Graduate Programmes Lille

cnrs

Université de Lille

CRIStAL

Centre de Recherche en Informatique, Signal et Automatique de Lille

ircica

IOT: SECURITY & FORMAL METHODS 101

Presented By : Hugo Forraz

IKS Days @ Univ-Lille | 2024

2XS EXTRA SMALL EXTRA SAFE

Founded by IPCEI-CIS

ME IN ONE SLIDE

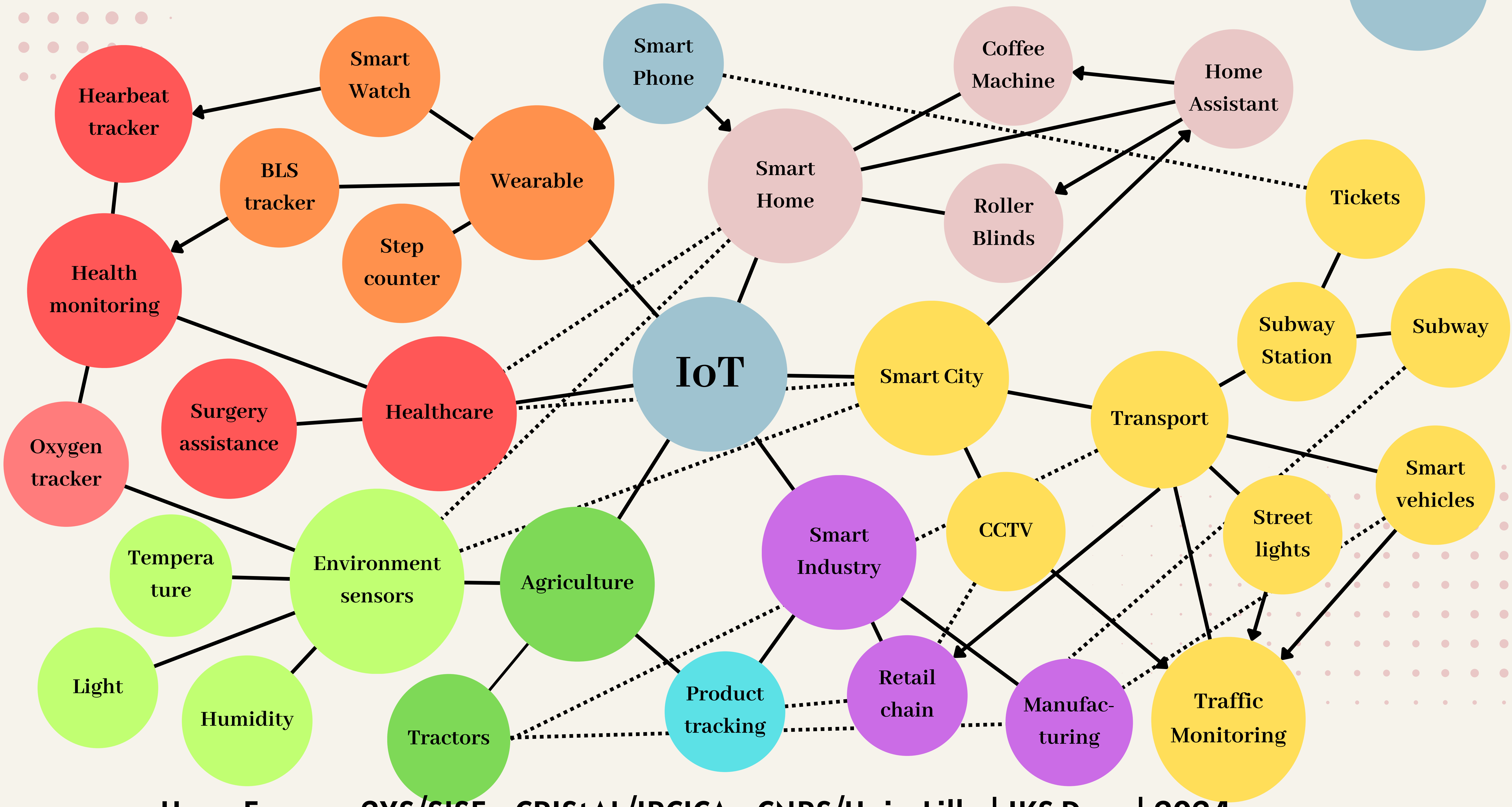
- Ph.D. candidate in the 2XS team @ CRIStAL
- Former IKS student (from “IoT & Cybersecurity”)
- Subject at the boundary of Computer Science & Mathematics

OVERVIEW

- Introduction
- What is “IoT” ??
- Security & Safety concerns
- Formal methods

SOME USAGES OF IOT

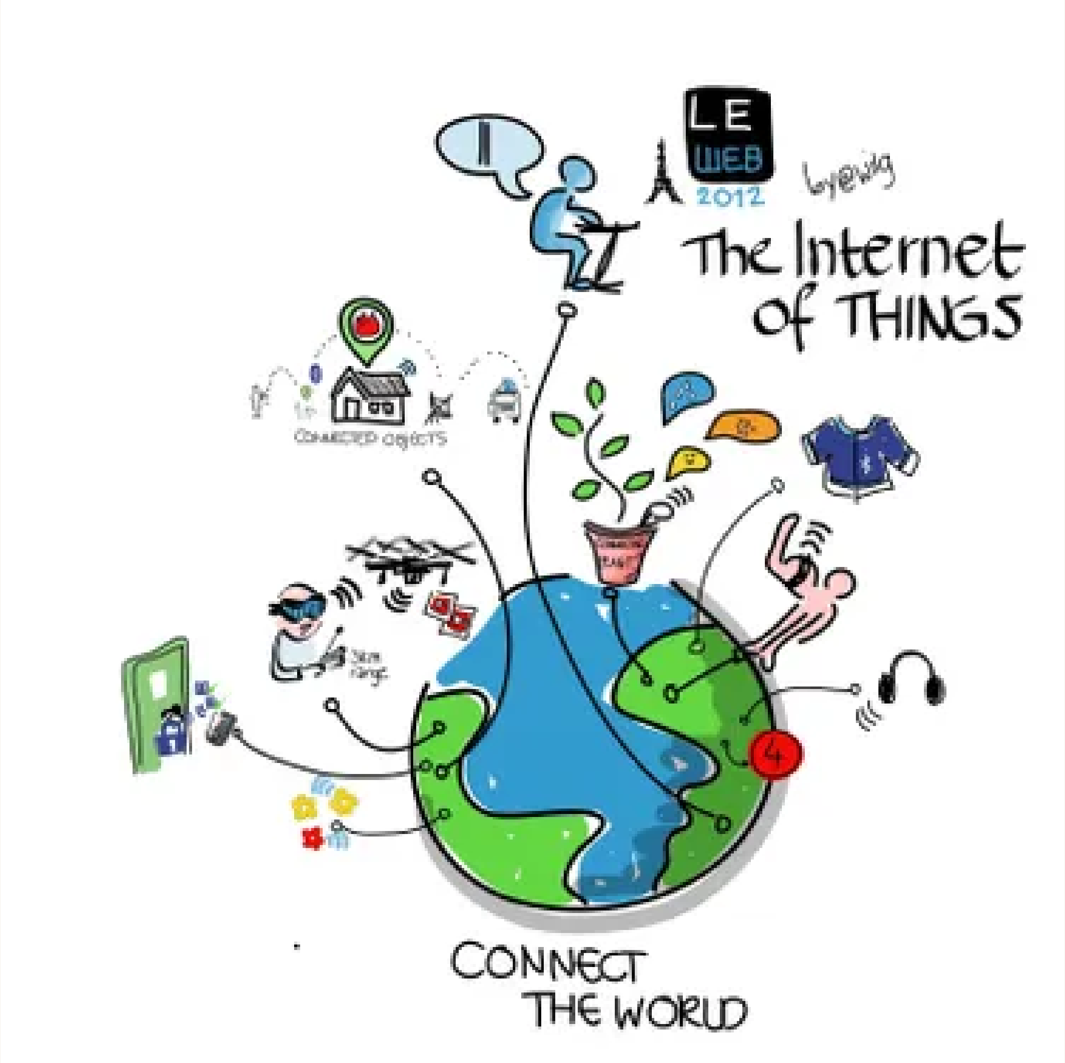
Side note: IoT is not only "this", those are only a few examples but at least a hundred bubbles and a thousand arrows could be added



STORY TIME !!

FORMAL DEFINITION

IoT: Short for Internet of things.
It describes devices with <u>sensors</u>, processing ability, <u>software</u> and other <u>technologies</u> that connect and exchange data with other devices and systems over the <u>Internet</u> or other communication networks.



Definition shamefully taken from :

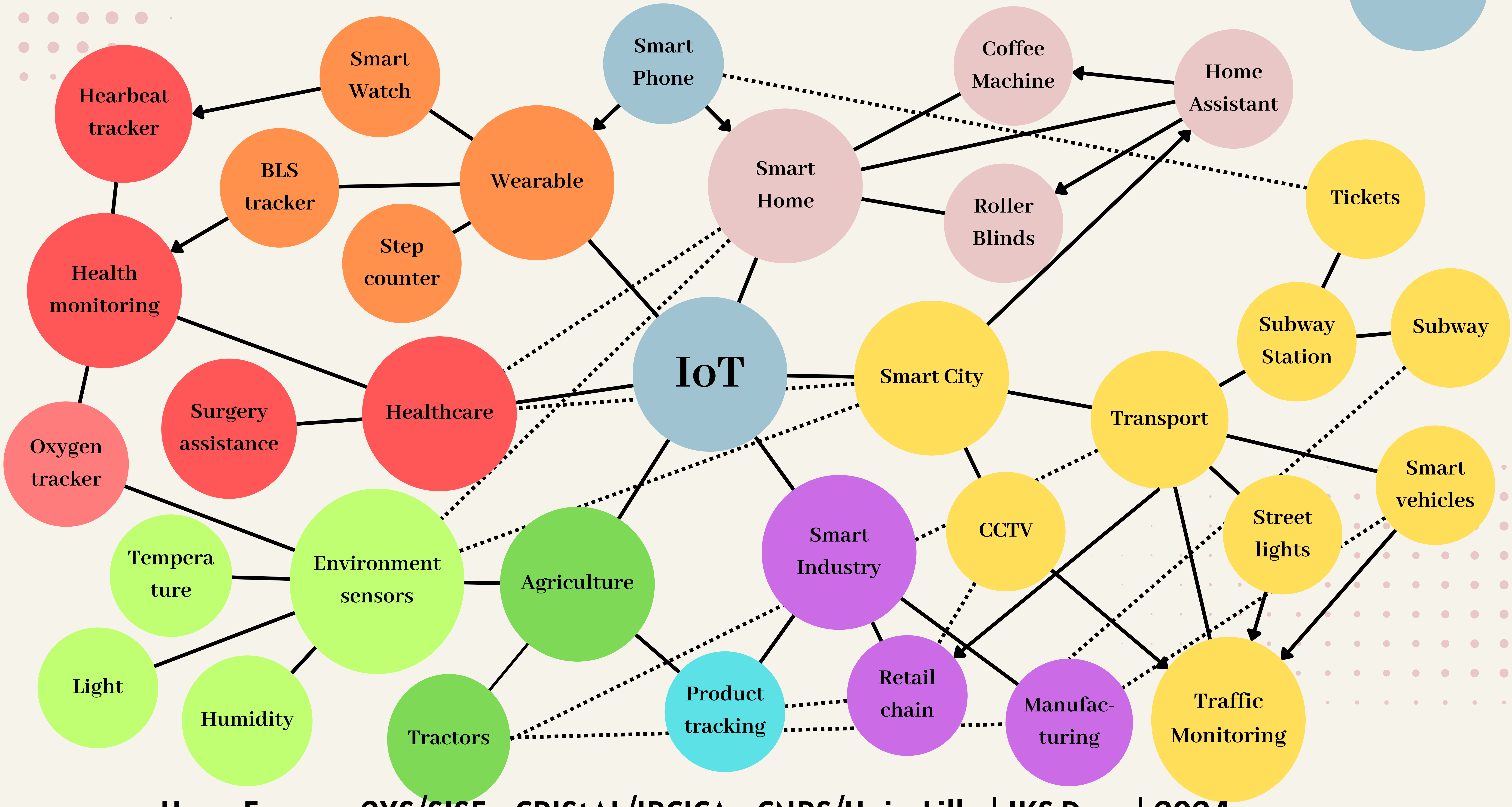
Internet of things

Internet of things (IoT) describes devices with sensors, processing ability, software and other technologies that connect and exchange data with...

Wikipedia

SOME USAGES OF IOT

Side note: IoT is not only "this", those are only a few examples but at least a hundred bubbles and a thousand arrows could be added



SAME STORY BUT BAD

Paranoia, paranoia
Everybody's comin' to get me

Lyrics of
“Flagpole Sitta”
by Harvey Danger

RISKS ENCOUNTERED

● Privacy issues

Disclosure of personal information such as the health condition or private images/videos.

E.g.:

- A smartwatch disclosing heart conditions.
- Home assistants offering everyday data to a private company.
- Spying/tracking through CCTVs.

● Security issues

Unauthorized access to a device in order to do something it was not intended to do.

E.g.:

- Connecting to someone's connected lights to turn on lights at their place.
- Putting black paint on CCTV.
- Turning off an oxygen machine in an hospital.

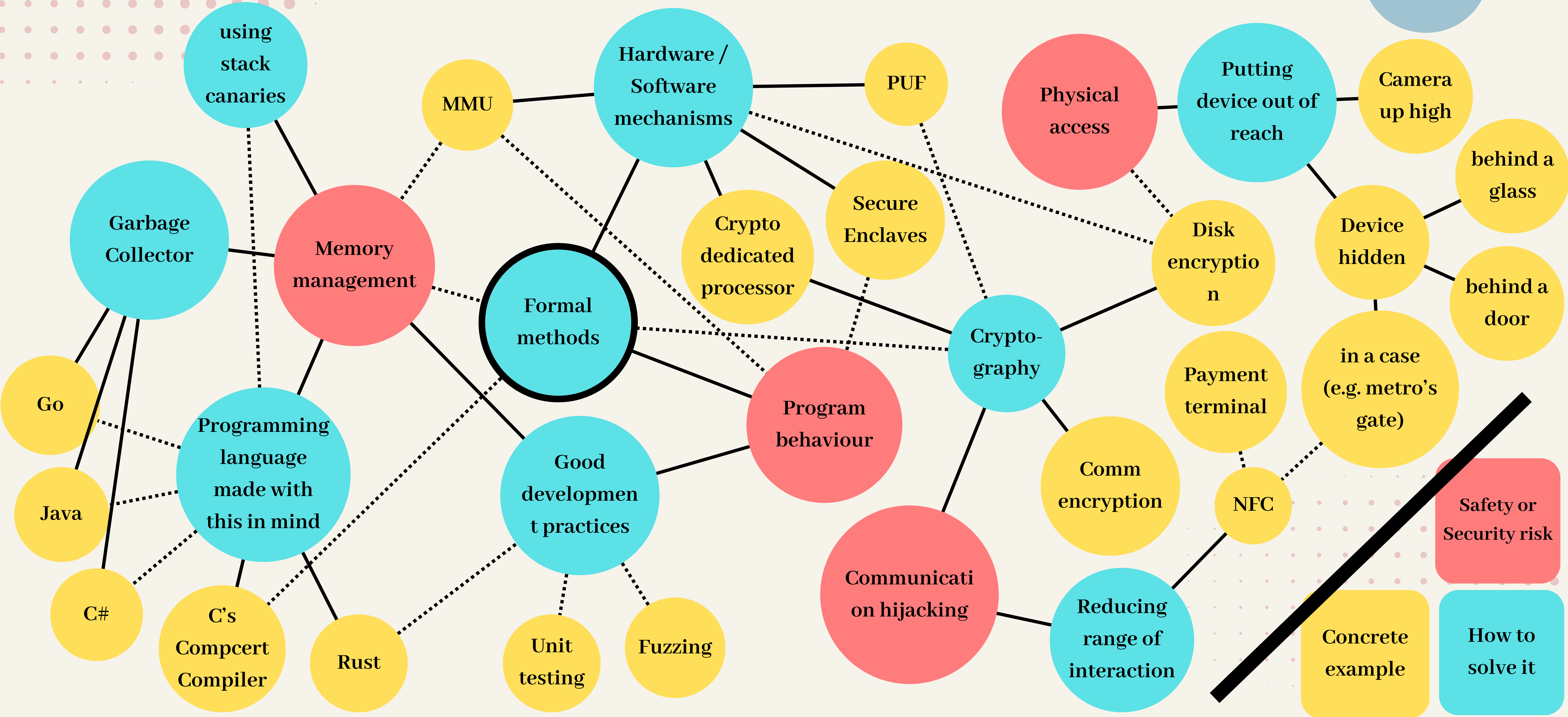
● Safety issues

Malfunction of a system that may cause undesired effects on the environment

E.g.:

- A connected alarm clock unconfigured that rings at 4am rather than 8am.
- A car's Anti-lock Braking System (ABS) that ends up in letting the car drift towards a wall.

ANOTHER HARD TO GRASP GRAPH



FORMAL METHO-WHAT?

Mathematically rigorous techniques for the specification, development, analysis, and verification of software and hardware systems. The use of formal methods for software and hardware design is motivated by the expectation that, as in other engineering disciplines, performing appropriate mathematical analysis can contribute to the reliability and robustness of a design.

Definition shamefully taken from :

Formal methods

In computer science, formal methods are mathematically rigorous techniques for the specification, development, analysis, and...

Wikipedia

LEVELS OF FORMALISMS

0 **No formalisation :**
Most software lie there, you might find documentation and/or tests, written by the developer or someone else.

1 **Formal Specification :**
Description of the component through mathematical formulae / formalisms.

2 **Formal Verification :**
Verify parts of the specification described above.

3 **Formal Synthesis :**
Generate correct code from the the verified specification.

Hugo Forraz - 2XS/SISE - CRIStAL/IRCICA - CNRS/Univ. Lille | IKS Days | 2024

CERTIFIED PROGRAMMING

That's where the fun starts

Method that is the
closest to maths
in how its used.

Uses tools such as :
Isabelle/HOL ; Coq ; AGDA

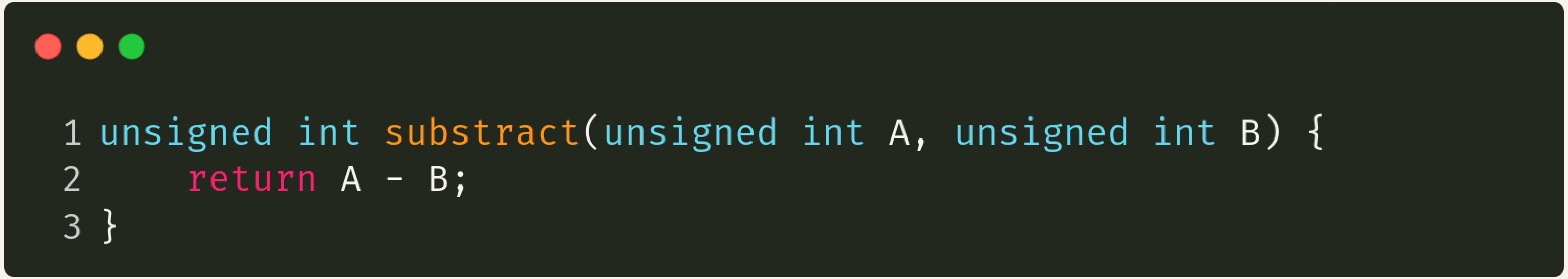
Goal :
Prove anything related to programs whether it is the hardware or the software.

SUBSTRACTION

As maths

$$13 - 10 = 3$$

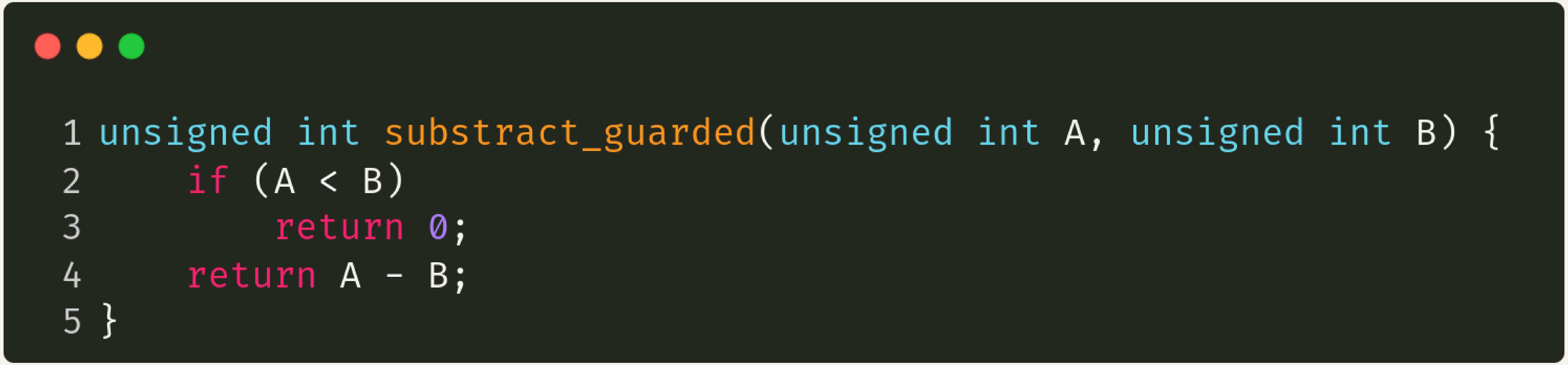
SIMPLE C FUNCTION



```c
unsigned int substract(unsigned int A, unsigned int B) {
    return A - B;
}
```

Hugo Forraz - 2XS/SISE - CRIStAL/IRCICA - CNRS/Univ. Lille | IKS Days | 2024

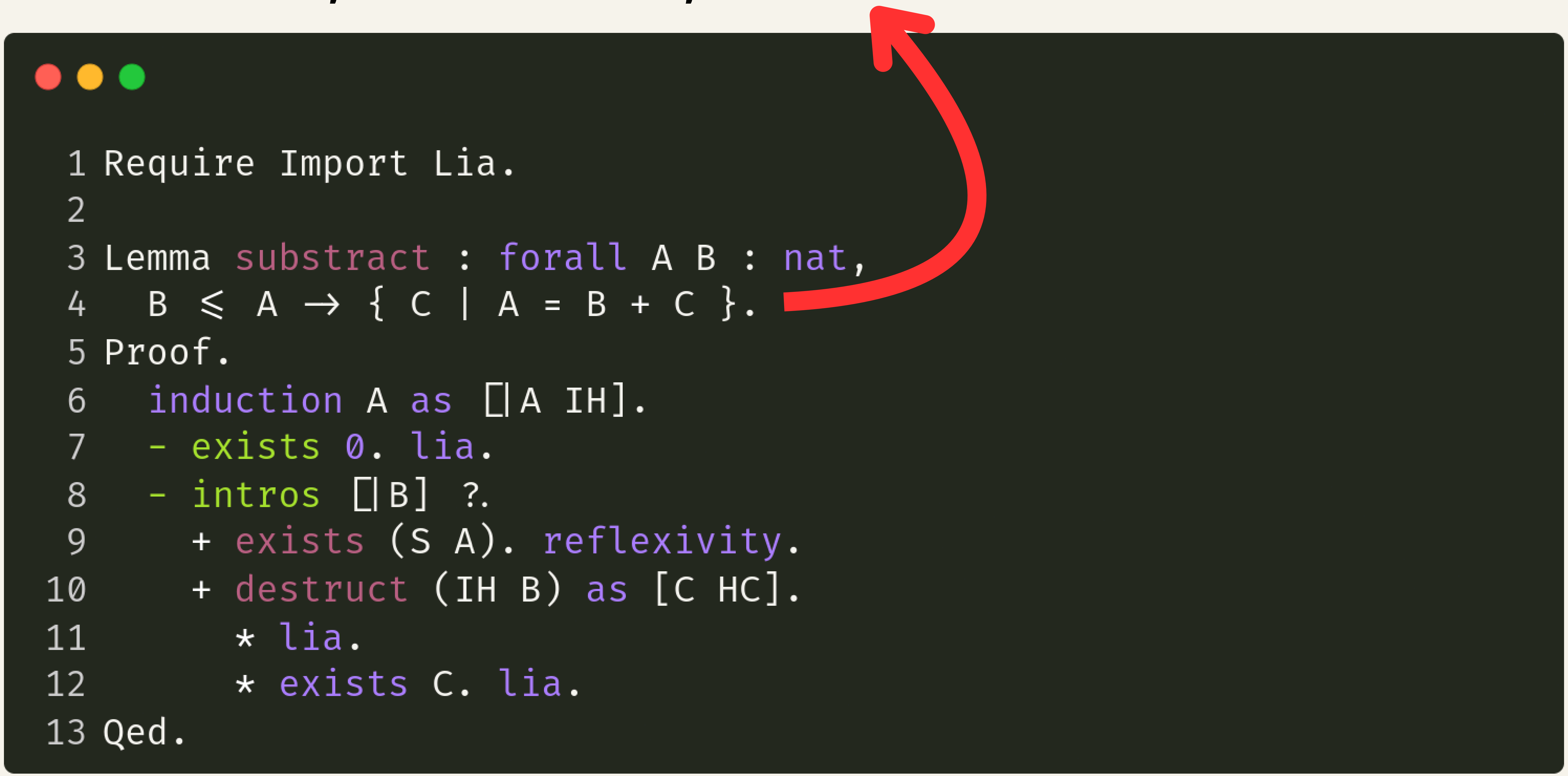
GUARDED C FUNCTION



```c
unsigned int substract_guarded(unsigned int A, unsigned int B) {
    if (A < B)
        return 0;
    return A - B;
}
```

PROVEN SUBSTRACTION IN COQ

$\forall$ A, B : ℕ s.t. B ≤ A, $\exists$ C : ℕ s.t. A-B = C

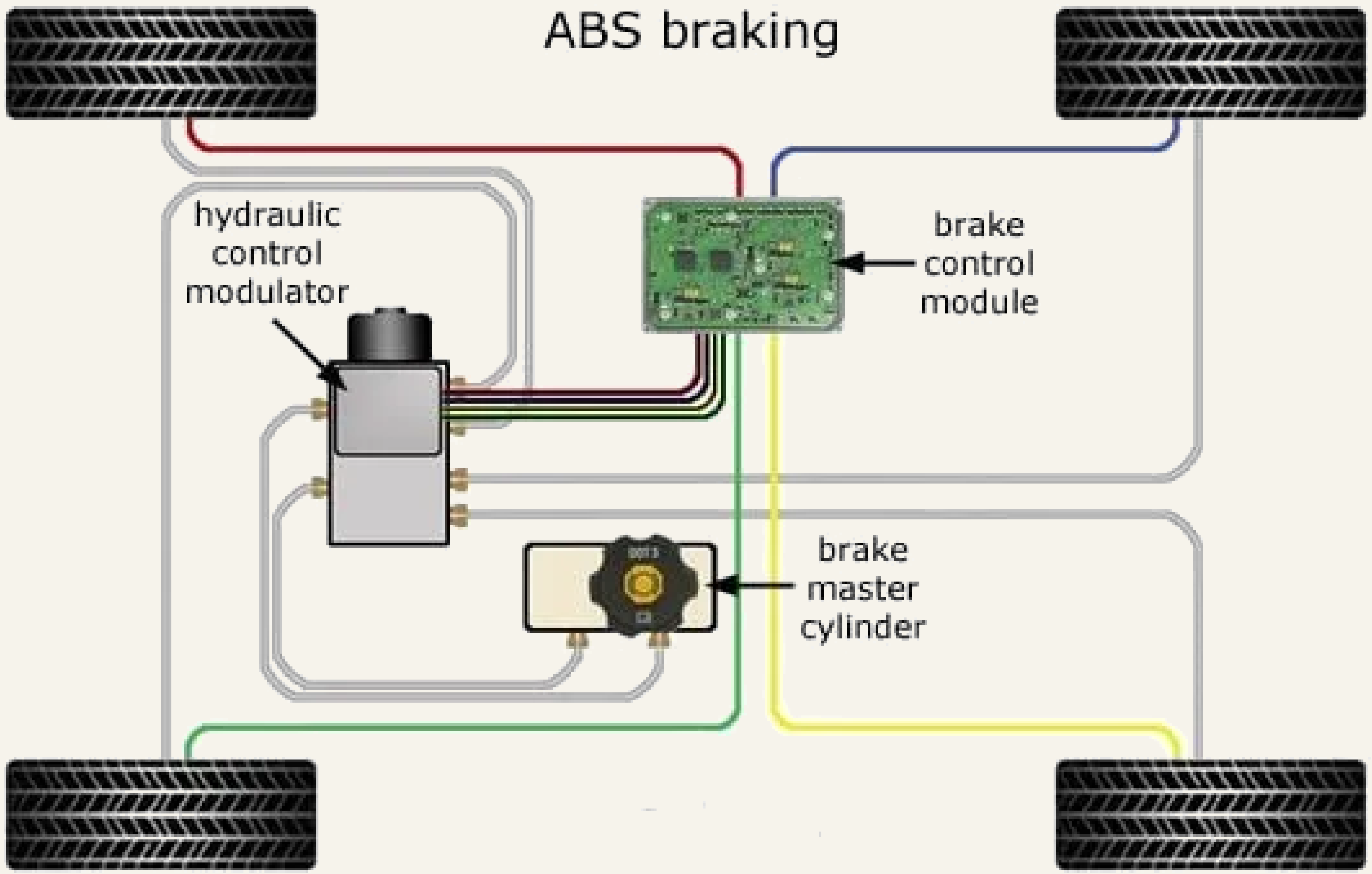


```
Require Import Lia.

Lemma substract : forall A B : nat,
  B ⩽ A → { C | A = B + C }.
Proof.
  induction A as [|A IH].
  - exists 0. lia.
  - intros [|B] ?.
    + exists (S A). reflexivity.
    + destruct (IH B) as [C HC].
      * lia.
      * exists C. lia.
Qed.
```

REAL WORLD EXAMPLE

Life critical system: ABS in cars



Security

Attacking the radio component of the car to write that we sent a signal when one was not sent.

Safety

ETCS (Electronic Throttle Control System) sending the wrong information (e.g.: accelerating rather than braking).

IKS @ Univ-Lille | 2024

THANK YOU

Presented By : Hugo Forraz