CELTIC-NEXT DAY

02nd December 2020, 09:30 – 16:00 CET

Building Robust Software Supply Chains

(DevOps, DevSecOps, Dependency Management)

Frédéric Loiret - loiret@kth.se
Benoit Baudry – baudry@kth.se

Teaser

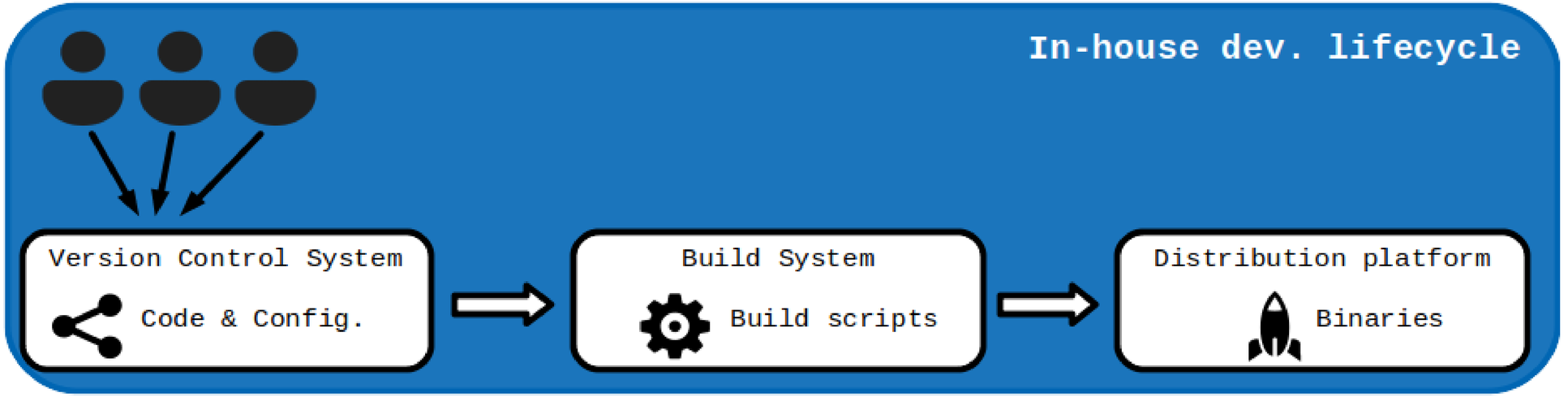
Reality of software development nowadays

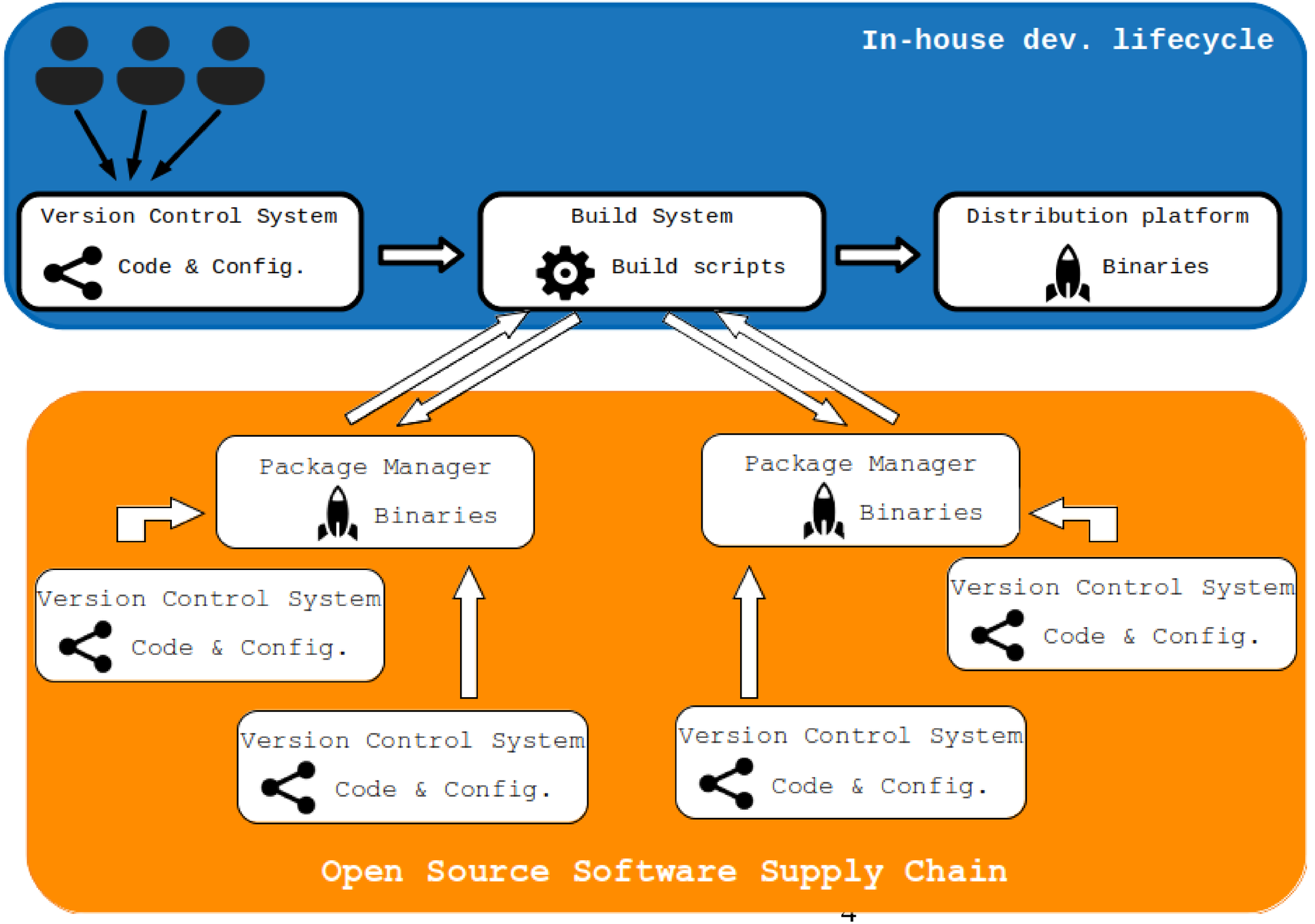
- Huge amount of code developed by third-parties

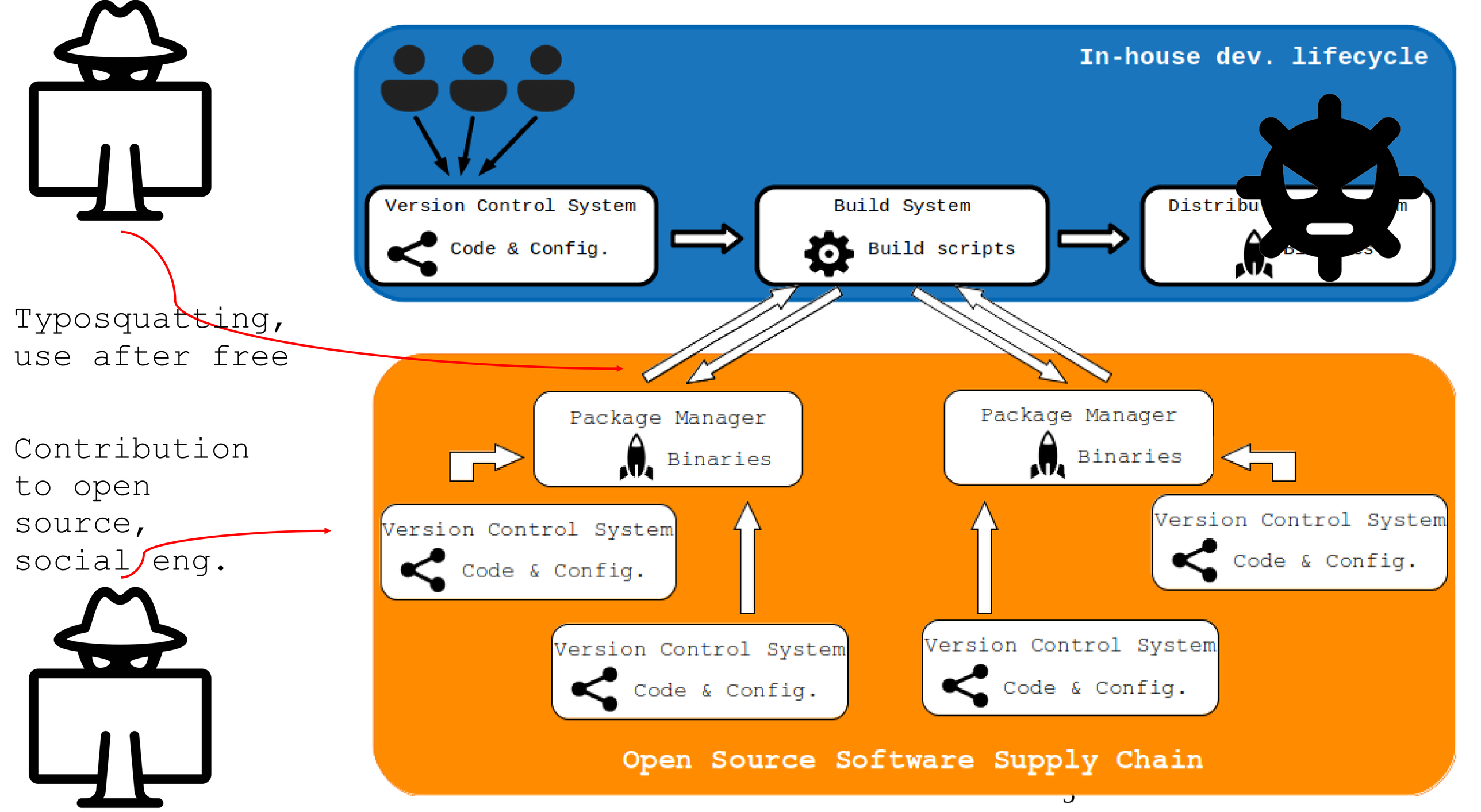
→ More reliability (safety & security) with less resources (computing power, storage, bandwidth, development time)

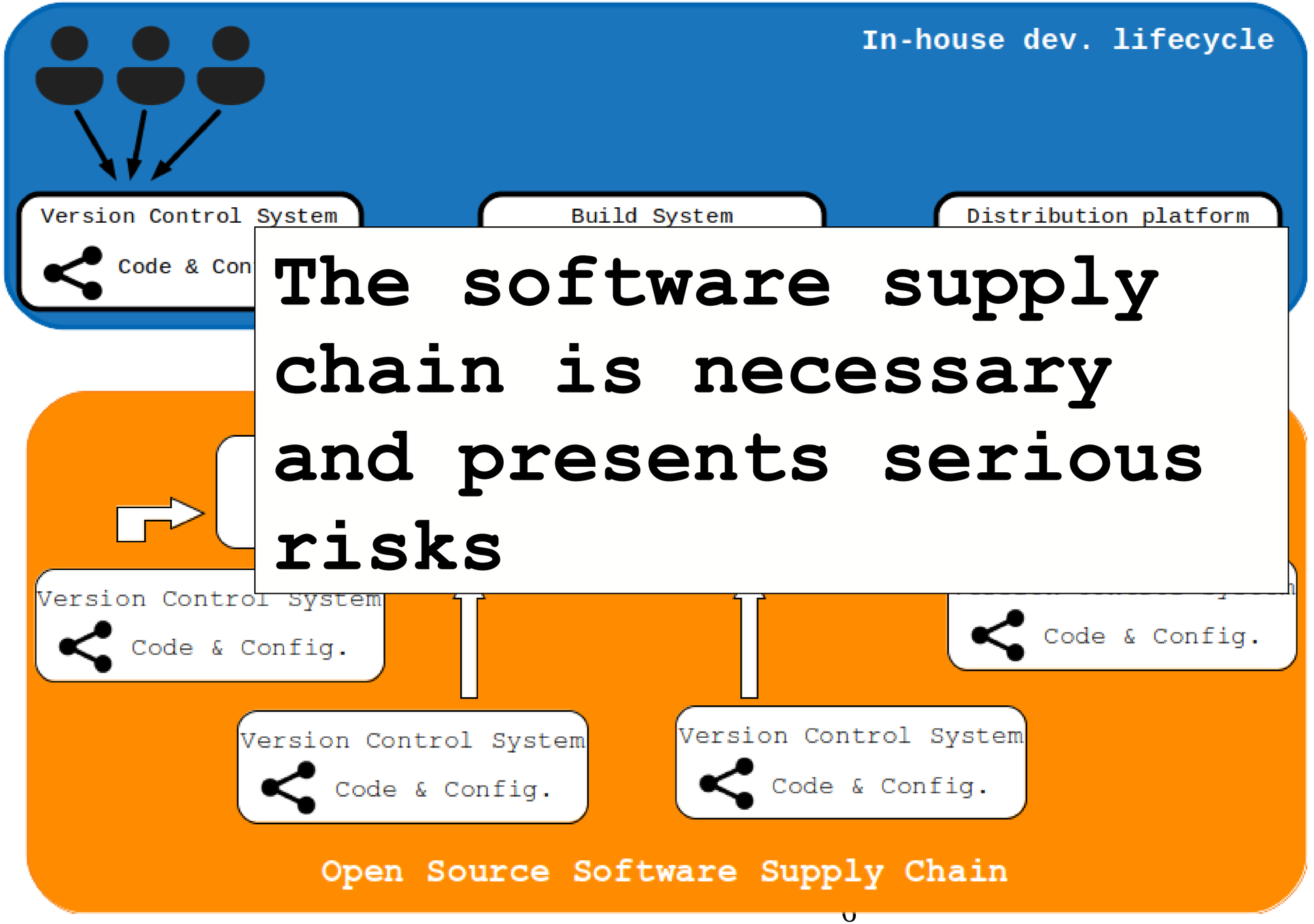
→ Mitigate security risks due to the *Software Supply Chain*

Proposal
Introduction




In-house dev. lifecycle
Version Control System
Code & Config.
Build System
Build scripts
Distribution platform
Binaries
Package Manager
Binaries
Package Manager
Binaries
Version Control System
Code & Config.
Version Control System
Code & Config.
Version Control System
Code & Config.
Version Control System
Code & Config.
Open Source Software Supply Chain


In-house dev. lifecycle
Version Control System
Code & Config.
Build System
Build scripts
Typosquatting,
use after free
Contribution
to open
source,
social eng.
Package Manager
Binaries
Package Manager
Binaries
Version Control System
Code & Config.
Version Control System
Code & Config.
Version Control System
Code & Config.
Version Control System
Code & Config.
Open Source Software Supply Chain


In-house dev. lifecycle
Version Control System
Code & Con
Build System
Distribution platform
The software supply chain is necessary and presents serious risks
Version Control System
Code & Config.
Code & Config.
Version Control System
Code & Config.
Version Control System
Code & Config.
Open Source Software Supply Chain

Mitigate the Risks of the Software Supply Chain

- *Understand open source ecosystem*
  - OSS licences analysis
  - Metrics: mean time to fix or upgrades, etc.
- *Secure the development pipeline*
  - Signed commits
  - Reproducible builds
- *Dependency management*
  - Inspect, test
  - Remove, harden
  - Isolate

Expected Outcomes

- *New (open-source) software tools*
- *Reduced attack surface of deployed products*

Organisation Profile

CASTOR Software Research Centre

Industry-Academia collaboration between Ericsson, Saab, and KTH

Stockholm, Sweden

www.castor.kth.se

Partners

- **Sweden**
  - **KTH**
  - Saab
  - Ericsson
  - FindOut? (SME)

- **France**
  - **INRIA**
  - Orange
  - Thales TGS
  - Airbus Bretagne?
  - GAIA X?,
  - ALTRAN?

- **Germany**
  - **Eclipse GmbH**
  - Siemens?
  - Bosch?
  - Audi?
  - Continental?
  - RedHat?
  - IOTA Foundation?

- Belgium?

→ We are mainly looking for industrial partners and solution providers in the areas mentioned on slide #7

Contact Info

For more information and for interest to participate please contact:

Frédéric Loiret
loiret@kth.se

Benoit Baudry
Baudry@kth.se