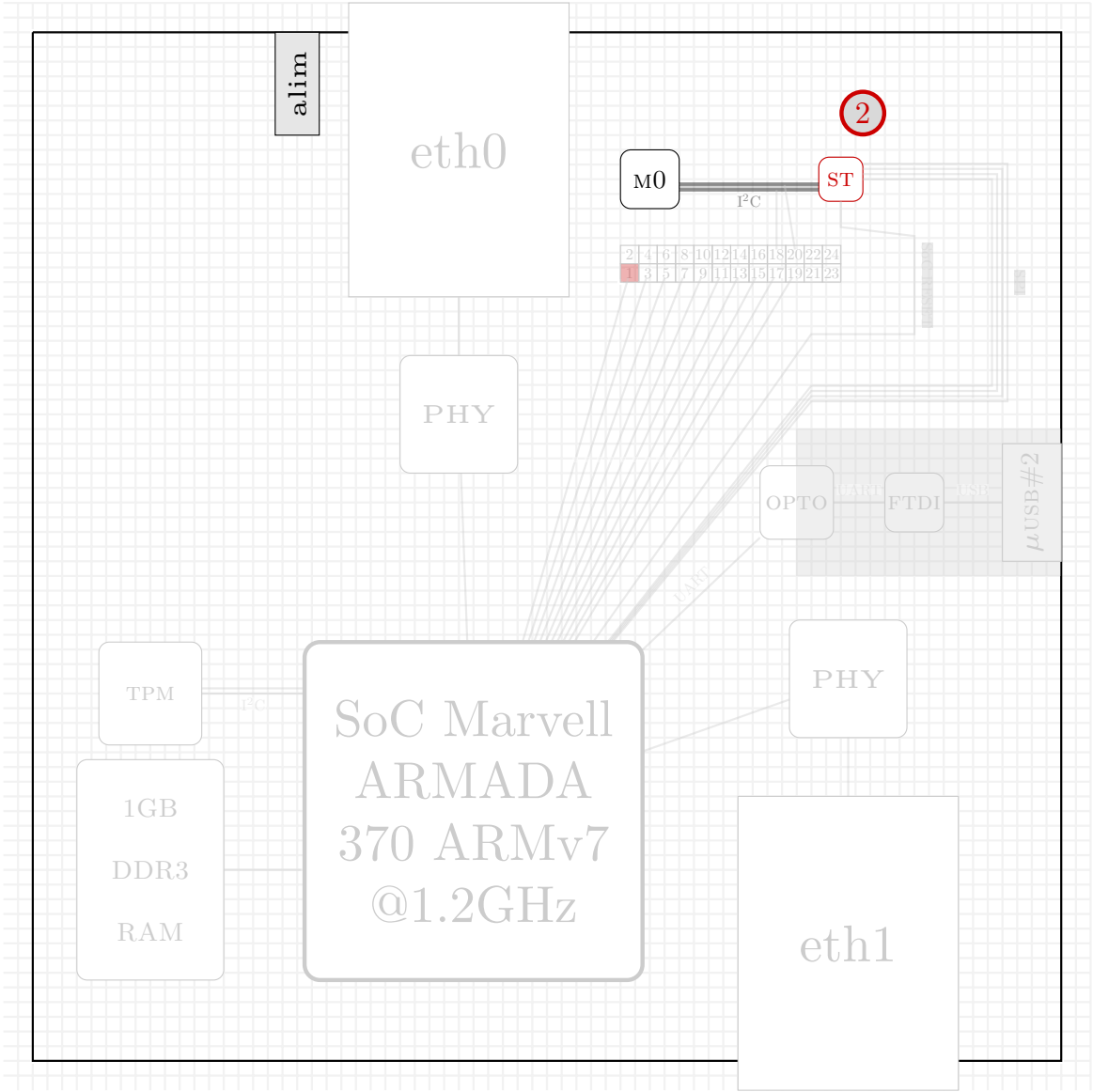

88F8710-A1
C120
HALO
HFJ11-1G41E-L12
1426RL


alim
eth0
M0
ST
I²C
2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23
PHY
OPTO
FTDI
µUSB#2
TPM
I²C
SoC Marvell
ARMADA
370 ARMv7
@1.2GHz
PHY
1GB
DDR3
RAM
eth1



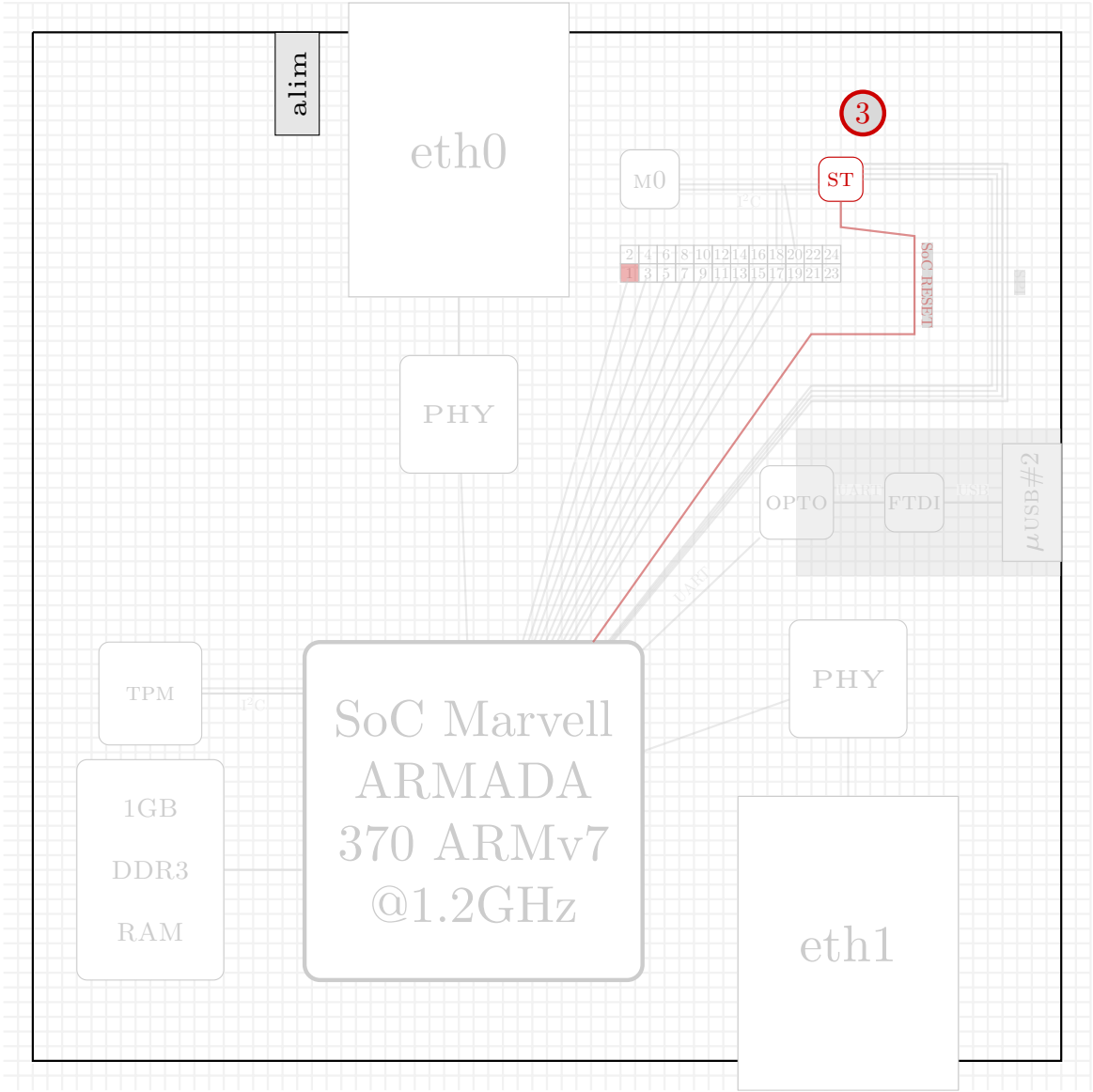
Logique de boot

1. Alimentation/démarrage du M0



Logique de boot

1. Alimentation/démarrage du M0
2. Alimentation/démarrage du ST33

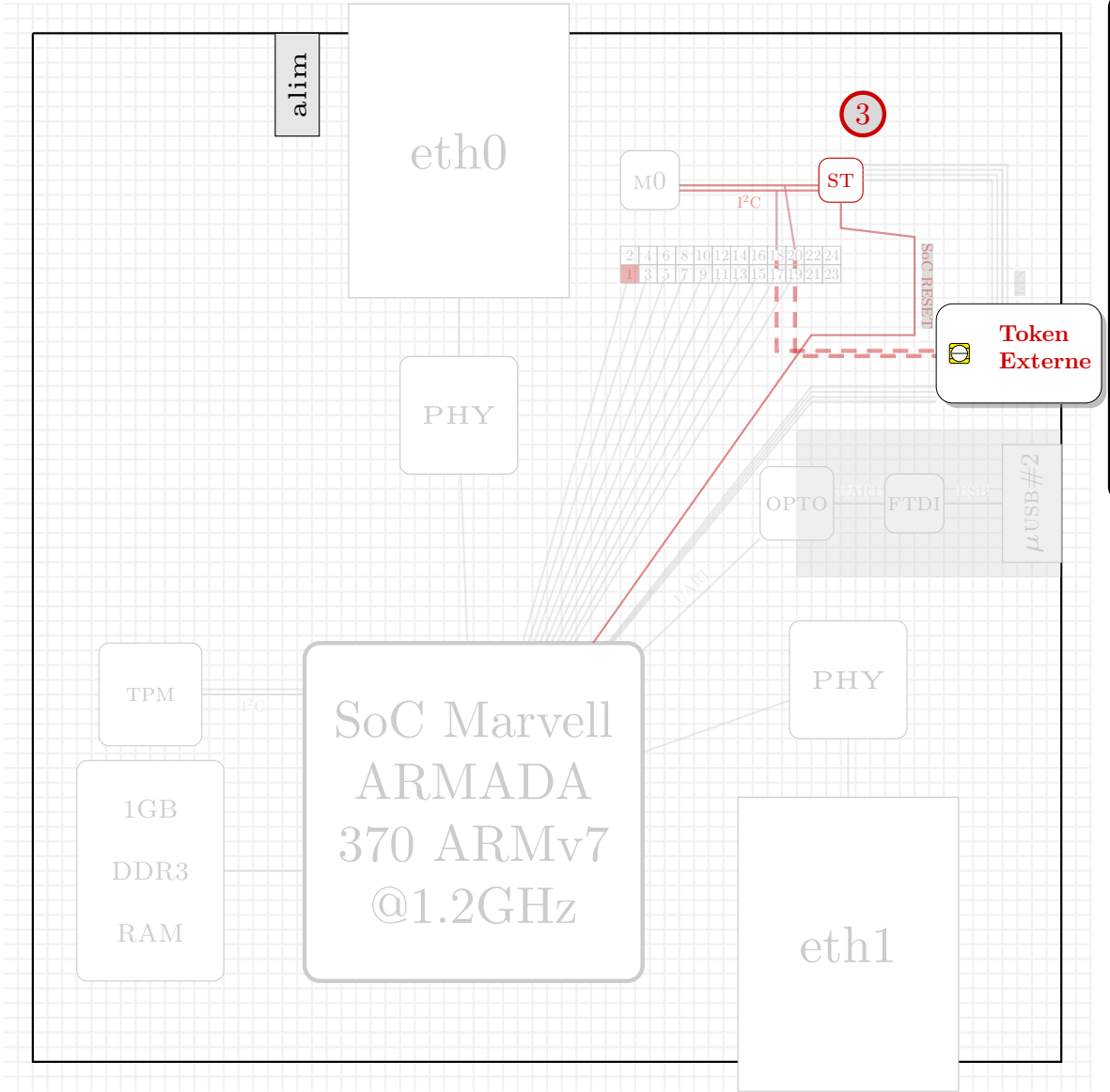


Logique de boot

1. Alimentation/démarrage du M0

2. Alimentation/démarrage du ST33

3.
   - SoC maintenu sous *reset* par le ST33
   - Vérifications par le ST33 avant levée du *reset* : intégrité

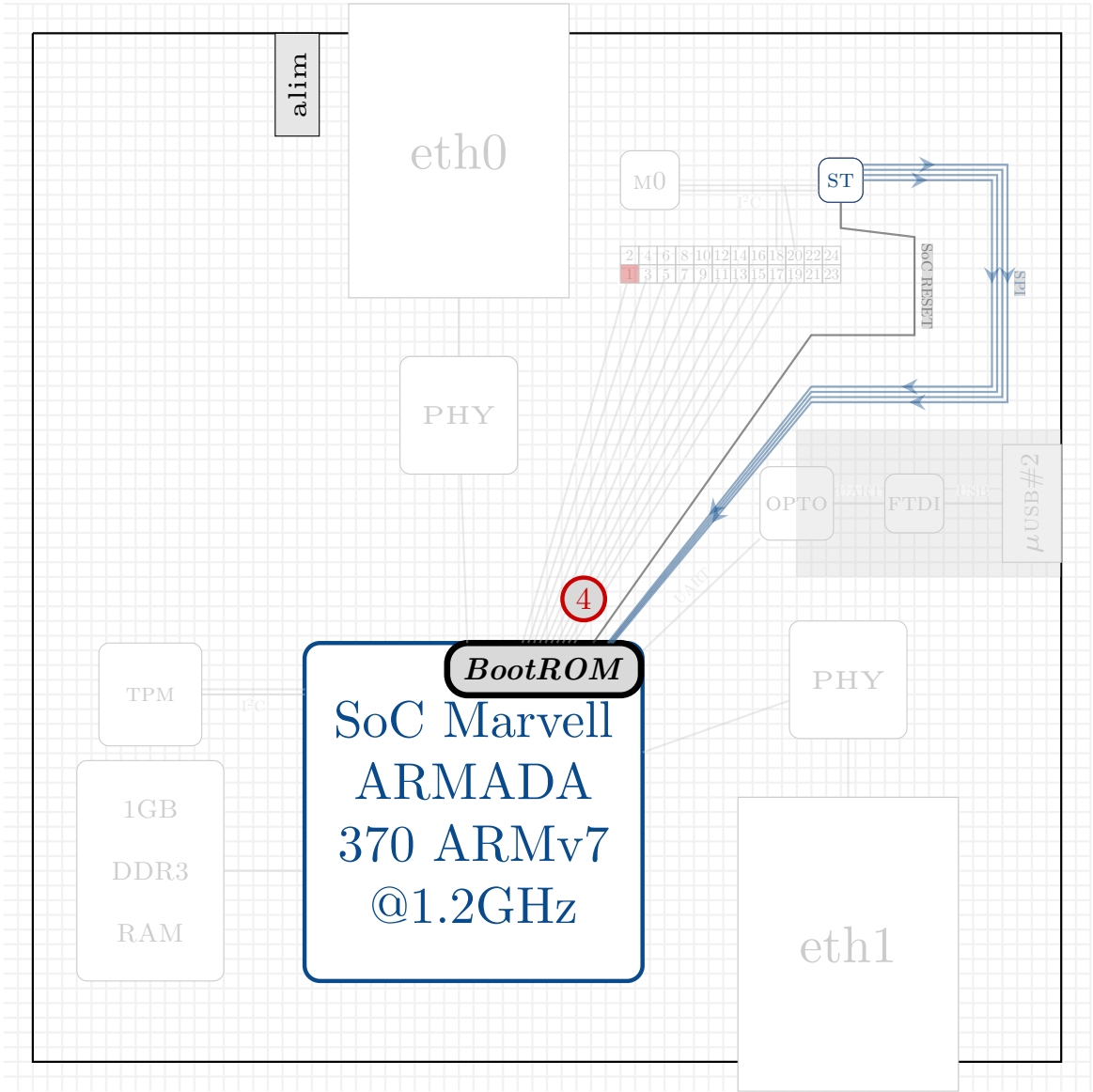


Logique de boot

1. Alimentation/démarrage du M0

2. Alimentation/démarrage du ST33

3.
   - SoC maintenu sous *reset* par le ST33
   - Vérifications par le ST33 avant levée du *reset* : intégrité, authentification pré-boot



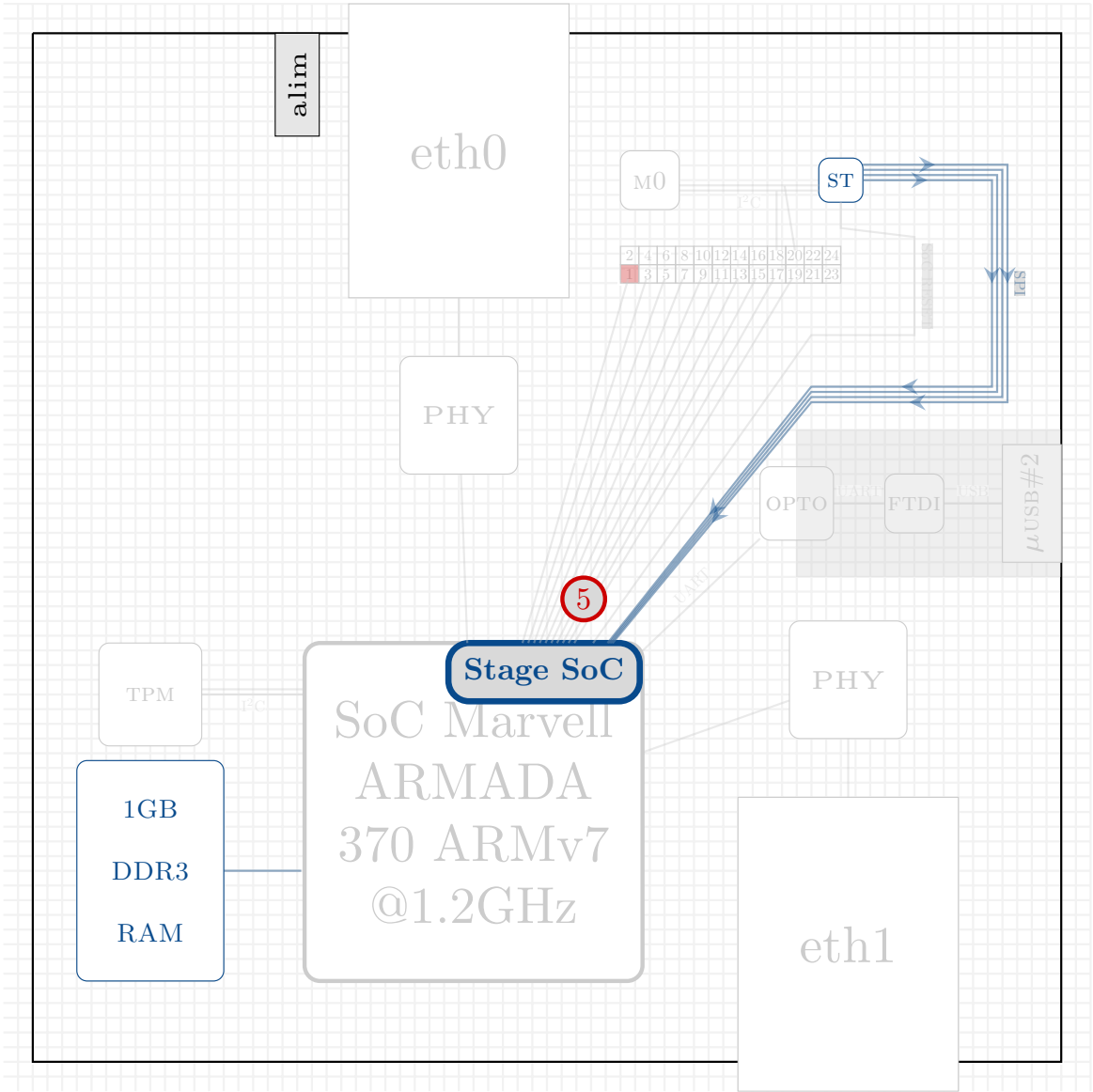
Logique de boot

1. Alimentation/démarrage du M0

2. Alimentation/démarrage du ST33

3.
   - SoC maintenu sous *reset* par le ST33
   - Vérifications par le ST33 avant levée du *reset* : intégrité, authentification pré-boot

4. Envoi Stage SoC via le bus SPI



Logique de boot

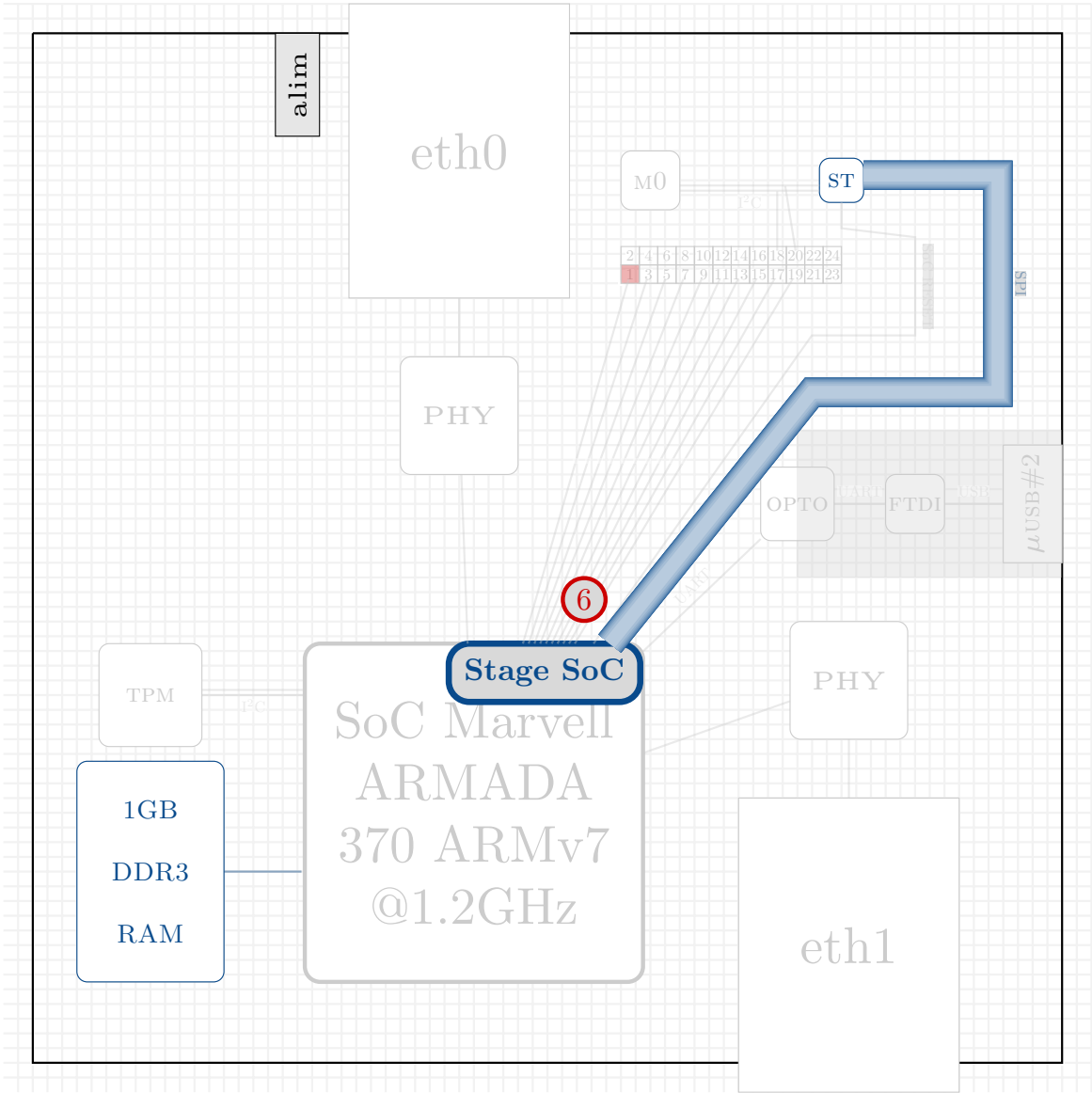
1. Alimentation/démarrage du M0

2. Alimentation/démarrage du ST33

3.
   - SoC maintenu sous *reset* par le ST33
   - Vérifications par le ST33 avant levée du *reset* : intégrité, authentification pré-boot

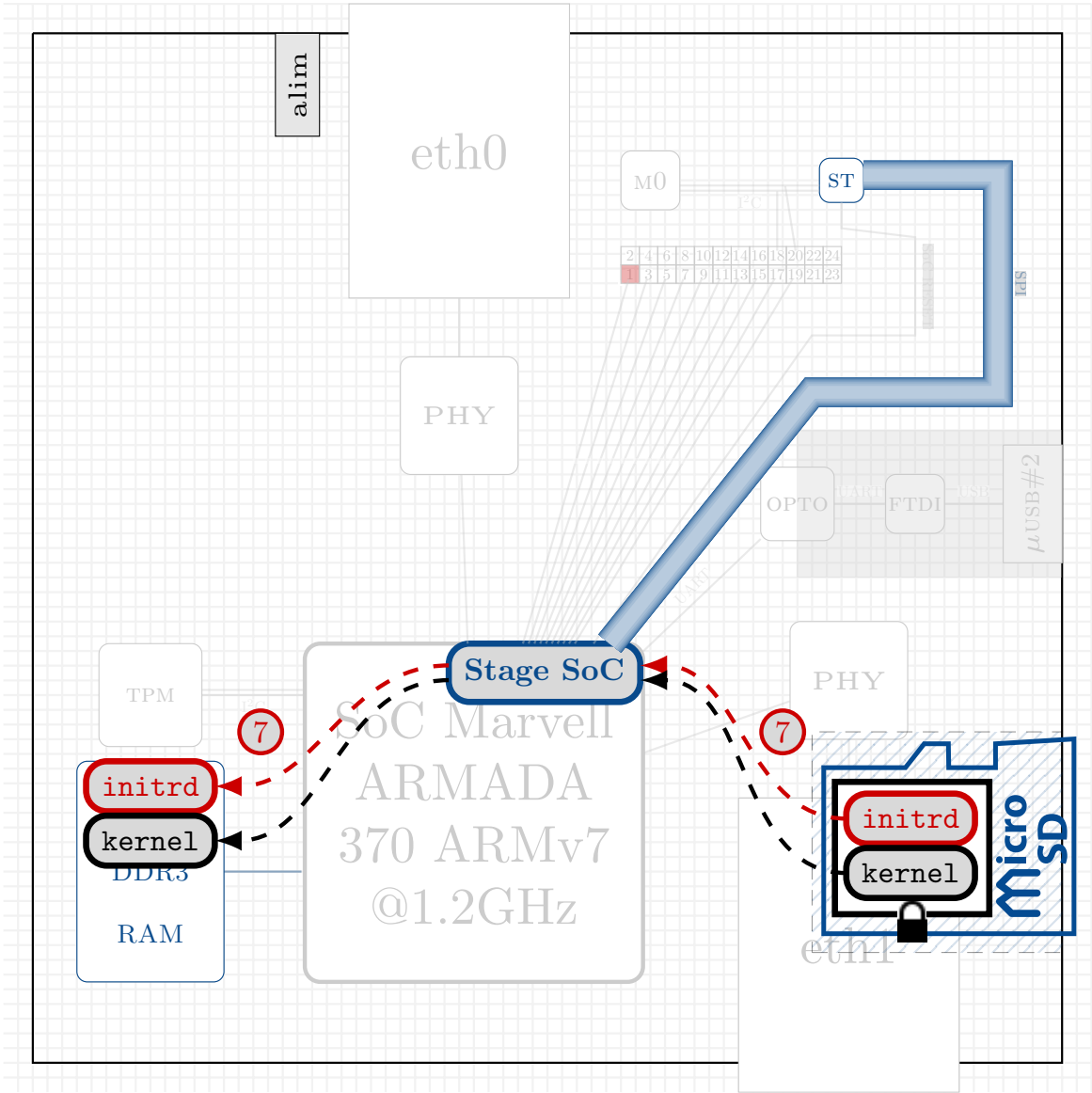
4. Envoi Stage SoC via le bus SPI

5. Exécution par la *bootROM*



Logique de boot

1. Alimentation/démarrage du M0
2. Alimentation/démarrage du ST33
3.
   - SoC maintenu sous *reset* par le ST33
   - Vérifications par le ST33 avant levée du *reset* : intégrité, authentification pré-boot
4. Envoi Stage SoC via le bus SPI
5. Exécution par la *bootROM*
6. Négociation canal sécurisé ST33↔SoC



Logique de boot

1. Alimentation/démarrage du M0

2. Alimentation/démarrage du ST33

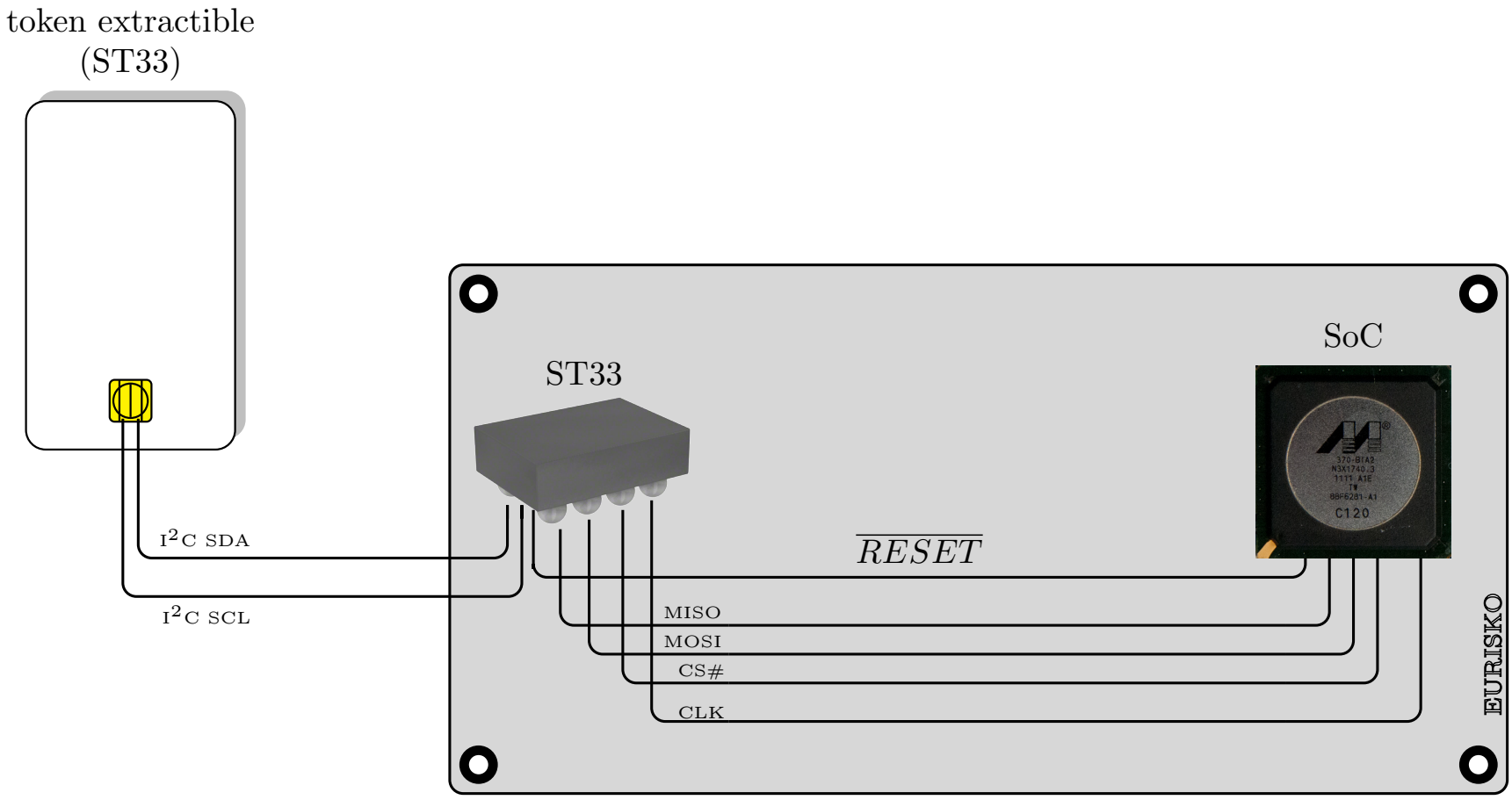
3.
   - SoC maintenu sous *reset* par le ST33
   - Vérifications par le ST33 avant levée du *reset* : intégrité, authentification pré-boot

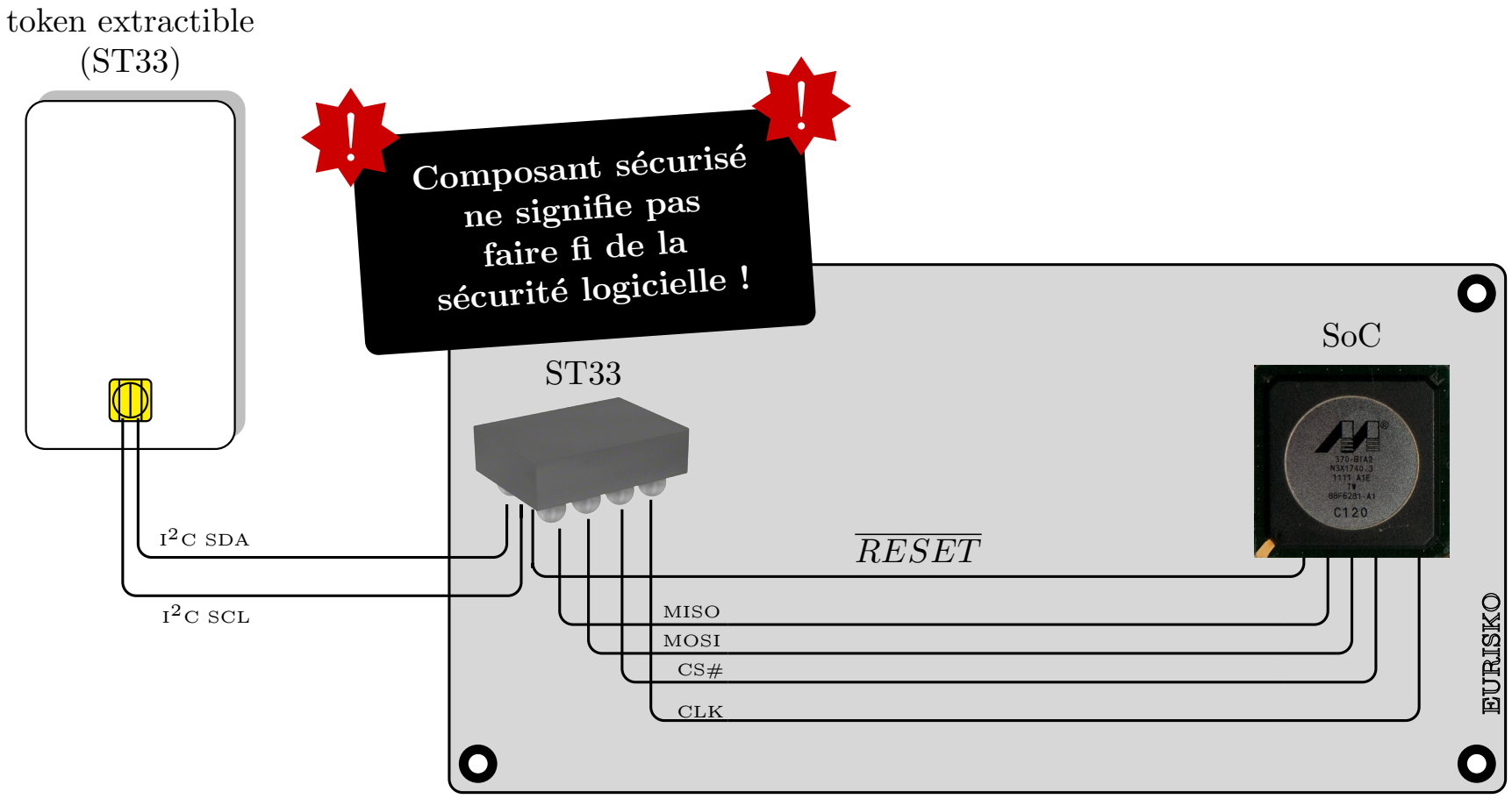
4. Envoi Stage SoC via le bus SPI

5. Exécution par la *bootROM*

6. Négociation canal sécurisé ST33↔SoC

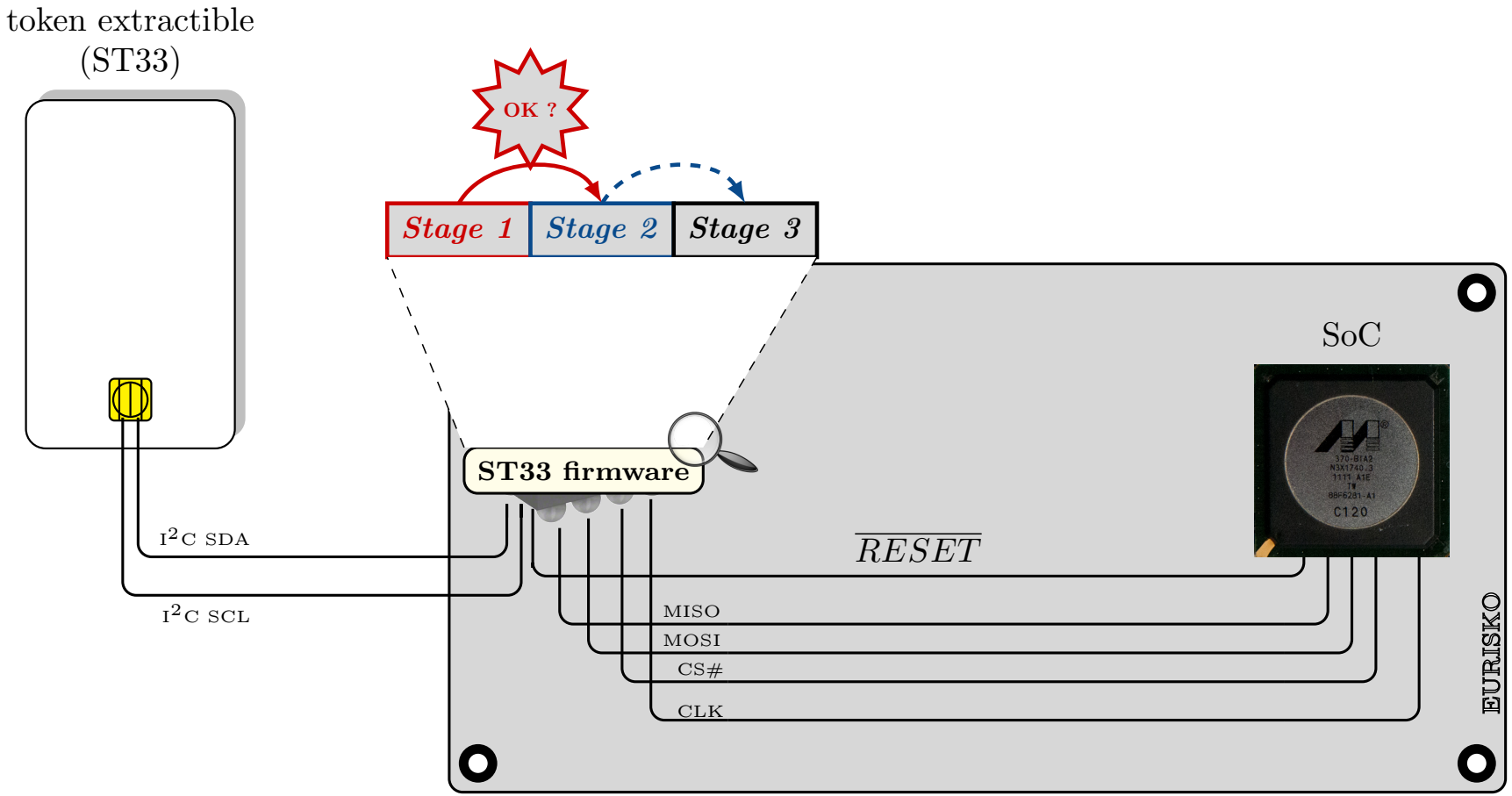
7. Déverrouillage de la plateforme :
   - Reconstruction de la clé de déchiffrement du second *stage*/noyau linux
   - Déchiffrement en RAM depuis la carte SD et exécution


token extractible
(ST33)
ST33
SoC
I²C SDA
I²C SCL
RESET
MISO
MOSI
CS#
CLK
EURISKO


token extractible
(ST33)
Composant sécurisé
ne signifie pas
faire fi de la
sécurité logicielle !
ST33
SoC
I²C SDA
I²C SCL
RESET
MISO
MOSI
CS#
CLK
EURISKO

Défense en profondeur OS

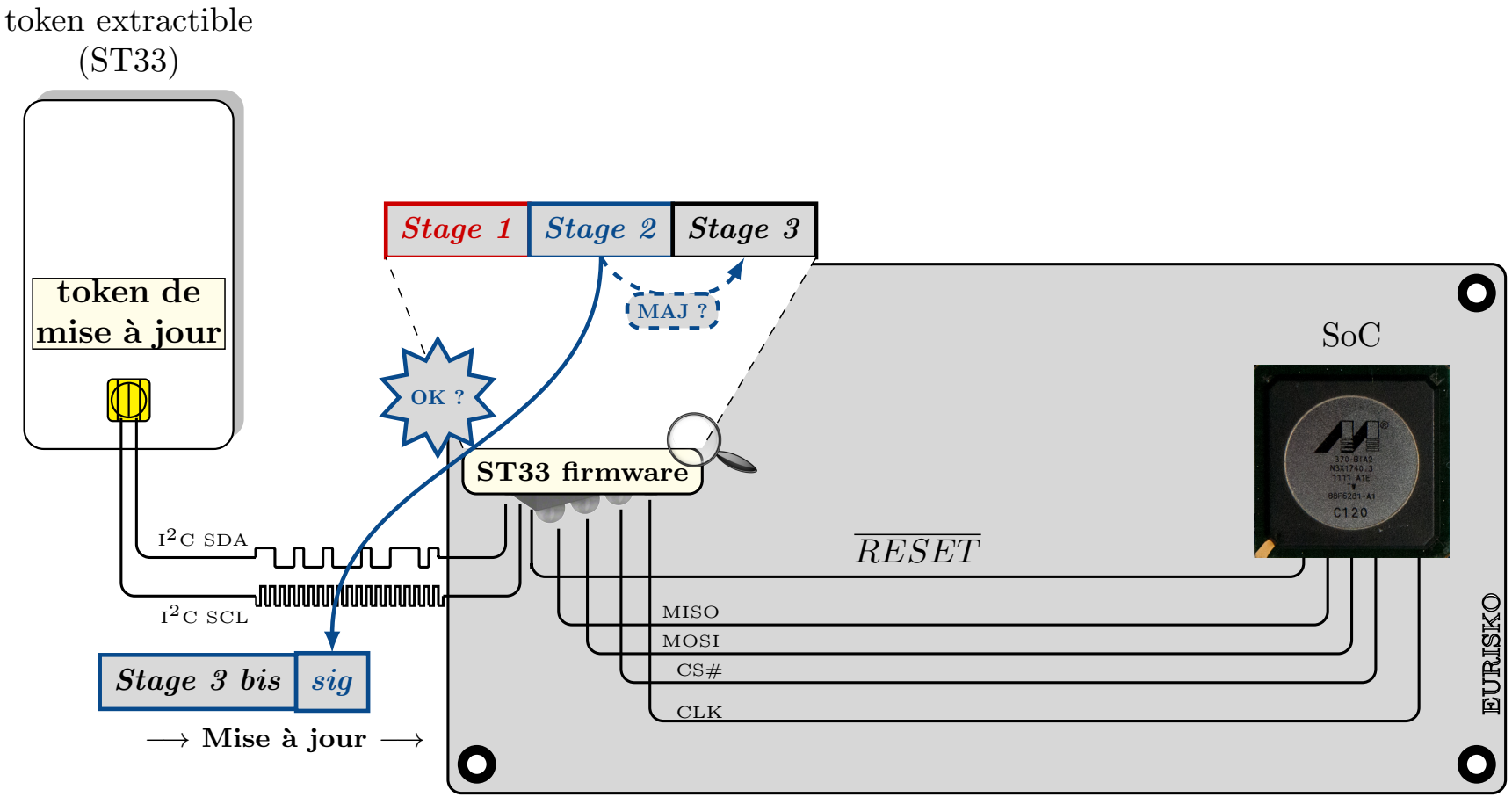
ST33 : démarrage *bare metal* en **plusieurs stages** qui se vérifient les uns les autres



Défense en profondeur OS

ST33 : démarrage *bare metal* en **plusieurs stages** qui se vérifient les uns les autres

ST33 : **mises à jour** signées et gérées par des *stages* dédiés

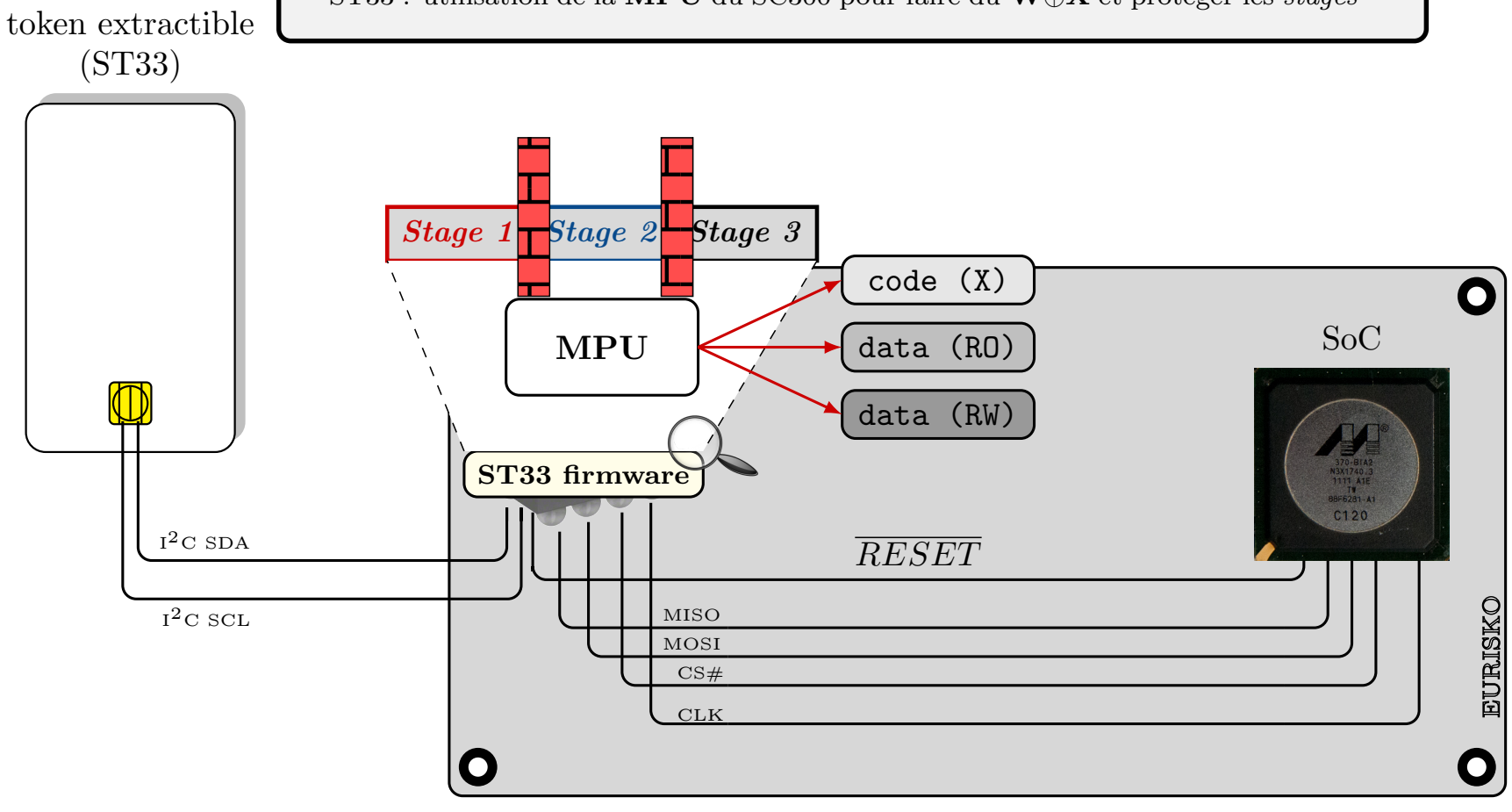


Défense en profondeur OS

ST33 : démarrage *bare metal* en **plusieurs stages** qui se vérifient les uns les autres

ST33 : **mises à jour** signées et gérées par des *stages* dédiés

ST33 : utilisation de la **MPU** du SC300 pour faire du **W⊕X** et protéger les *stages*



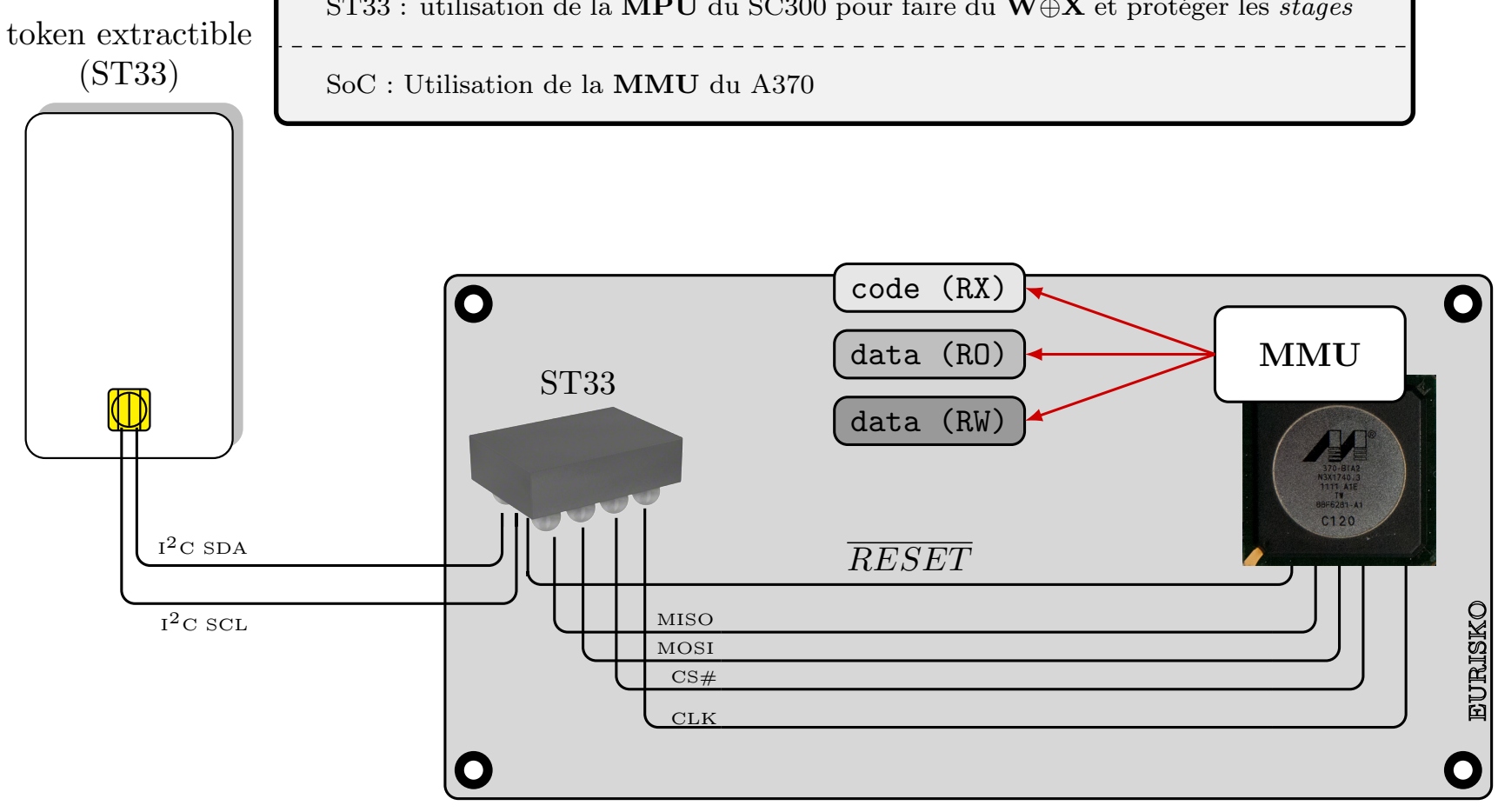
Défense en profondeur OS

ST33 : démarrage *bare metal* en **plusieurs stages** qui se vérifient les uns les autres

ST33 : **mises à jour** signées et gérées par des *stages* dédiés

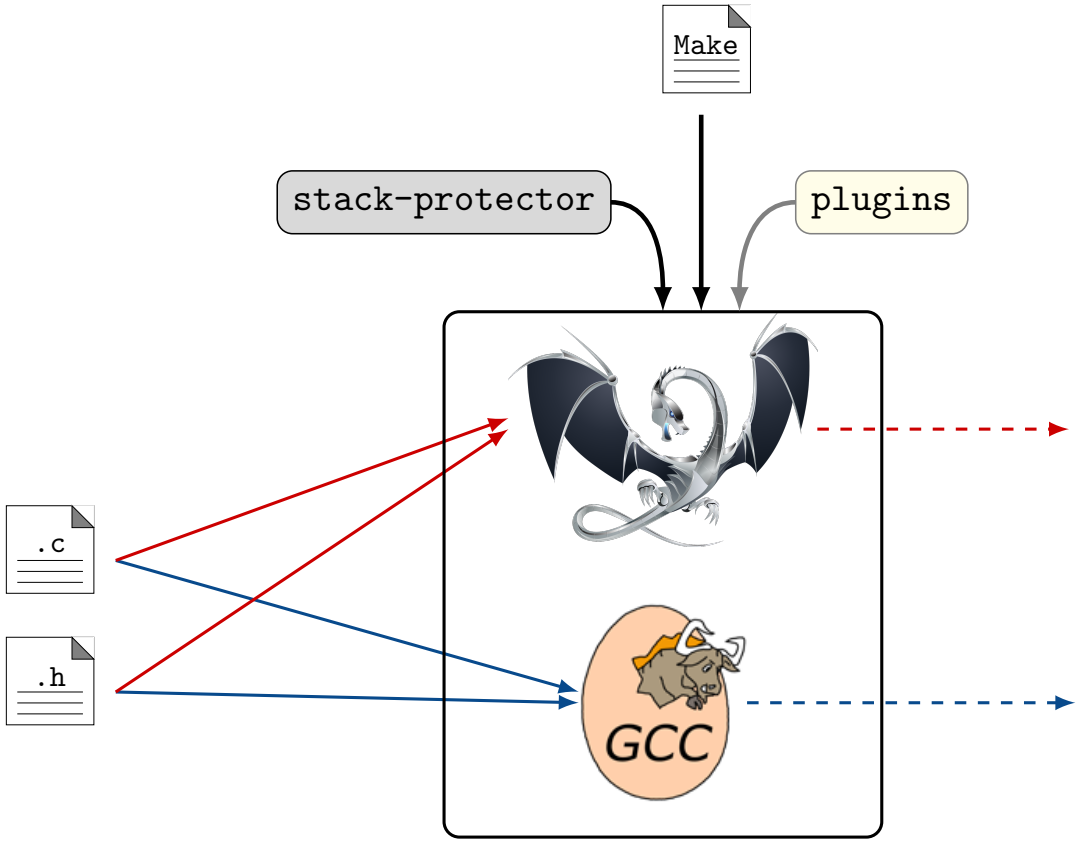
ST33 : utilisation de la **MPU** du SC300 pour faire du **W⊕X** et protéger les *stages*

SoC : Utilisation de la **MMU** du A370



Maîtrise et protection du code

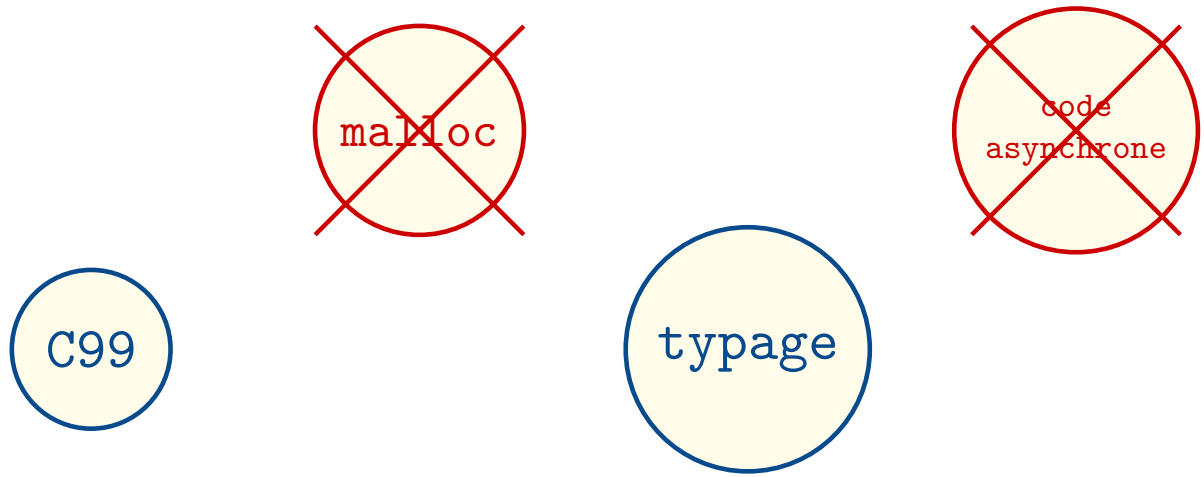
Utilisation de **toolchains diverses et maîtrisées** (gcc, clang, ...)



Maîtrise et protection du code

Utilisation de **toolchains diverses et maîtrisées** (gcc, clang, ...)

Règles de code : C99, pas d'allocation dynamique, typage du mieux que possible, code linéaire/synchrone, ...

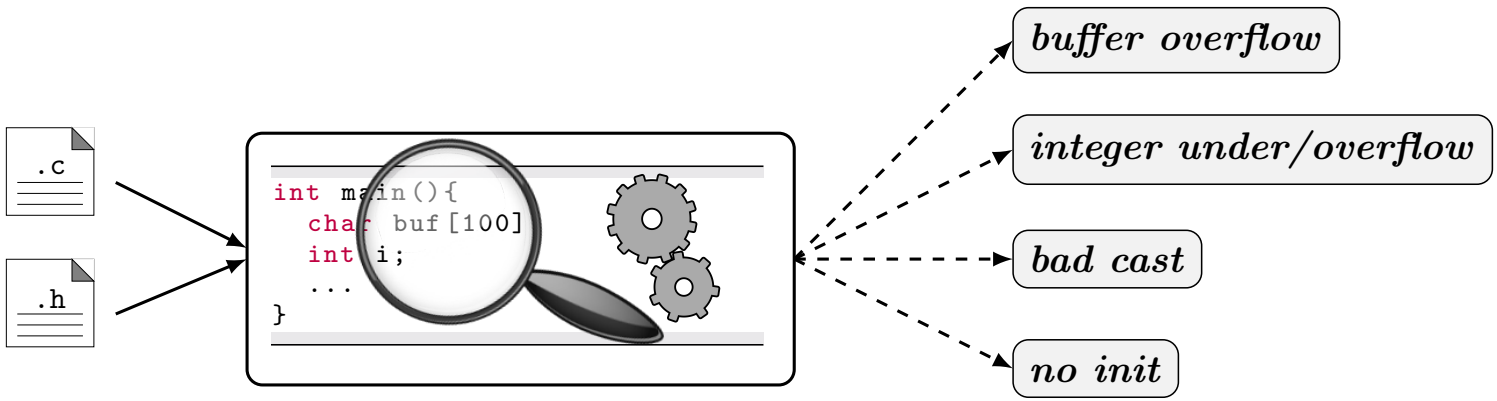


Maîtrise et protection du code

Utilisation de **toolchains diverses et maîtrisées** (gcc, clang, ...)

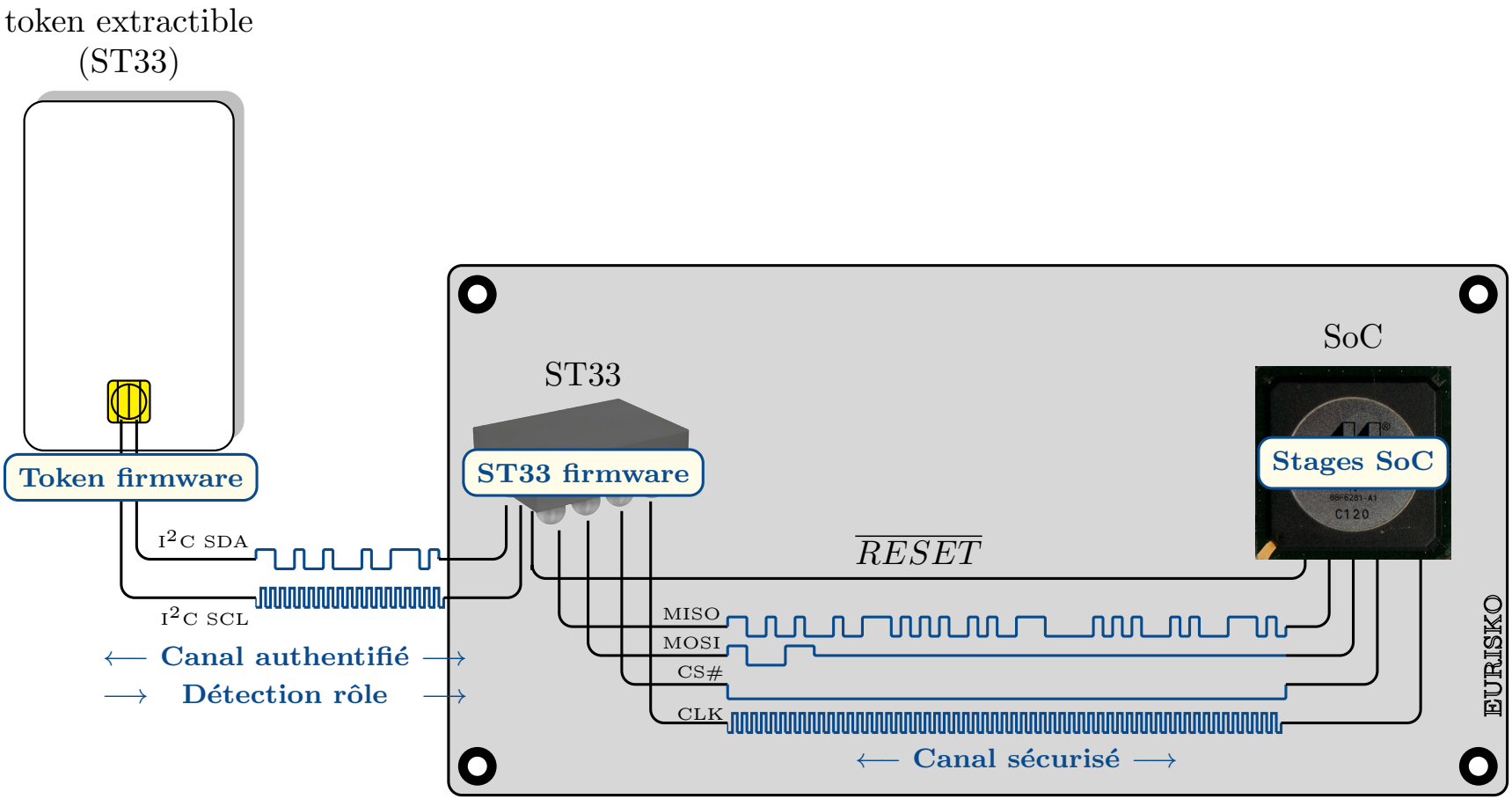
Règles de code : C99, pas d'allocation dynamique, typage du mieux que possible, code linéaire/synchrone, ...

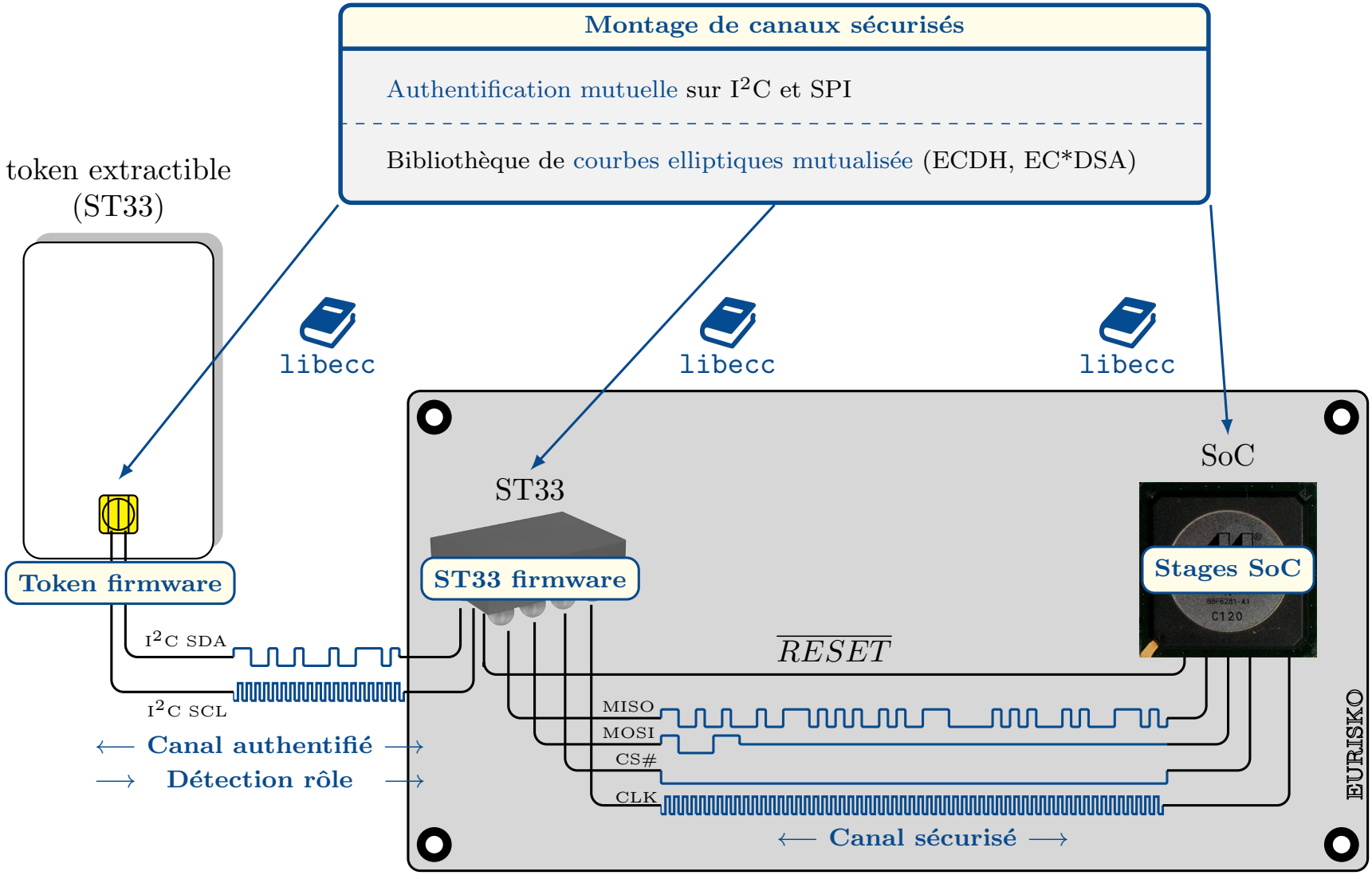
Utilisation d'outils **d'analyse statique de code**



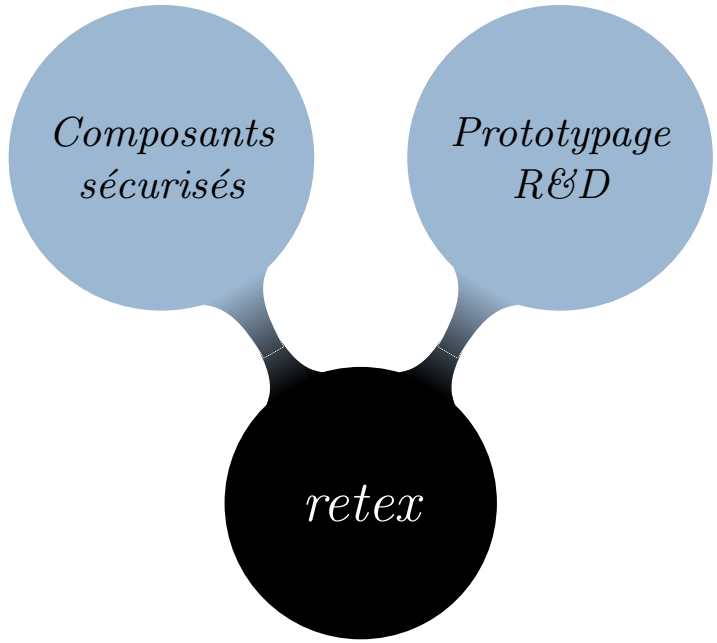
Montage de canaux sécurisés

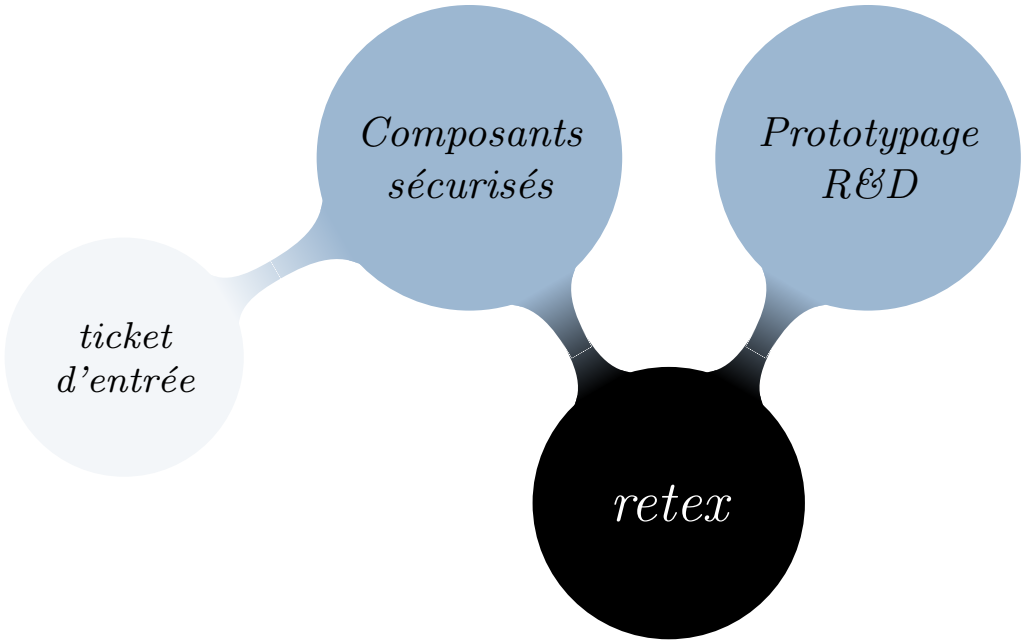
Authentification mutuelle sur I²C et SPI

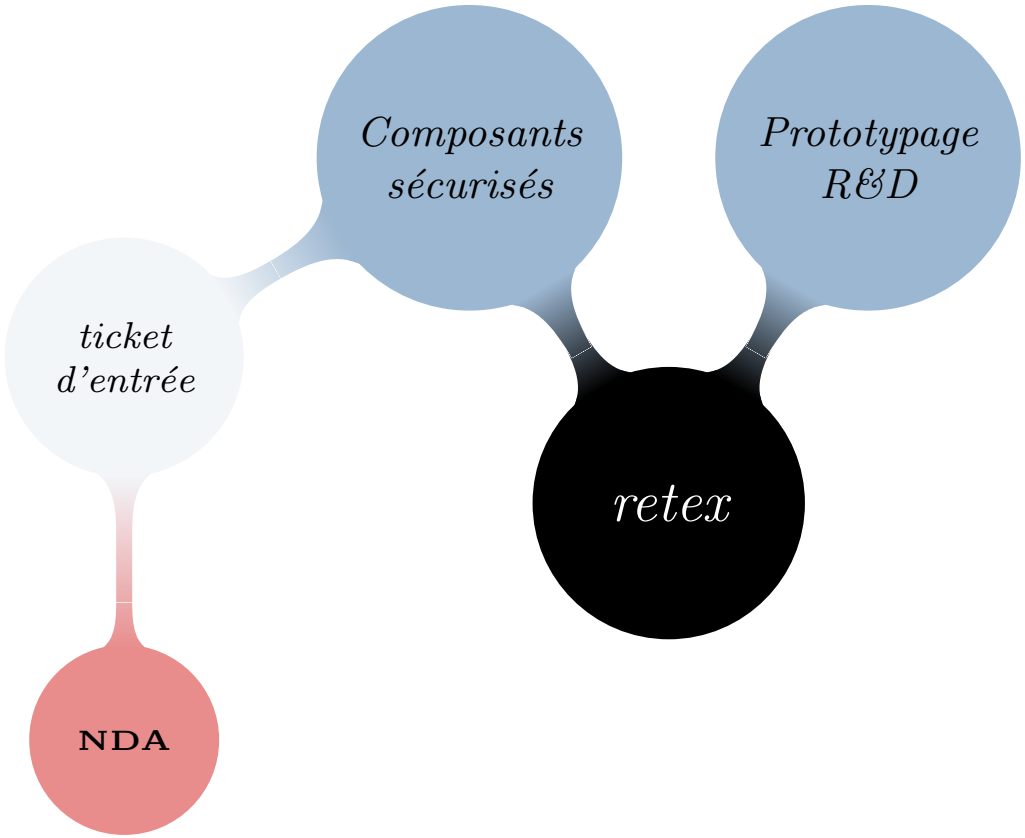


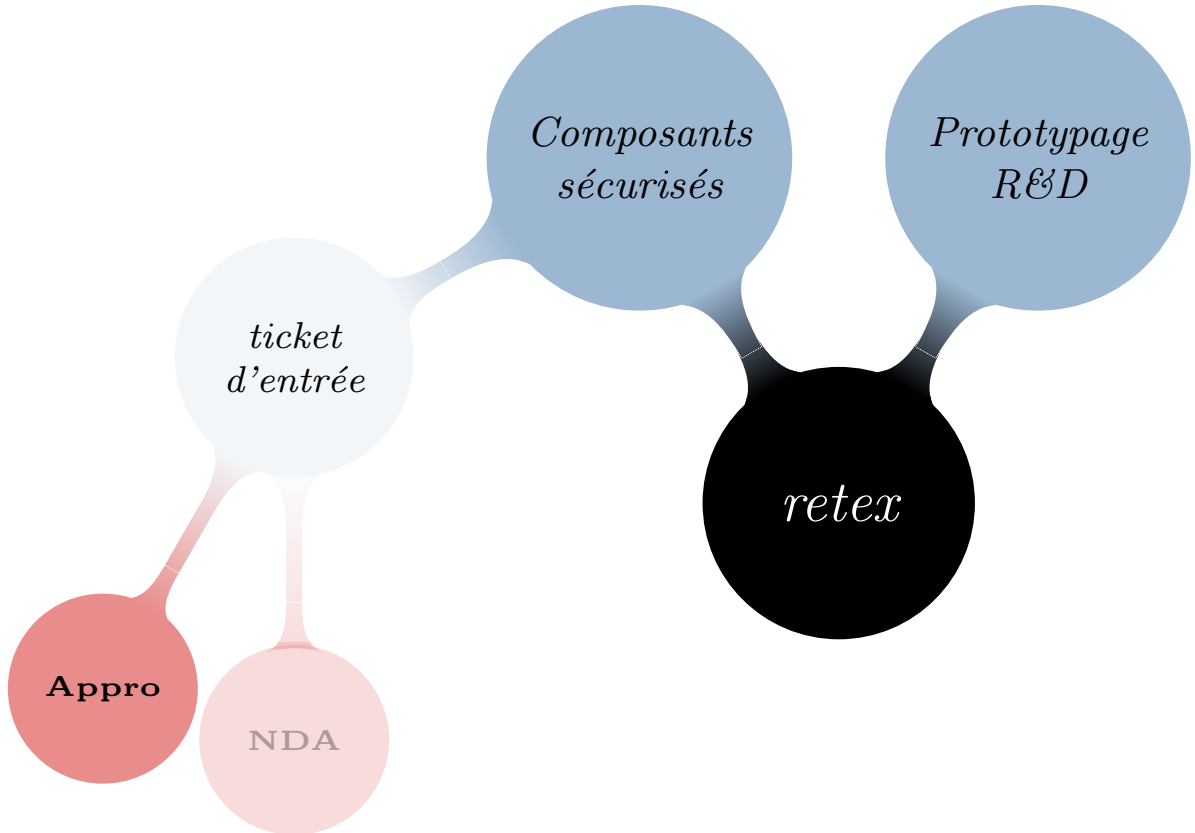

Montage de canaux sécurisés
Authentification mutuelle sur I²C et SPI
Bibliothèque de courbes elliptiques mutualisée (ECDH, EC*DSA)
token extractible
(ST33)
libecc
libecc
libecc
ST33
SoC
Token firmware
ST33 firmware
Stages SoC
I²C SDA
I²C SCL
RESET
MISO
MOSI
CS#
CLK
⟵ Canal authentifié ⟶
⟶ Détection rôle ⟶
⟵ Canal sécurisé ⟶
EURISKO

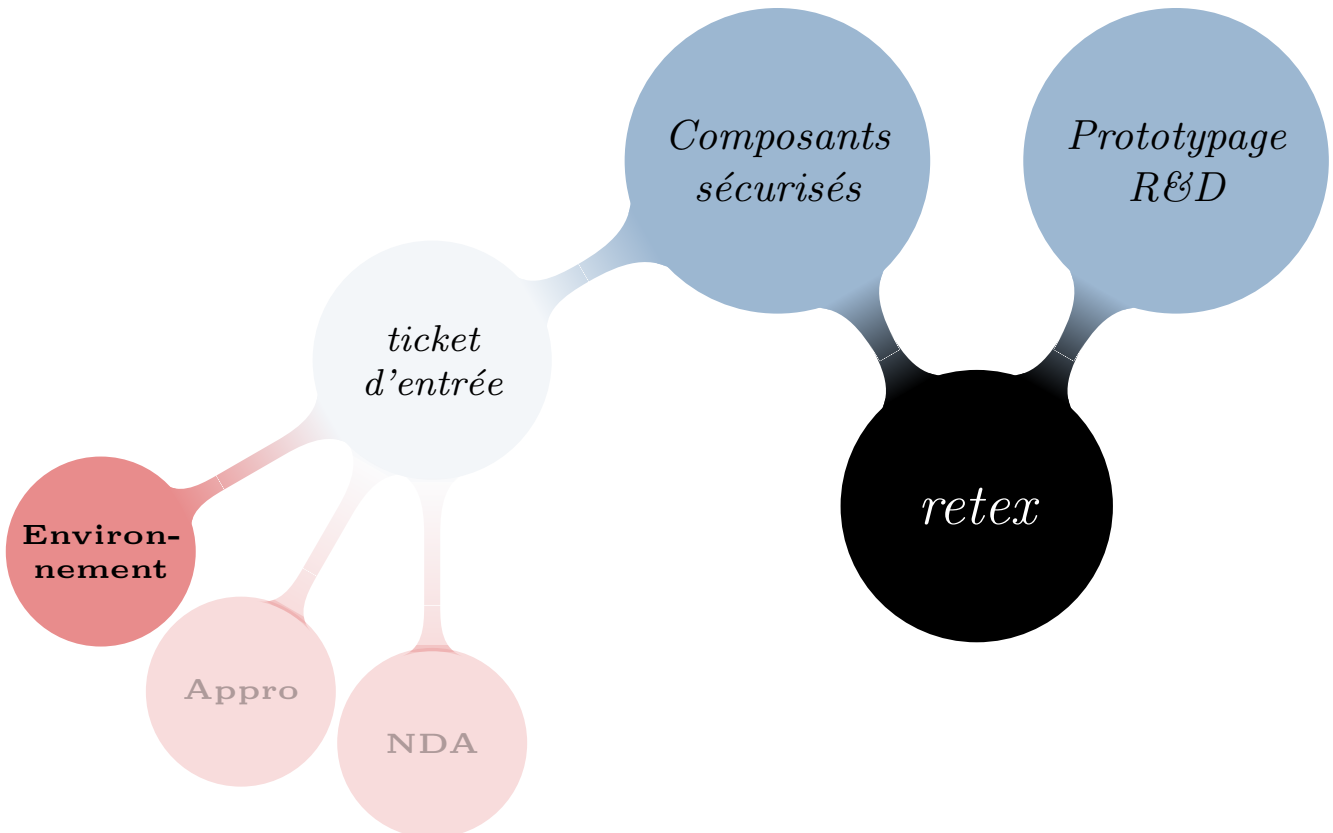

retex

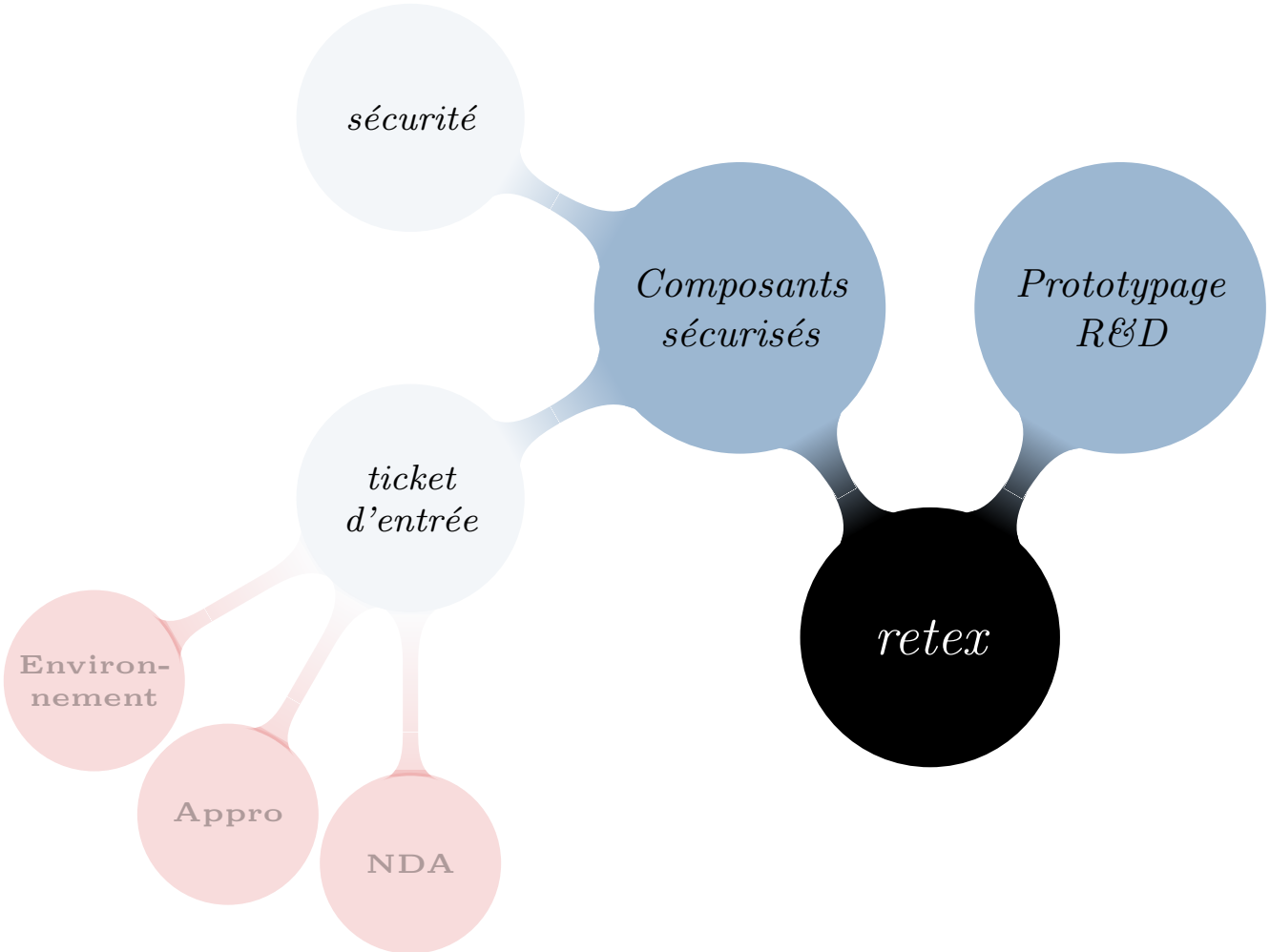

Composants sécurisés
Prototypage R&D
retex

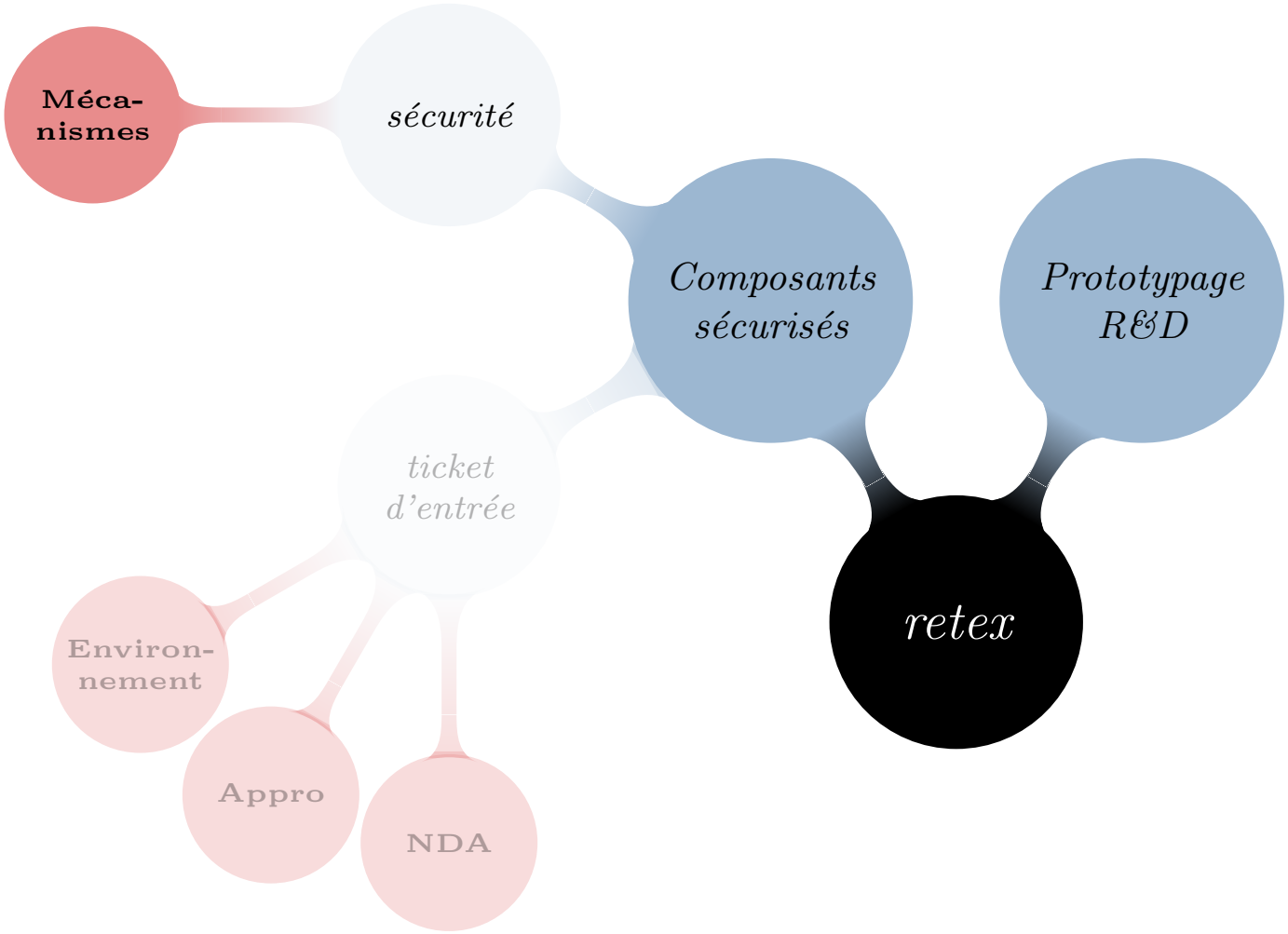

Composants sécurisés
Prototypage R&D
ticket d'entrée
retex

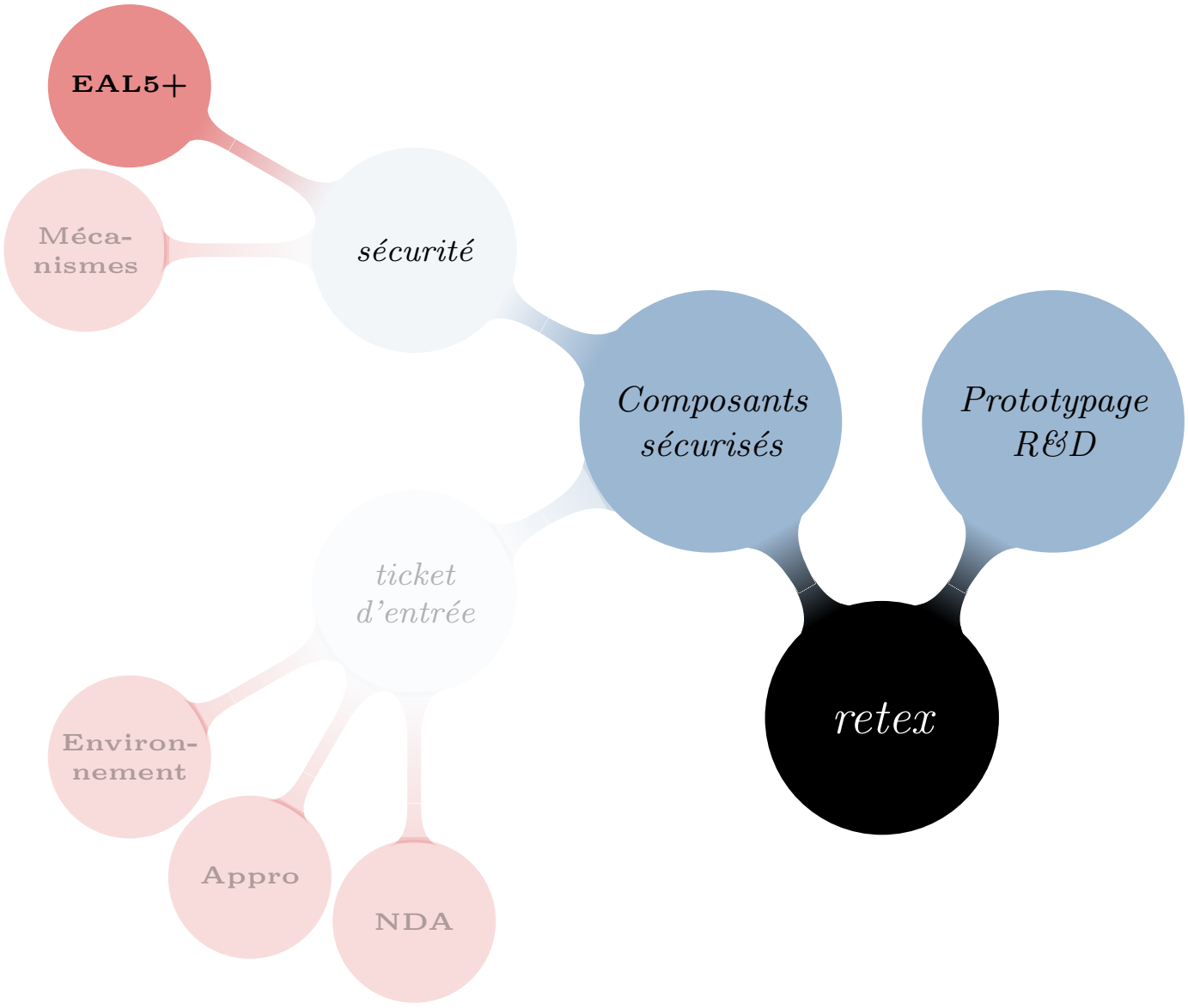

Composants sécurisés
Prototypage R&D
ticket d'entrée
retex
NDA

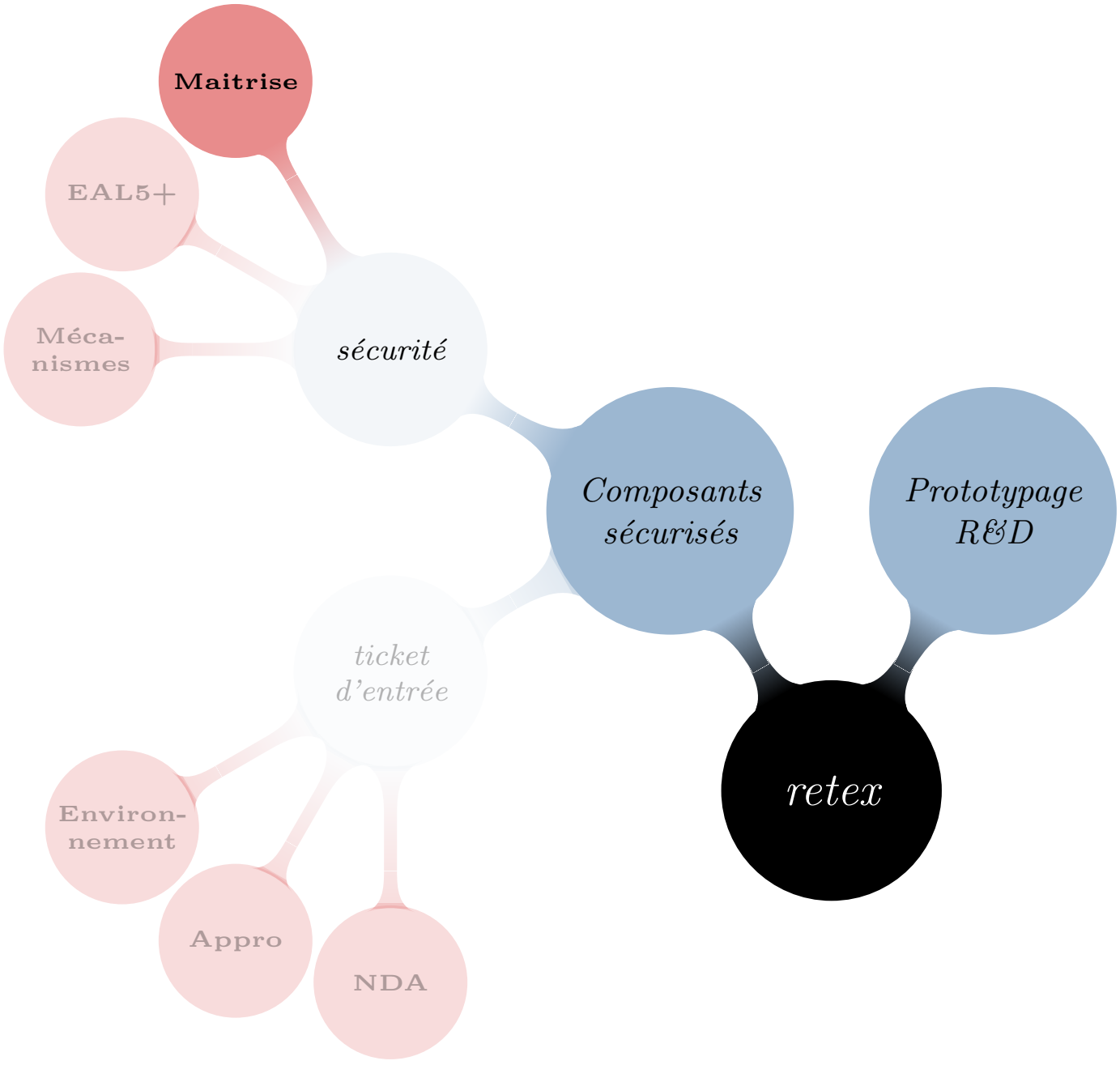

Composants sécurisés
Prototypage R&D
ticket d'entrée
retex
Appro
NDA

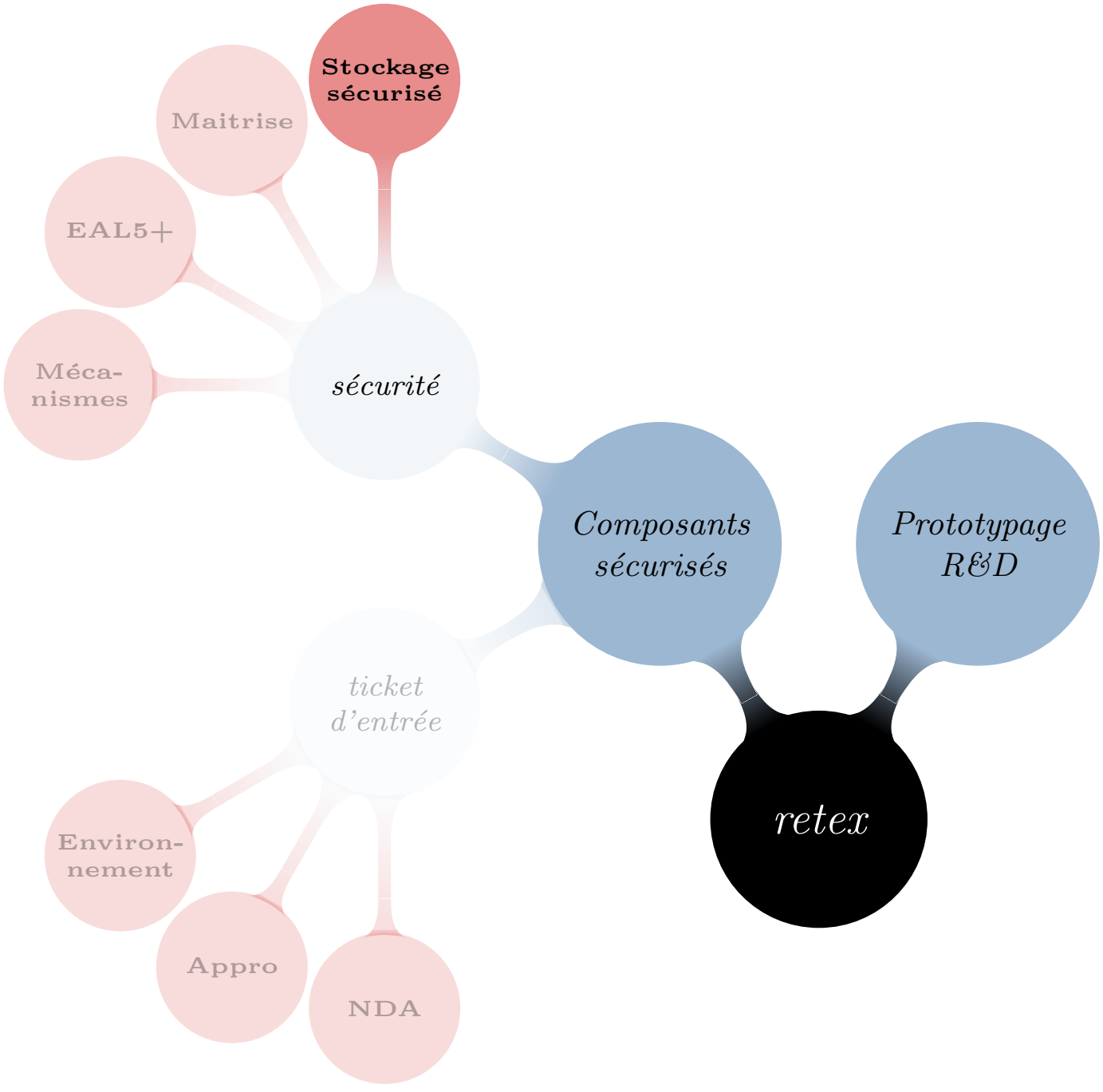

Composants sécurisés
Prototypage R&D
ticket d'entrée
retex
Environ-nement
Appro
NDA

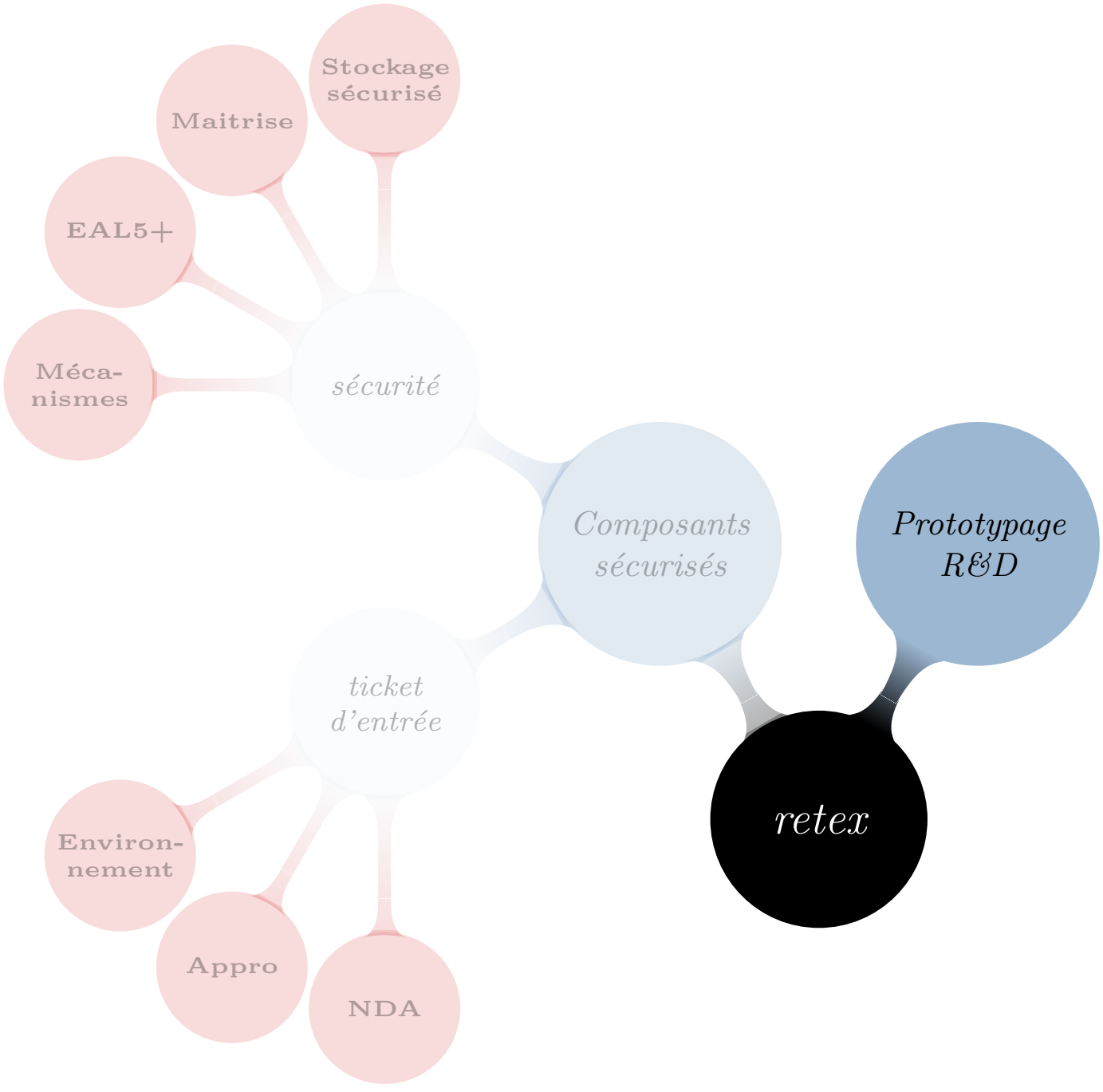

sécurité
Composants sécurisés
Prototypage R&D
ticket d'entrée
retex
Environ-nement
Appro
NDA

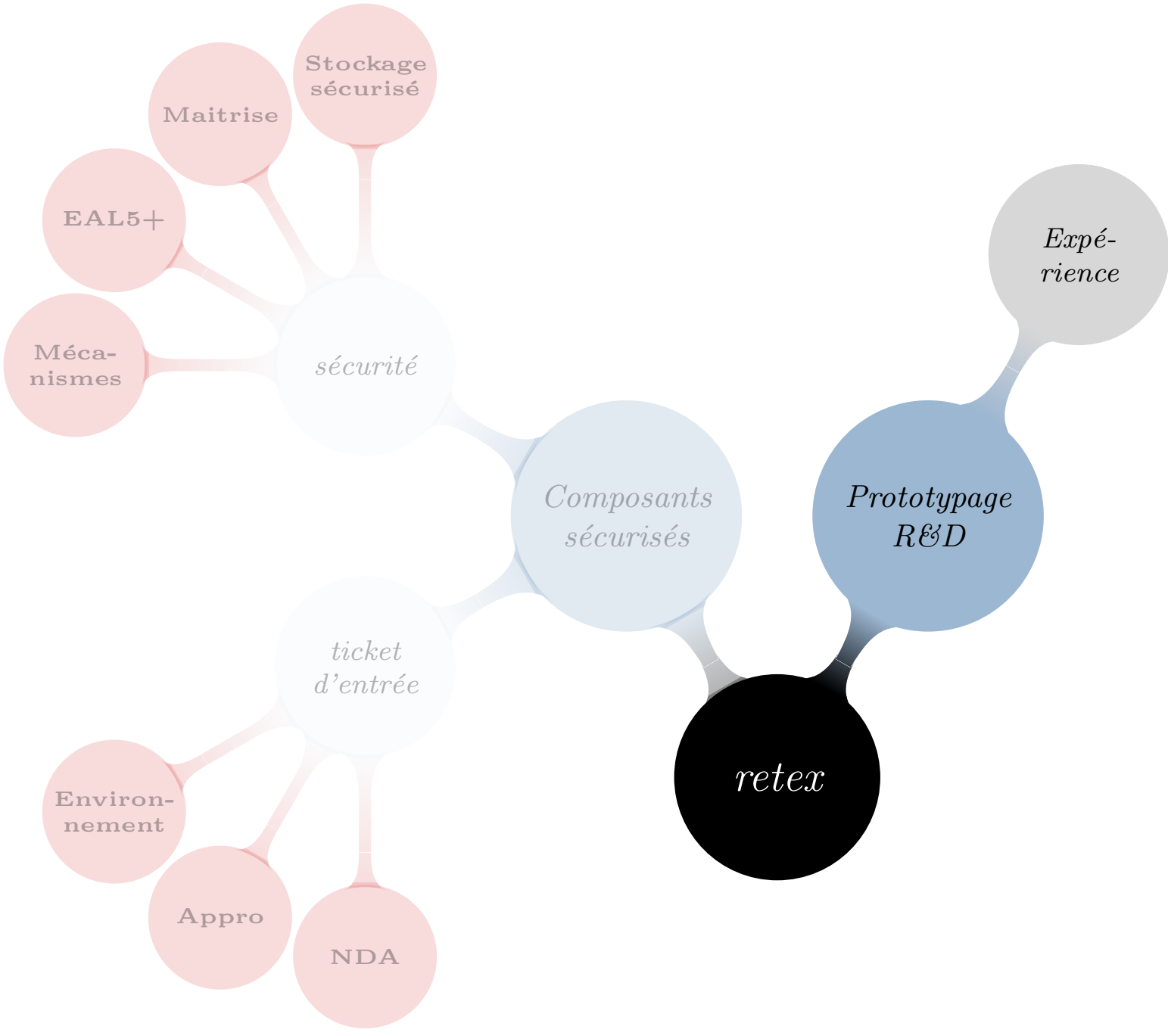

Méca-
nismes
sécurité
Composants
sécurisés
Prototypage
R&D
ticket
d'entrée
retex
Environ-
nement
Appro
NDA

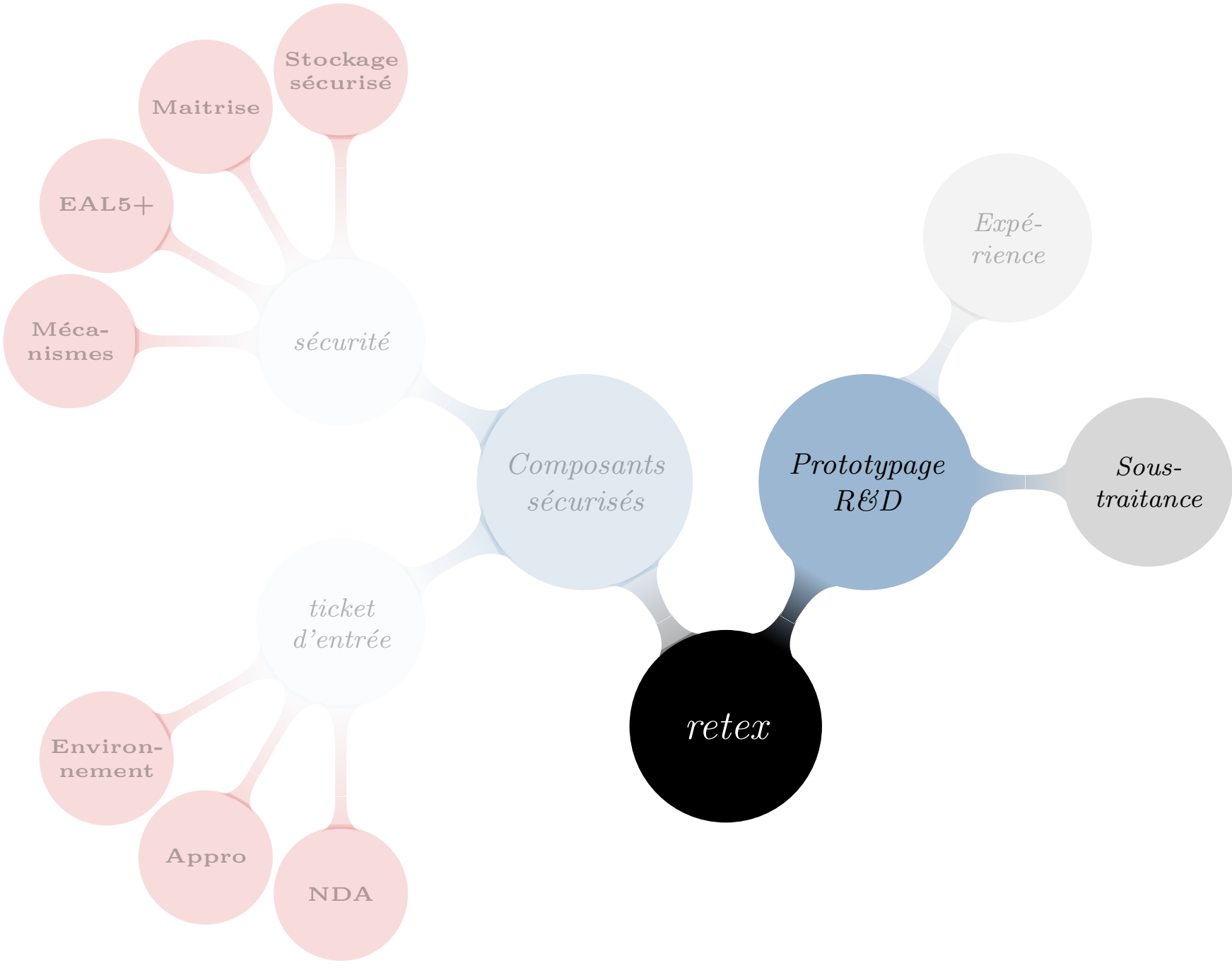

EAL5+
Méca-
nismes
sécurité
Composants
sécurisés
Prototypage
R&D
ticket
d'entrée
retex
Environ-
nement
Appro
NDA

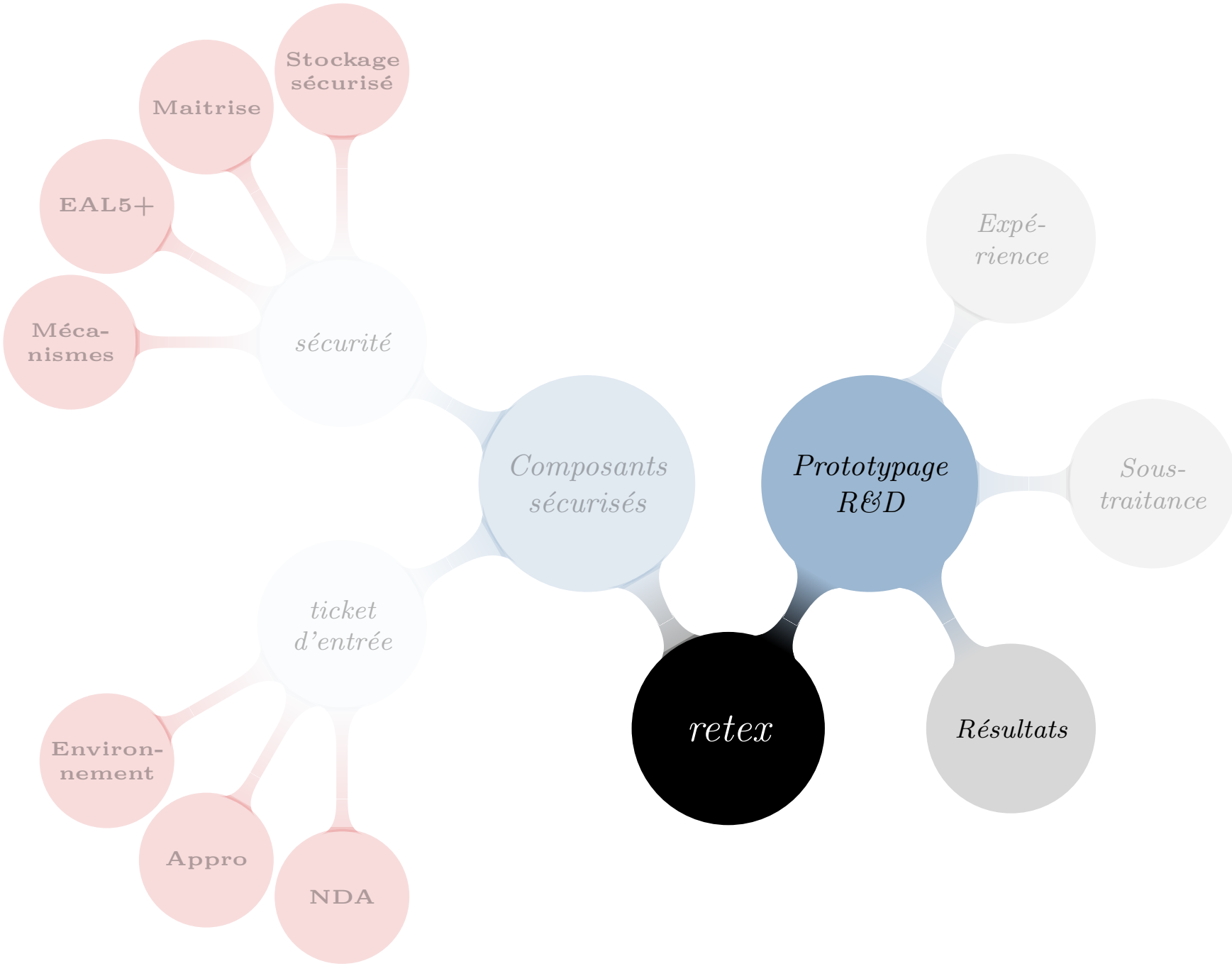

Maitrise
EAL5+
Méca-
nismes
sécurité
Composants
sécurisés
Prototypage
R&D
ticket
d'entrée
retex
Environ-
nement
Appro
NDA

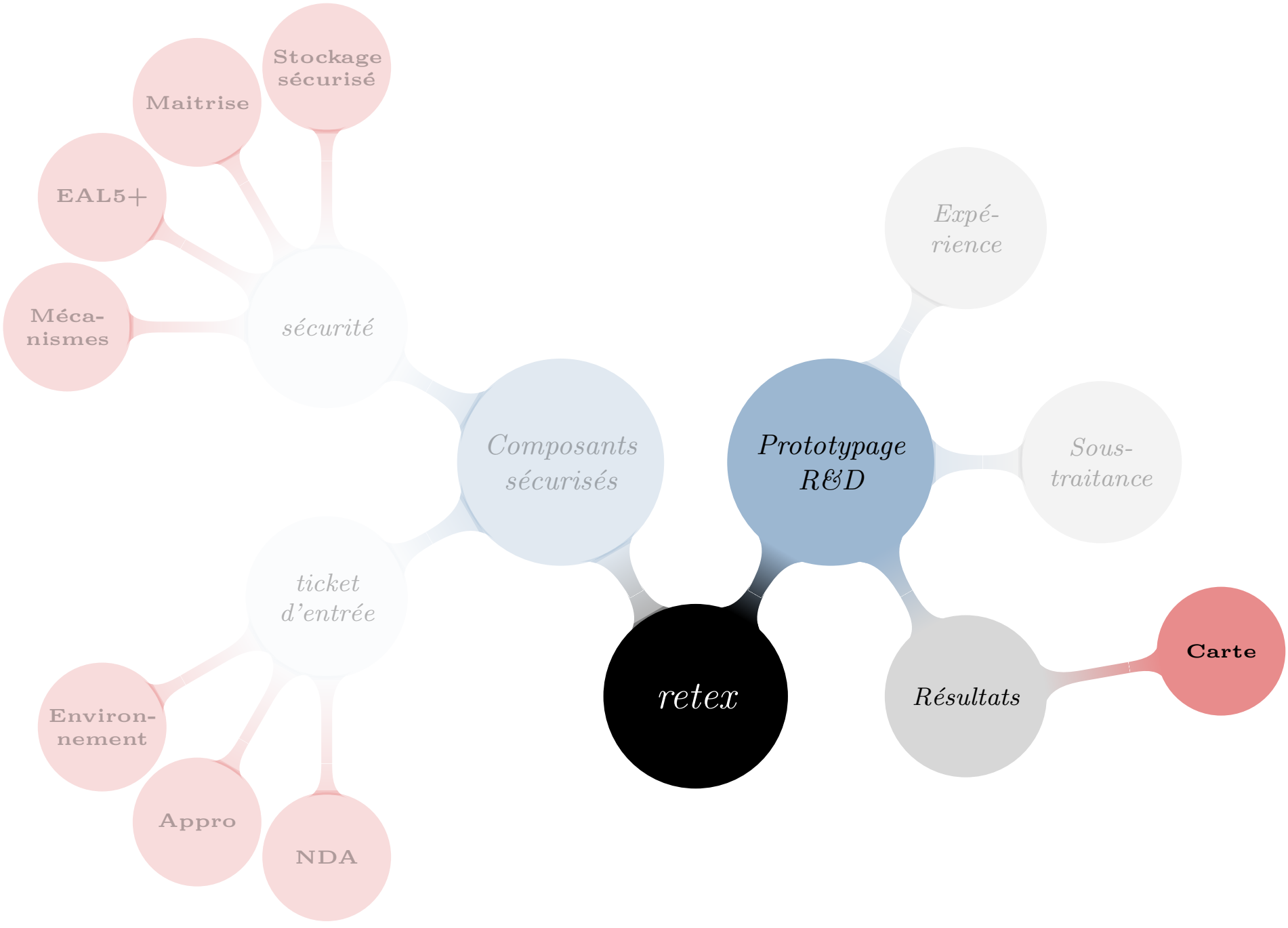

Stockage sécurisé
Maitrise
EAL5+
Méca-nismes
sécurité
Composants sécurisés
Prototypage R&D
retex
ticket d'entrée
Environ-nement
Appro
NDA

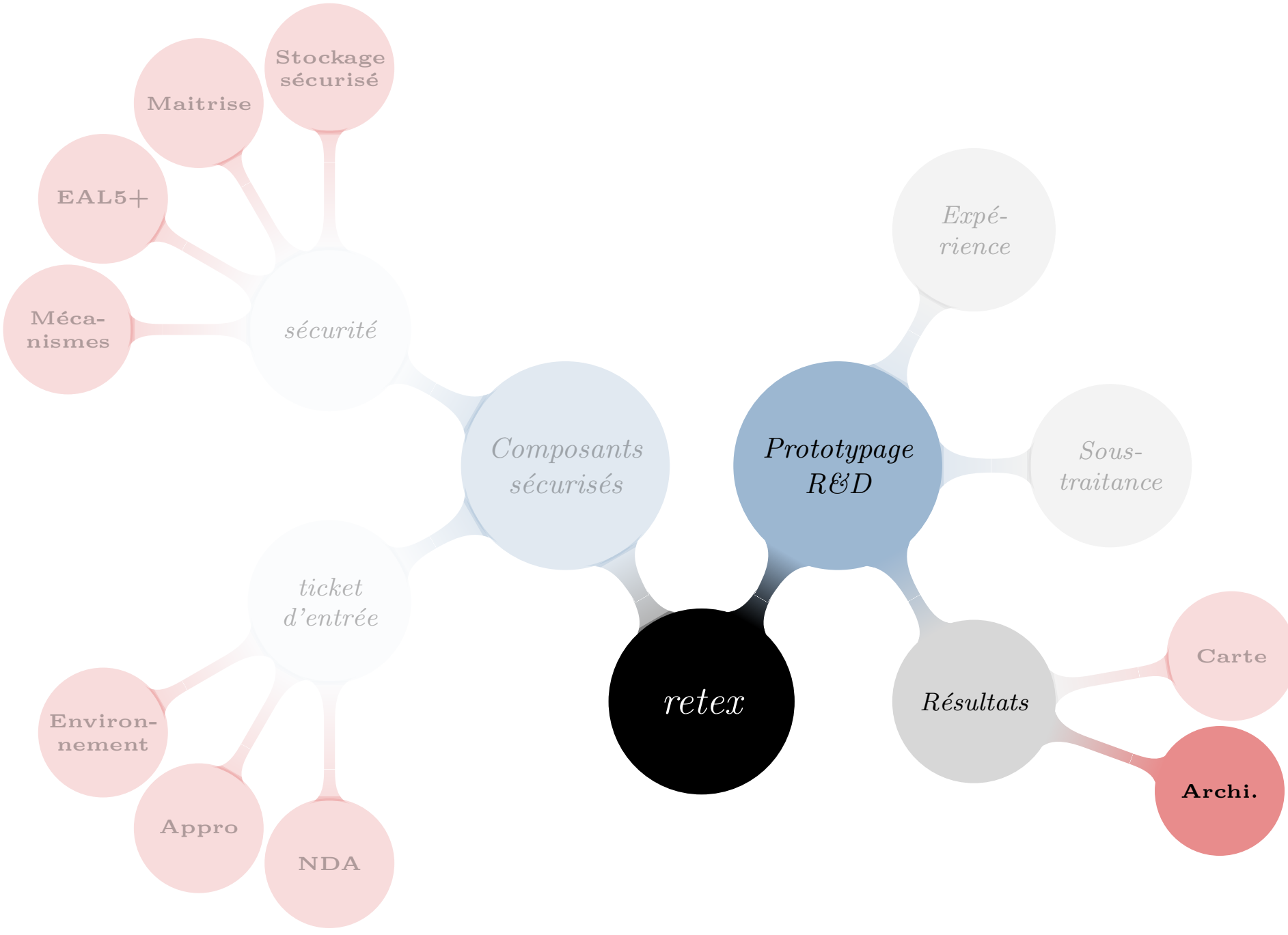

Stockage sécurisé
Maitrise
EAL5+
Méca-nismes
sécurité
Composants sécurisés
Prototypage R&D
retex
ticket d'entrée
Environ-nement
Appro
NDA

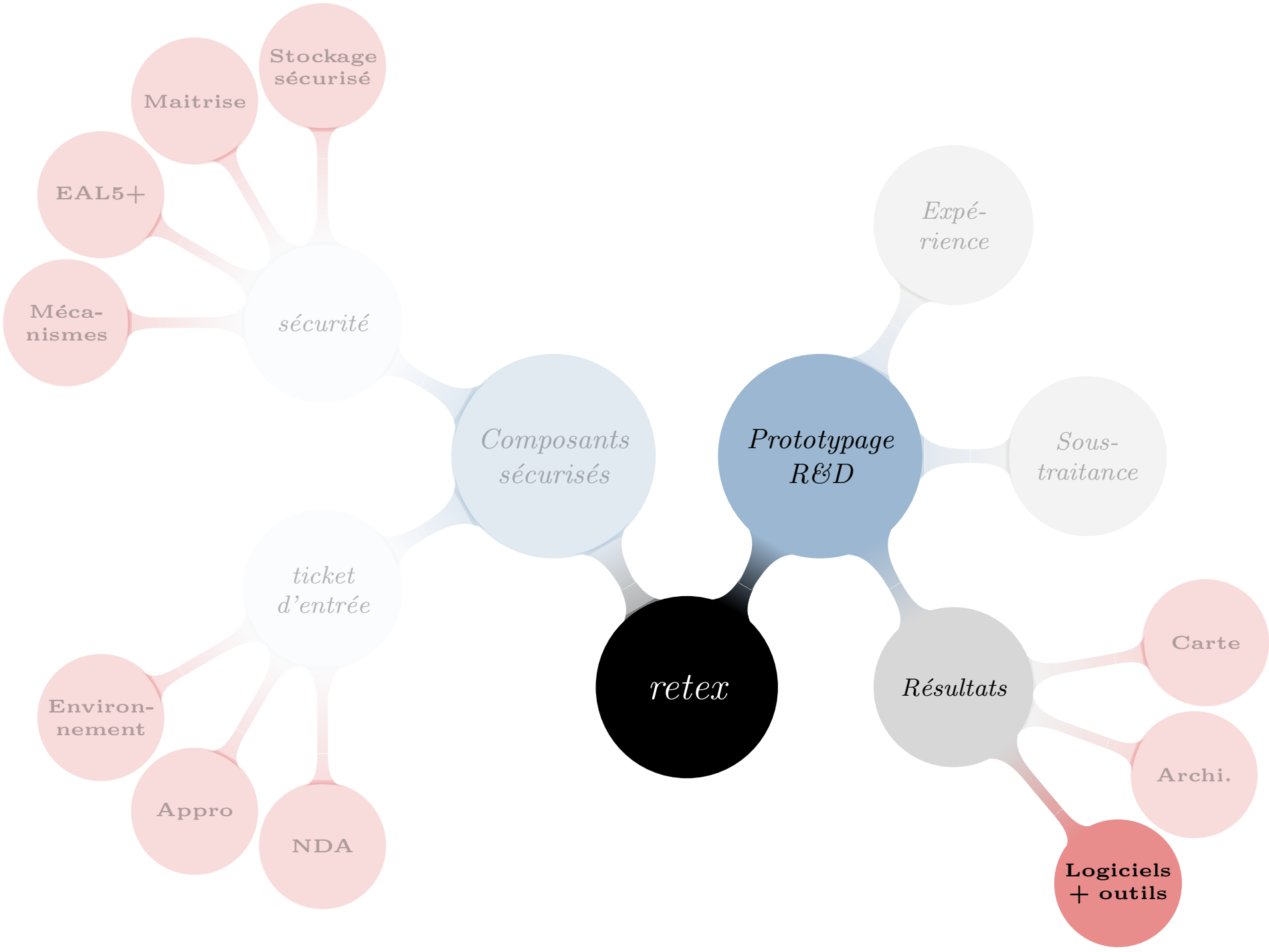

Stockage sécurisé
Maitrise
EAL5+
Méca-nismes
sécurité
Expé-rience
Composants sécurisés
Prototypage R&D
retex
ticket d'entrée
Environ-nement
Appro
NDA

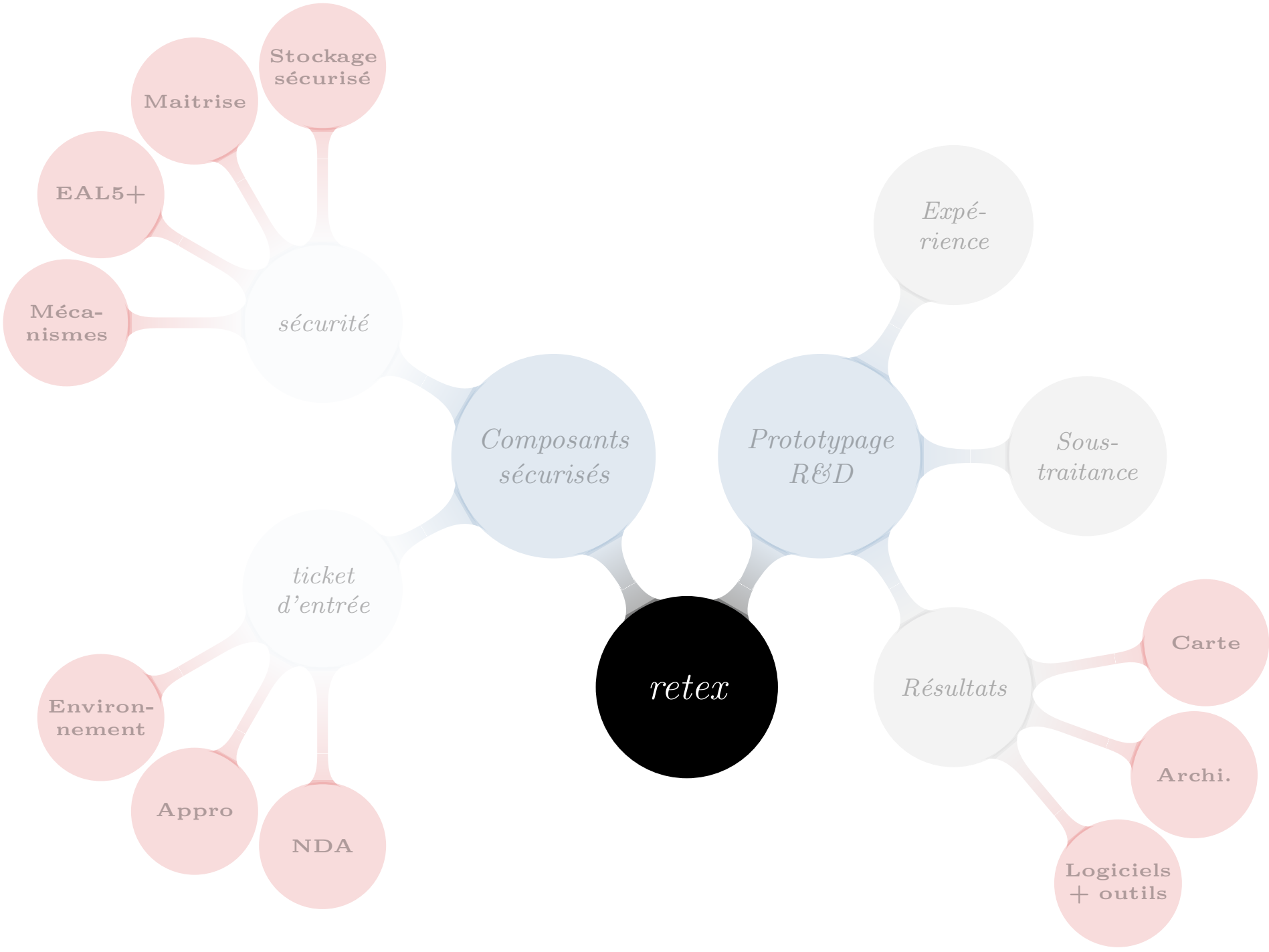

Stockage sécurisé
Maitrise
EAL5+
Méca-nismes
sécurité
Expé-rience
Composants sécurisés
Prototypage R&D
Sous-traitance
ticket d'entrée
Environ-nement
Appro
NDA
retex


Stockage sécurisé
Maitrise
EAL5+
Méca-nismes
sécurité
Composants sécurisés
ticket d'entrée
Environ-nement
Appro
NDA
Expé-rience
Prototypage R&D
Sous-traitance
retex
Résultats


Stockage sécurisé
Maitrise
EAL5+
Méca-nismes
sécurité
Composants sécurisés
ticket d'entrée
Environ-nement
Appro
NDA
retex
Prototypage R&D
Expé-rience
Sous-traitance
Résultats
Carte


Stockage sécurisé
Maitrise
EAL5+
Méca-nismes
sécurité
Composants sécurisés
ticket d'entrée
Environ-nement
Appro
NDA
Expé-rience
Prototypage R&D
Sous-traitance
retex
Résultats
Carte
Archi.


Stockage sécurisé
Maitrise
EAL5+
Méca-nismes
sécurité
Composants sécurisés
ticket d'entrée
Environ-nement
Appro
NDA
Expé-rience
Prototypage R&D
Sous-traitance
retex
Résultats
Carte
Archi.
Logiciels + outils


retex
Composants sécurisés
sécurité
Stockage sécurisé
Maitrise
EAL5+
Méca-nismes
ticket d'entrée
Environ-nement
Appro
NDA
Prototypage R&D
Expé-rience
Sous-traitance
Résultats
Carte
Archi.
Logiciels + outils