LISBOA | UNIVERSIDADE DE LISBOA

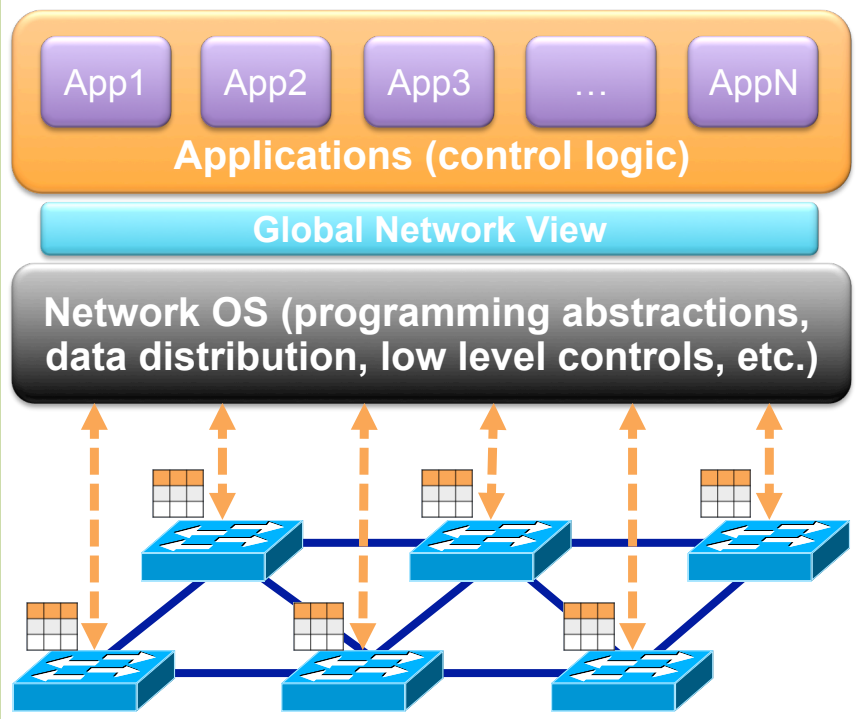
Towards Secure and Dependable Software-Defined Networks

Fernando M. V. Ramos
LaSIGE/FCUL, University of Lisbon
fvramos@fc.ul.pt
http://www.di.fc.ul.pt/~fvramos/
Joint work with Diego Kreutz and Paulo Veríssimo

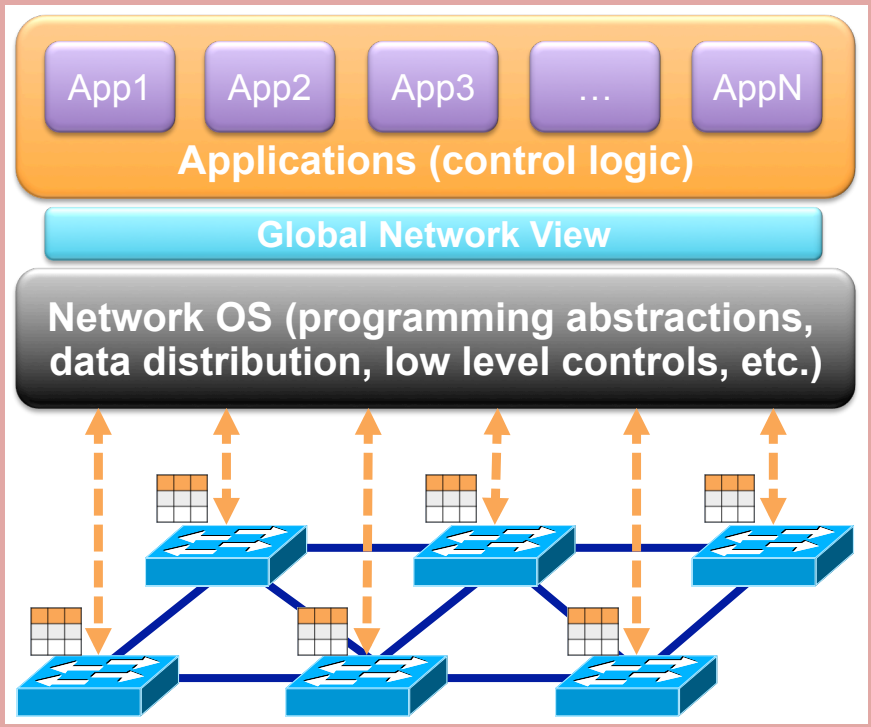
SDN in short

- Control and data planes **decoupled**
  - An enabler for innovation
  - More flexibility
- **Logical centralization** of network control
  - Easier to observe/infer and reason about network behavior
- Ability to **program** the network
  - Instead of configuring it (in a tedious, error-prone process)

Excellent, now **we** can program the network!



Wait, now **others** can program the network!



Nota Bene:

- Traditional networks have "**natural protections**" against common threats and vulnerabilities…
  - **closed** (proprietary) nature of network devices
  - **heterogeneity** of software
  - **decentralized** nature of the control plane
- …that SDNs *in principle* do not.

Outline

Main threat vectors in SDNs

Security & Dependability by design

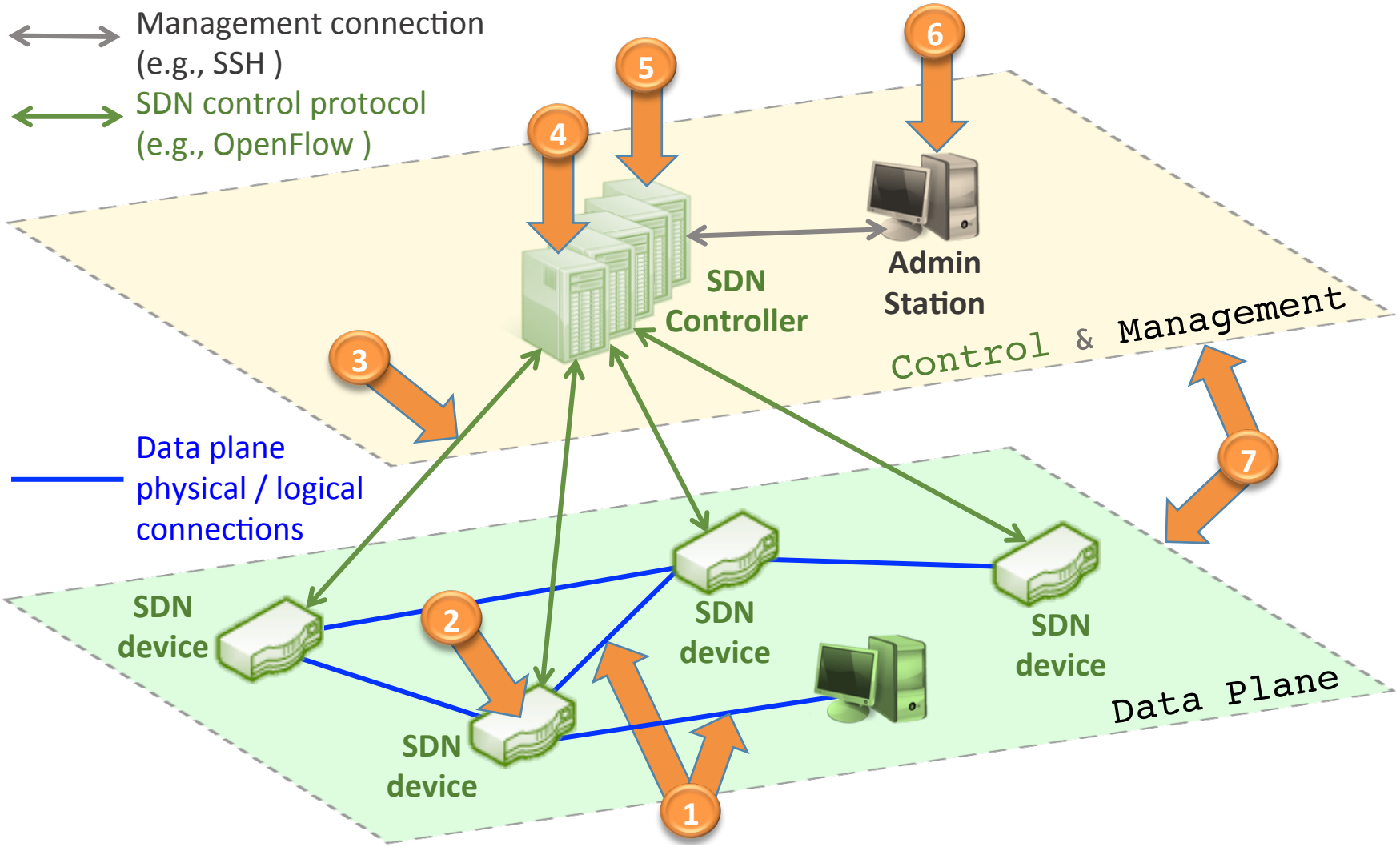
Final remarks

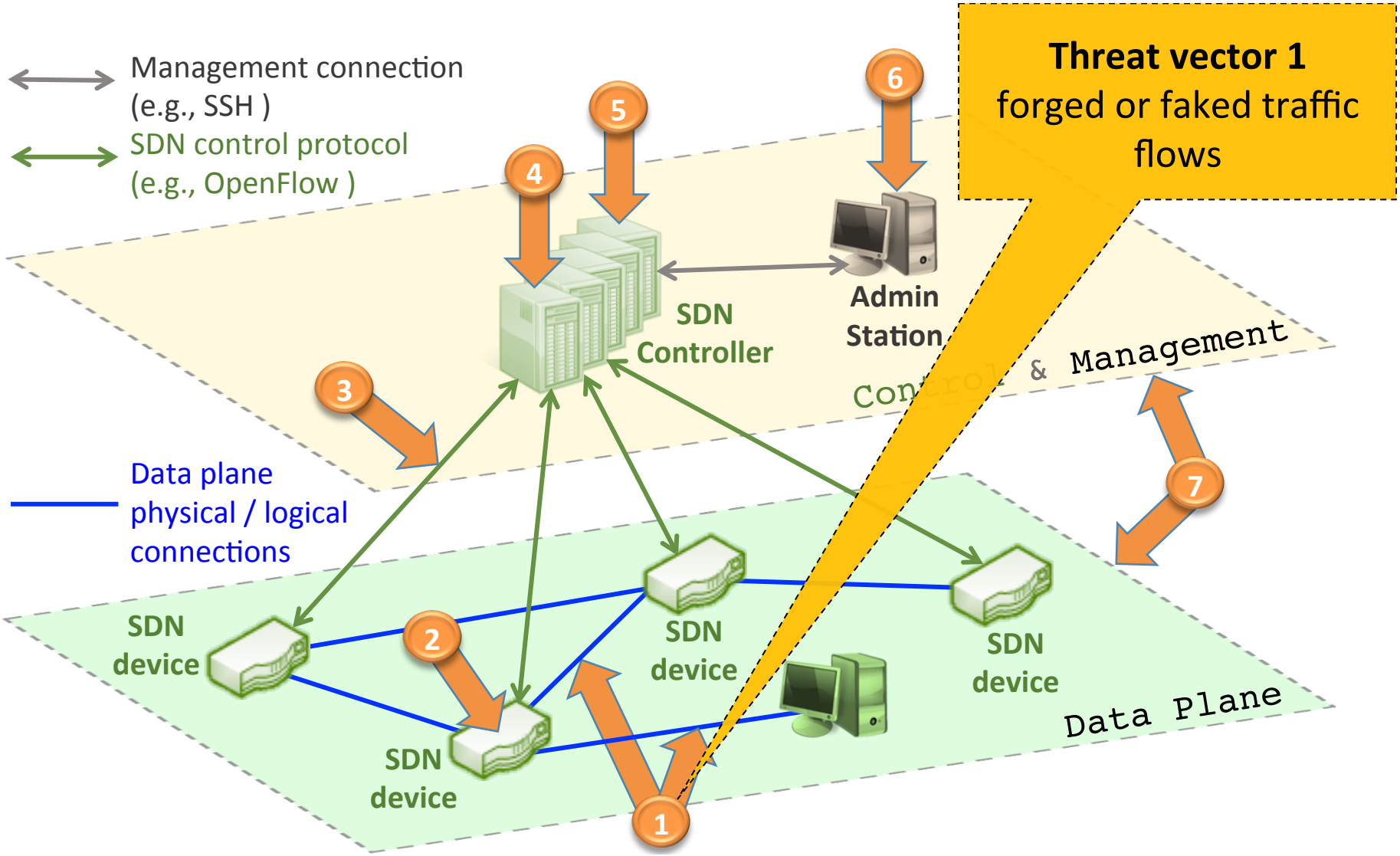
Outline

Main threat vectors in SDNs

Security & Dependability by design

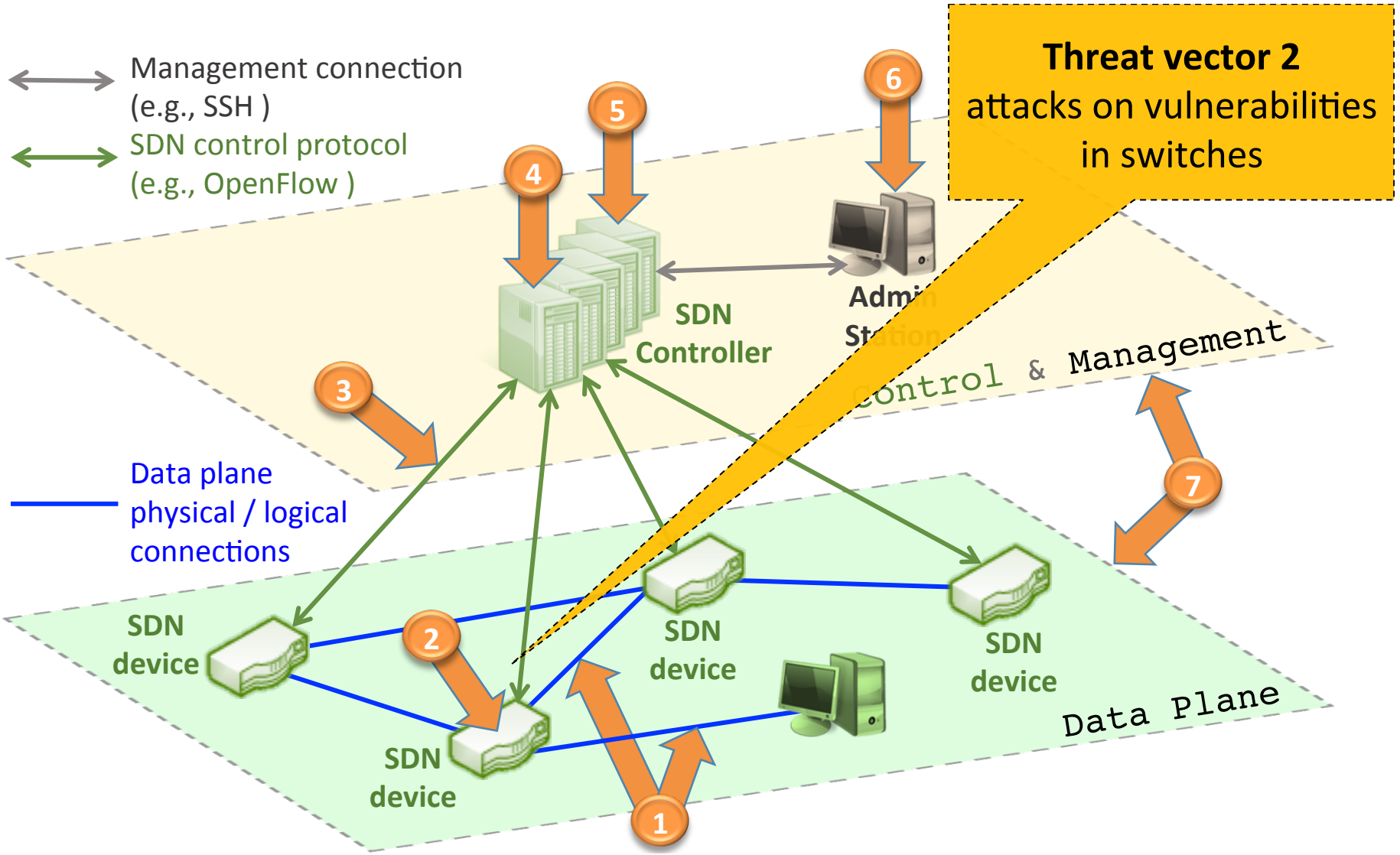
Final remarks


Management connection
(e.g., SSH)
SDN control protocol
(e.g., OpenFlow)
Data plane
physical / logical
connections
SDN
Controller
Admin
Station
Control & Management
SDN
device
SDN
device
SDN
device
SDN
device
Data Plane
1
2
3
4
5
6
7



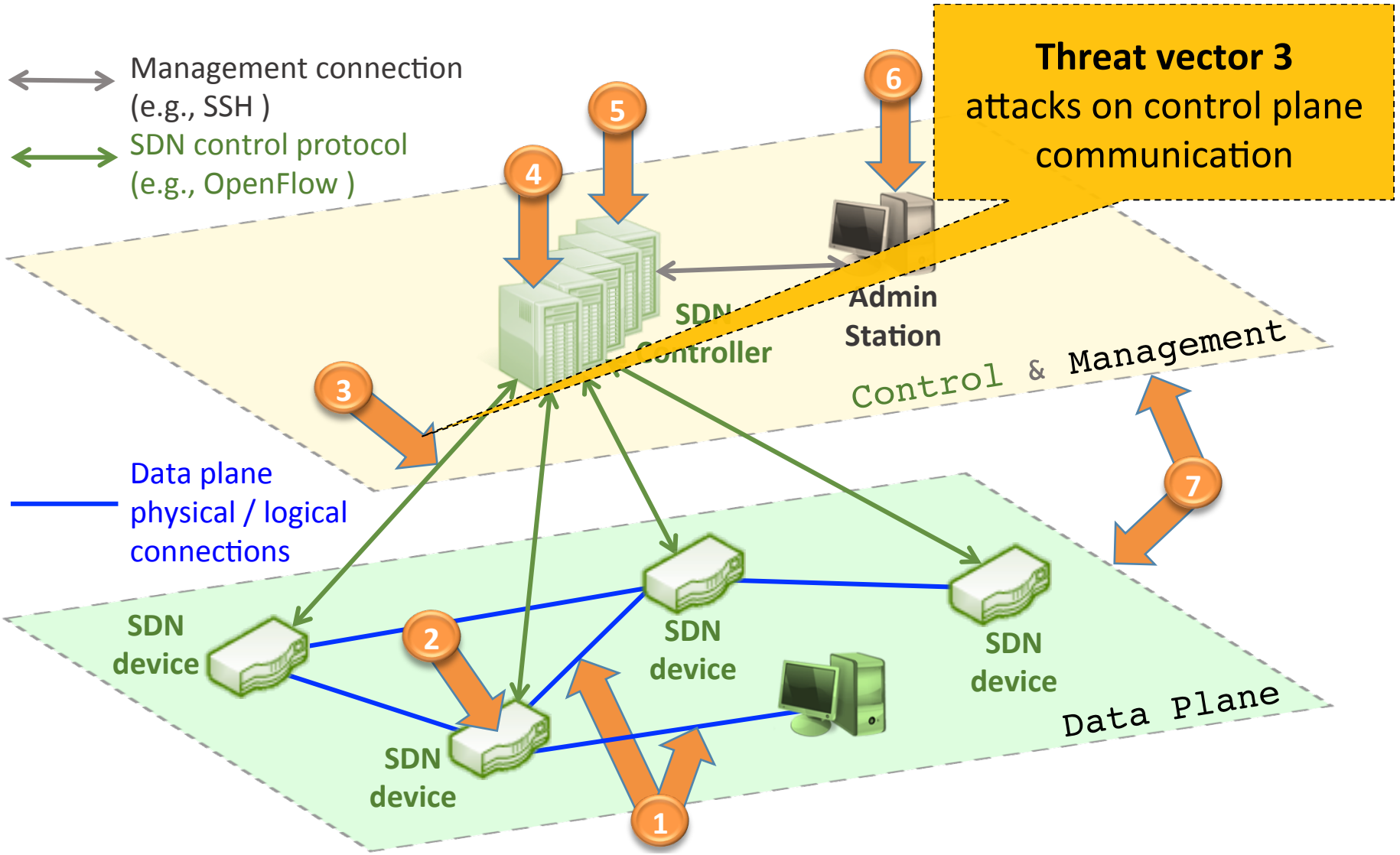
Not specific to SDNs, but can be a door for augmented DoS attacks.

Possible solutions: IDS + rate bounds for control plane requests



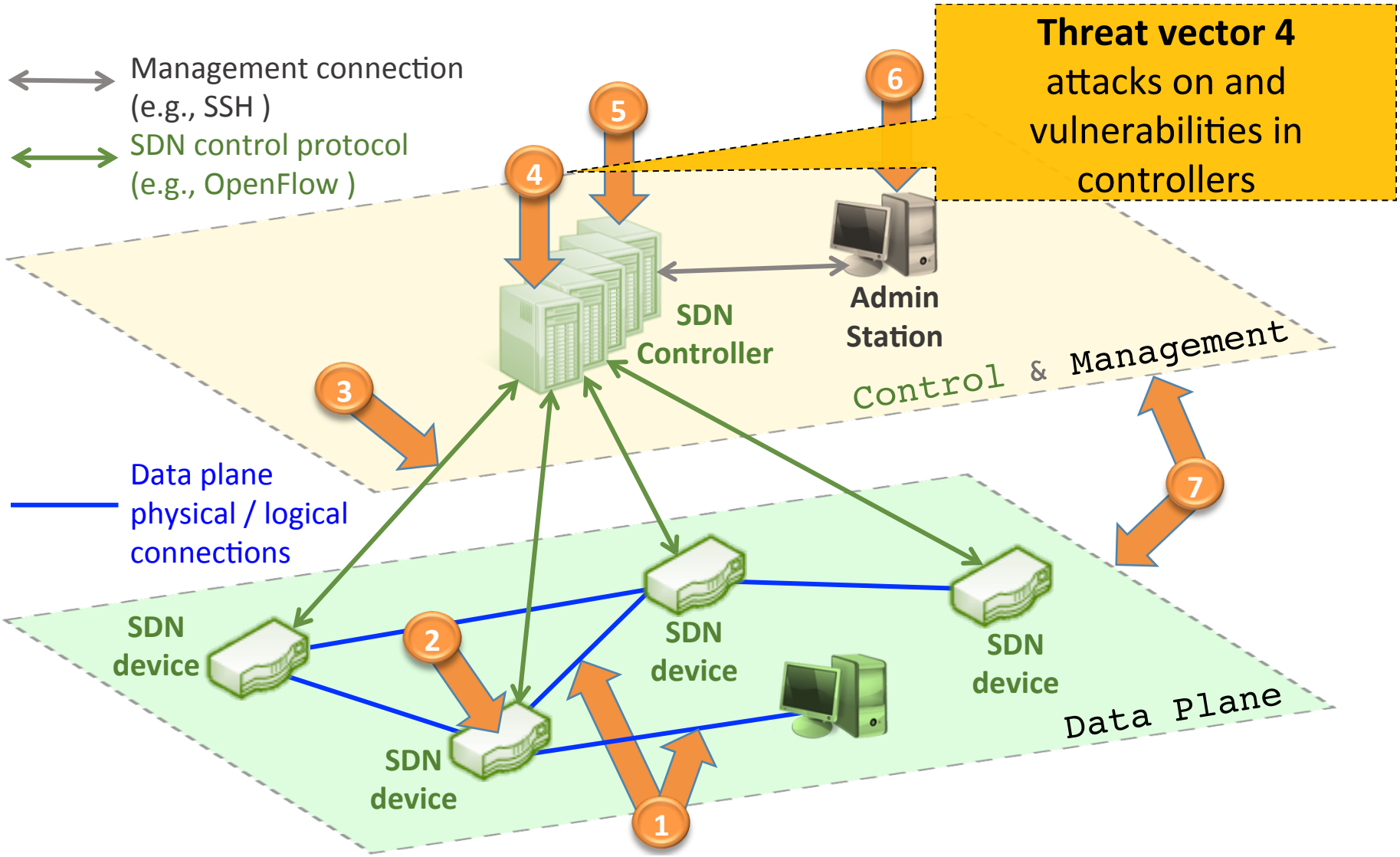
Not specific to SDNs, but now the impact is potentially augmented.

Possible solutions: sw/hw attestation with autonomic trust management



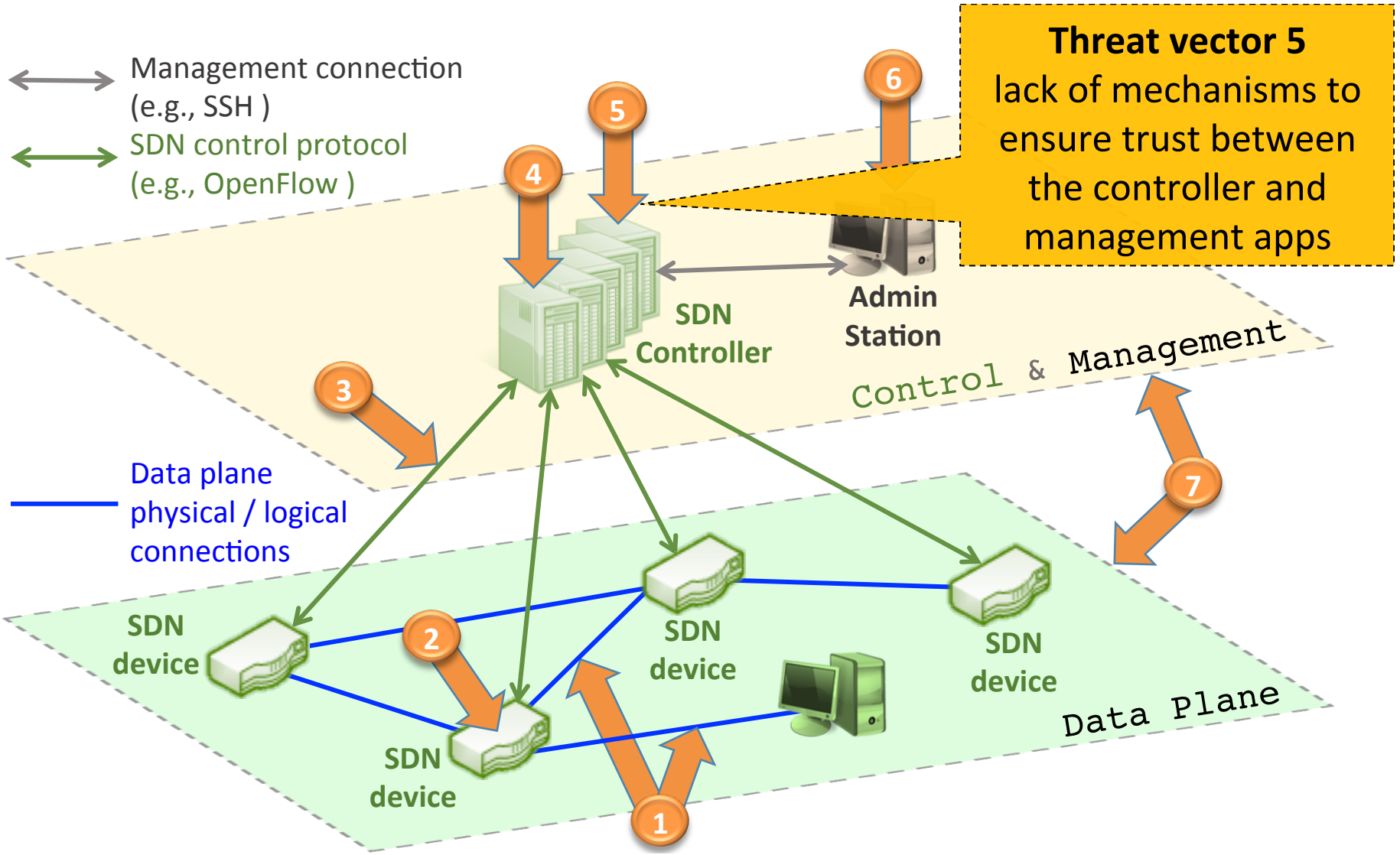
Specific to SDNs: communication with logically centralized controllers can be exploited.

Possible solutions: threshold cryptography across controller replicas



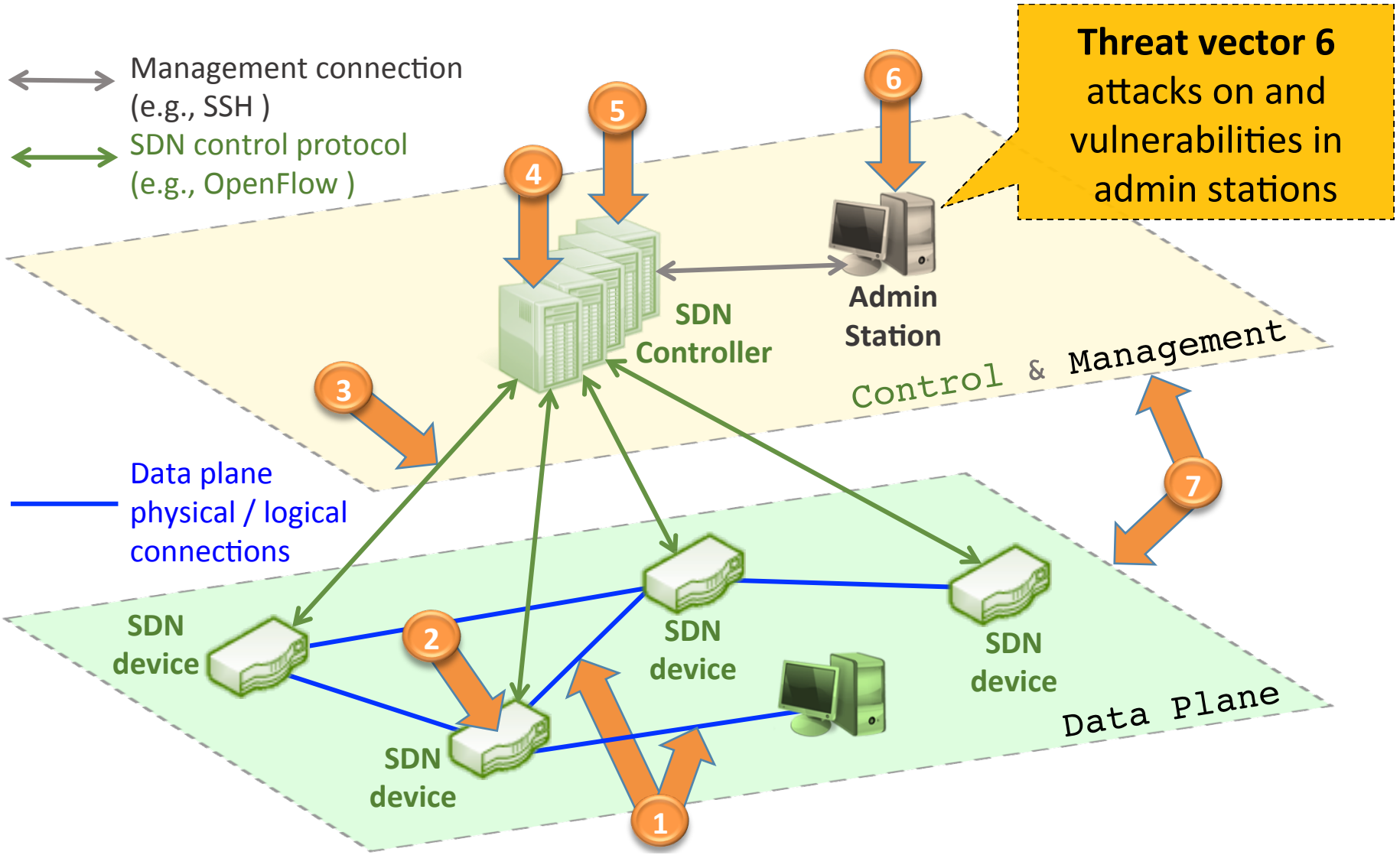
Specific to SDNs, controlling the controller may compromise the entire network.

Possible solutions: replication + diversity + recovery



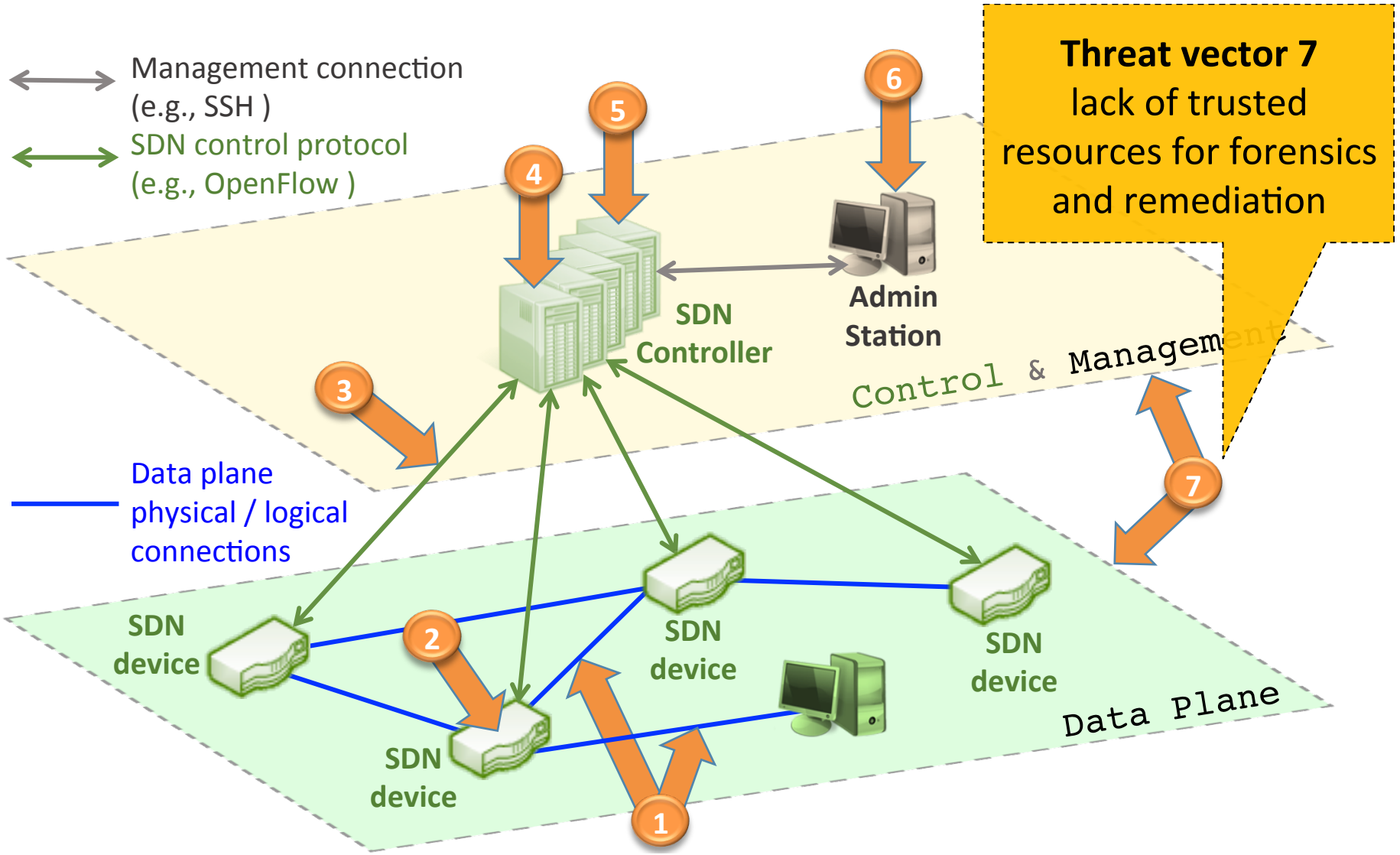
Specific to SDNs, malicious applications can now be easily developed and deployed on controllers.

Possible solutions: sw attestation with autonomic trust management



Not specific to SDNs, but now the impact is potentially augmented.

Possible solutions: double credential verification



Not specific to SDNs, but it is still critical to assure fast recovery and diagnosis when faults happen.

Possible solutions: indelible logging

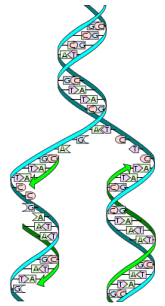
Outline

Main threat vectors in SDNs

Security & Dependability by design

Final remarks

Sec&Dep tools to consider

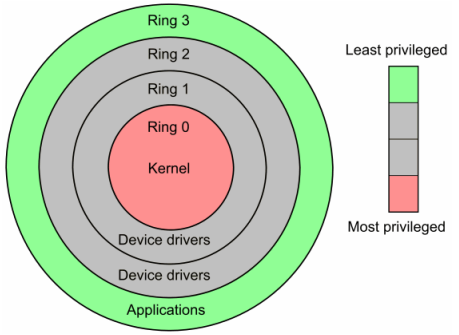


- Replication
  - Dynamic device association
  - Self-healing mechanisms for *perpetual* operation
- Diversity

- (Autonomic) trust
  - between controllers and devices
  - between applications and controller software

Sec&Dep tools to consider

- Security domains
  - kernel mode *vs* user mode



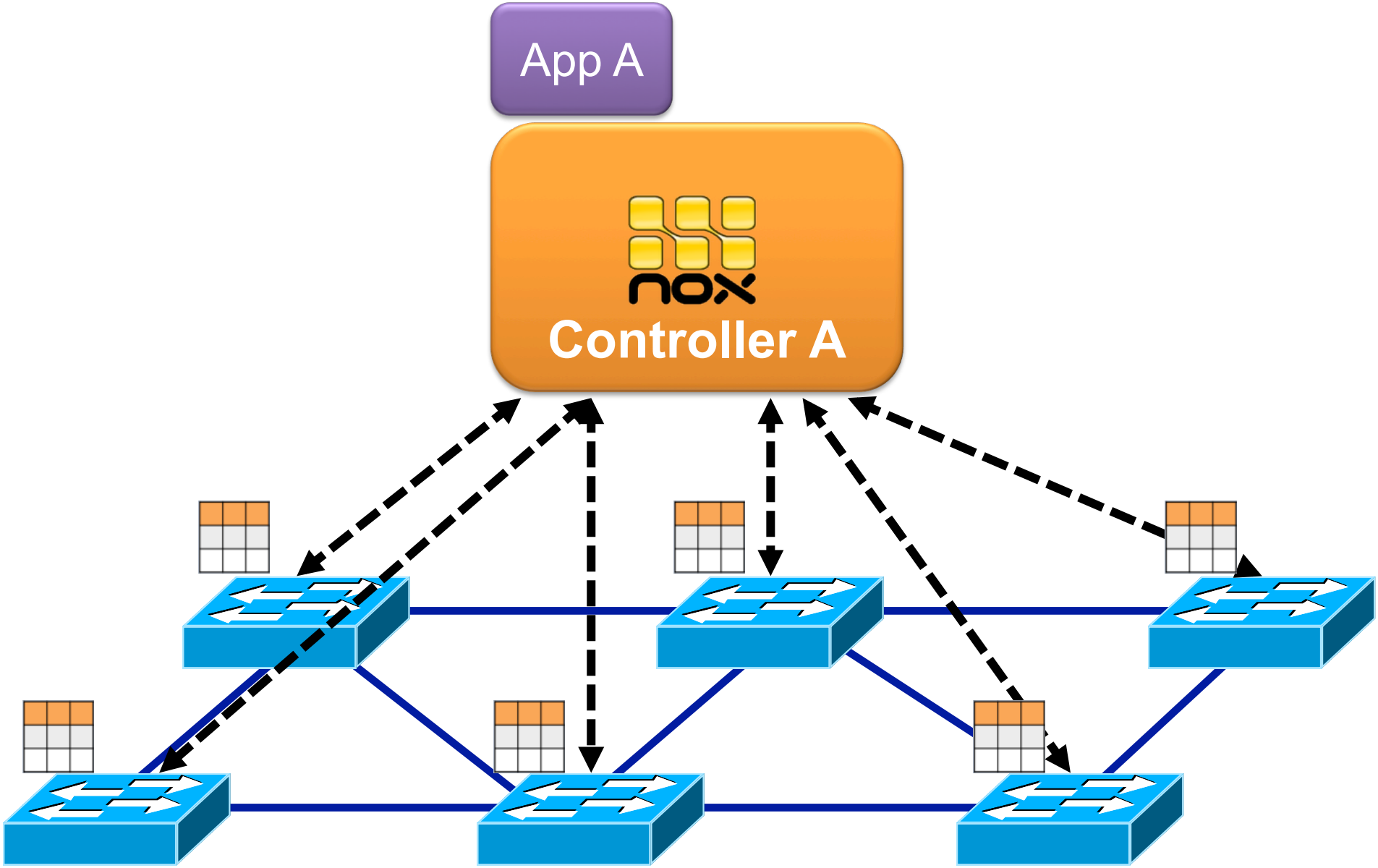
- Secure components for confidentiality
  - To store sensitive data

- Fast and reliable software update and patching

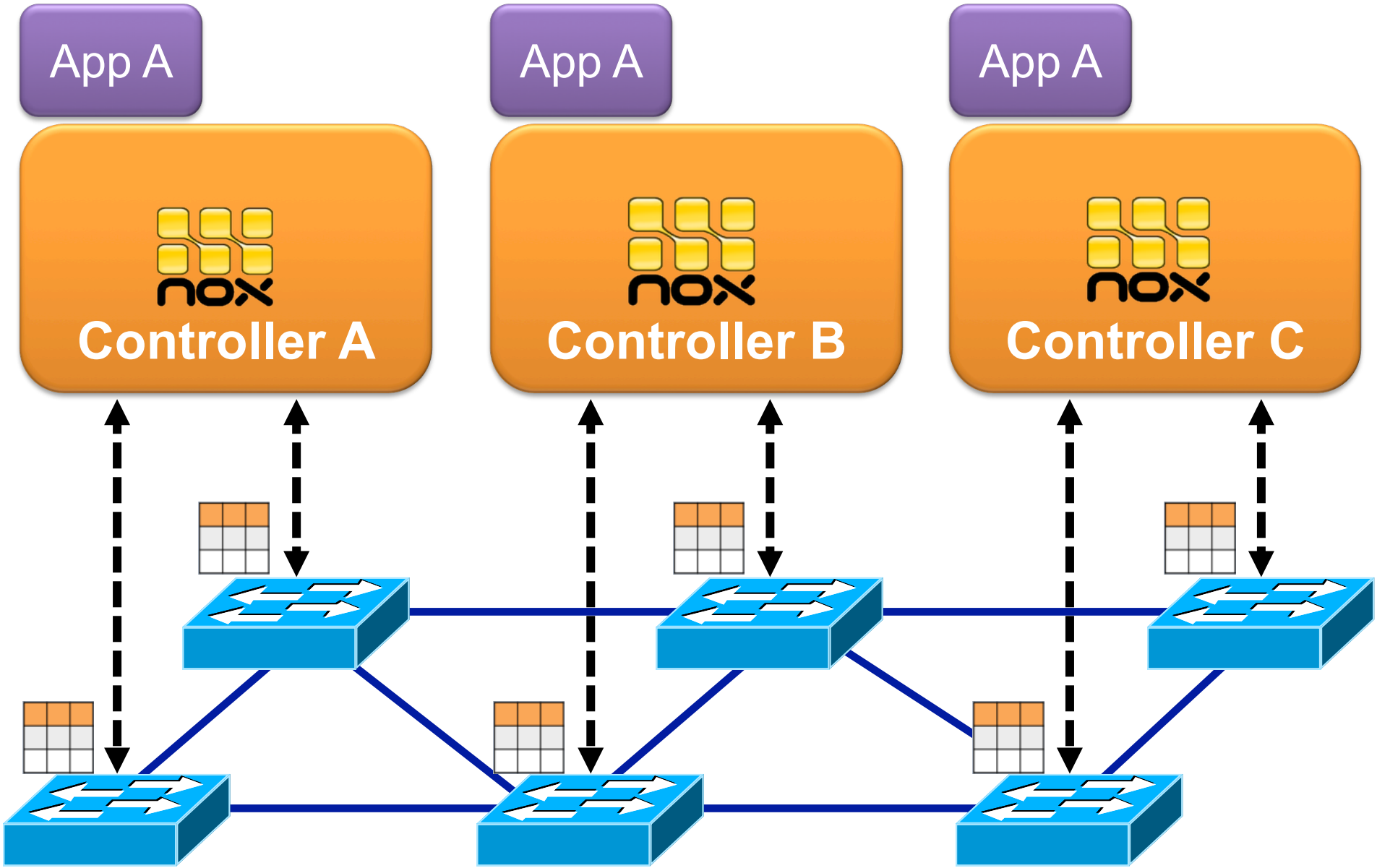
DESIGN OF A SEC&DEP SDN CONTROL PLATFORM

v0.1

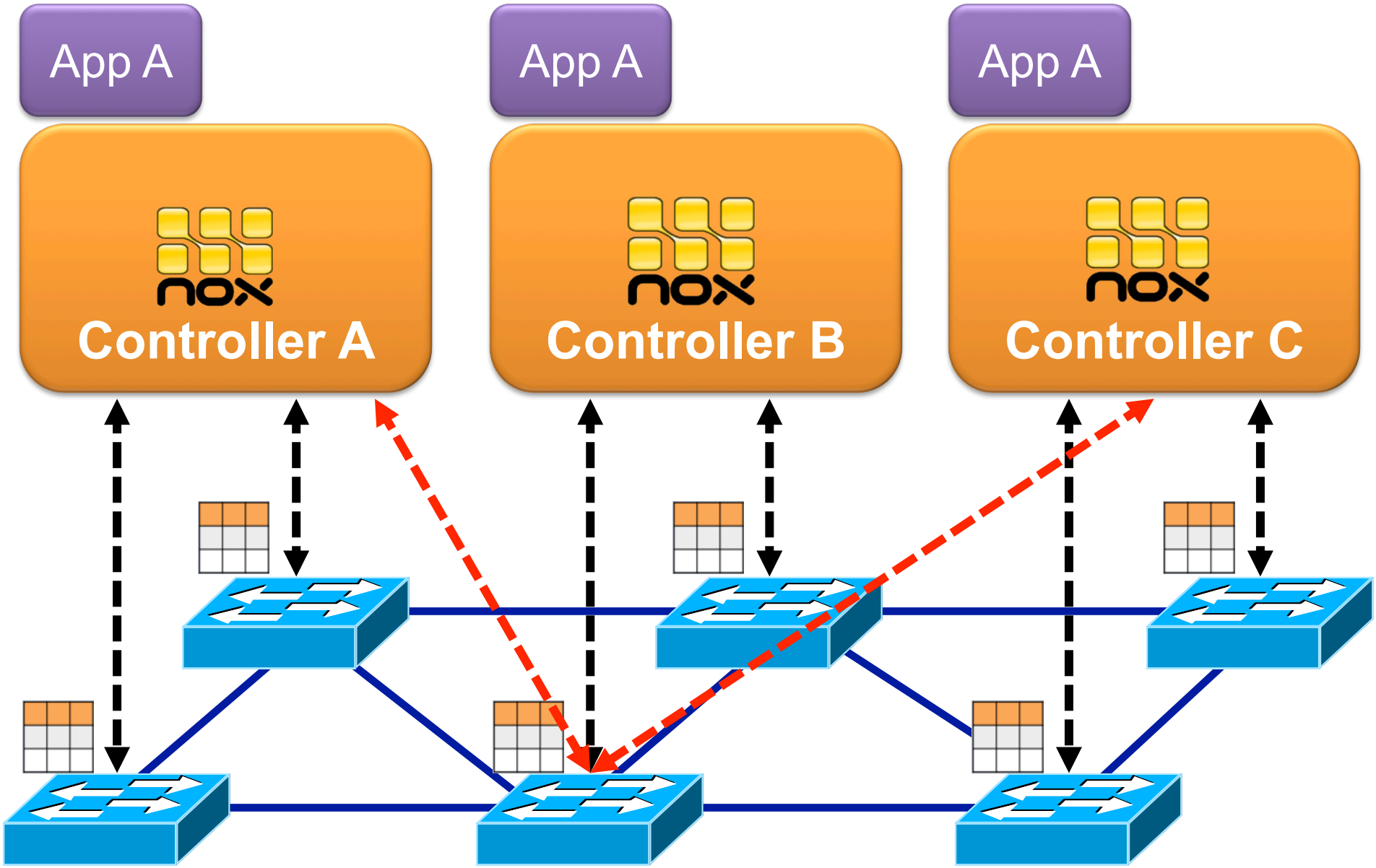
One single centralized controller



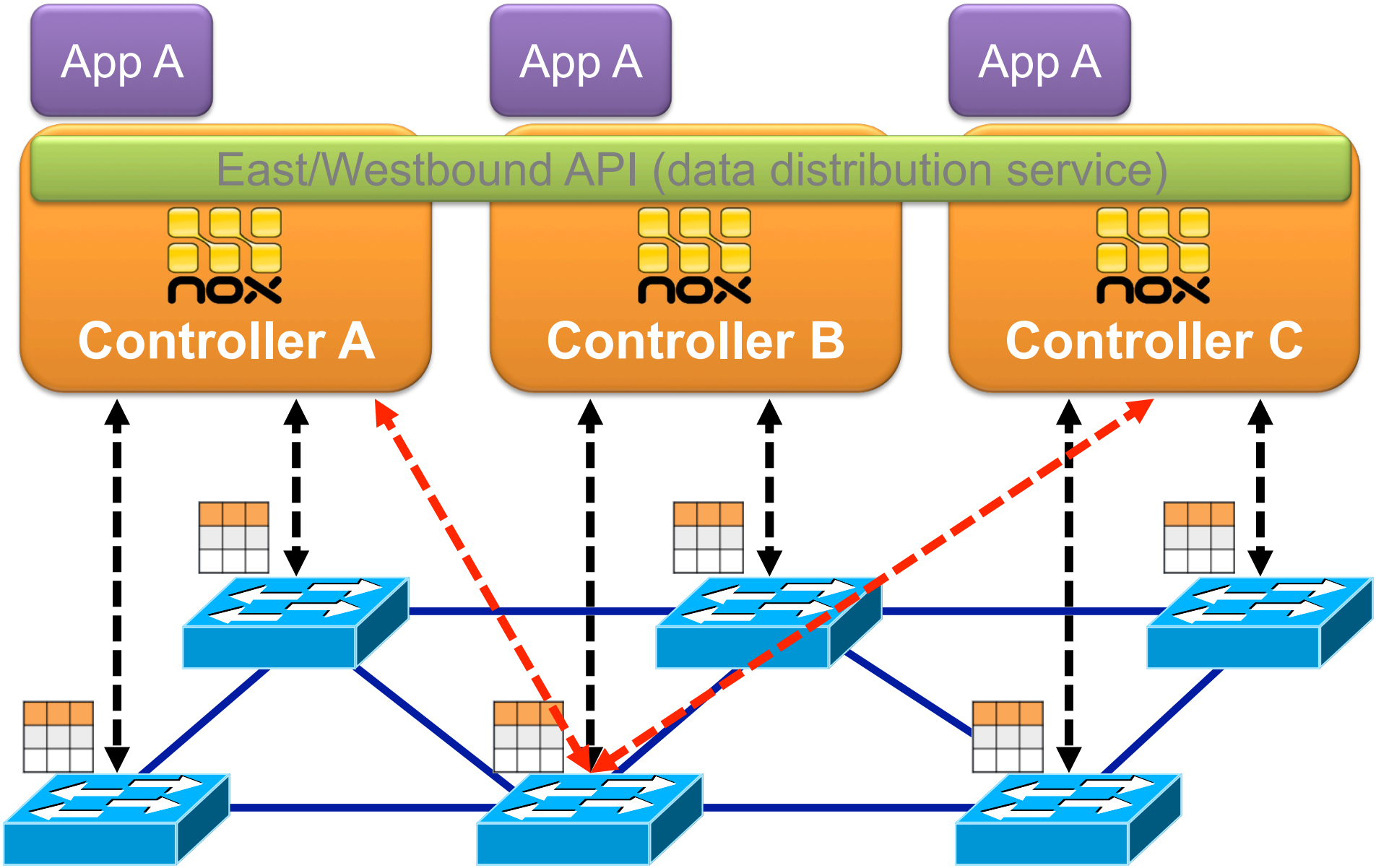
Multiple instances of a centralized controller



Master-slave controllers



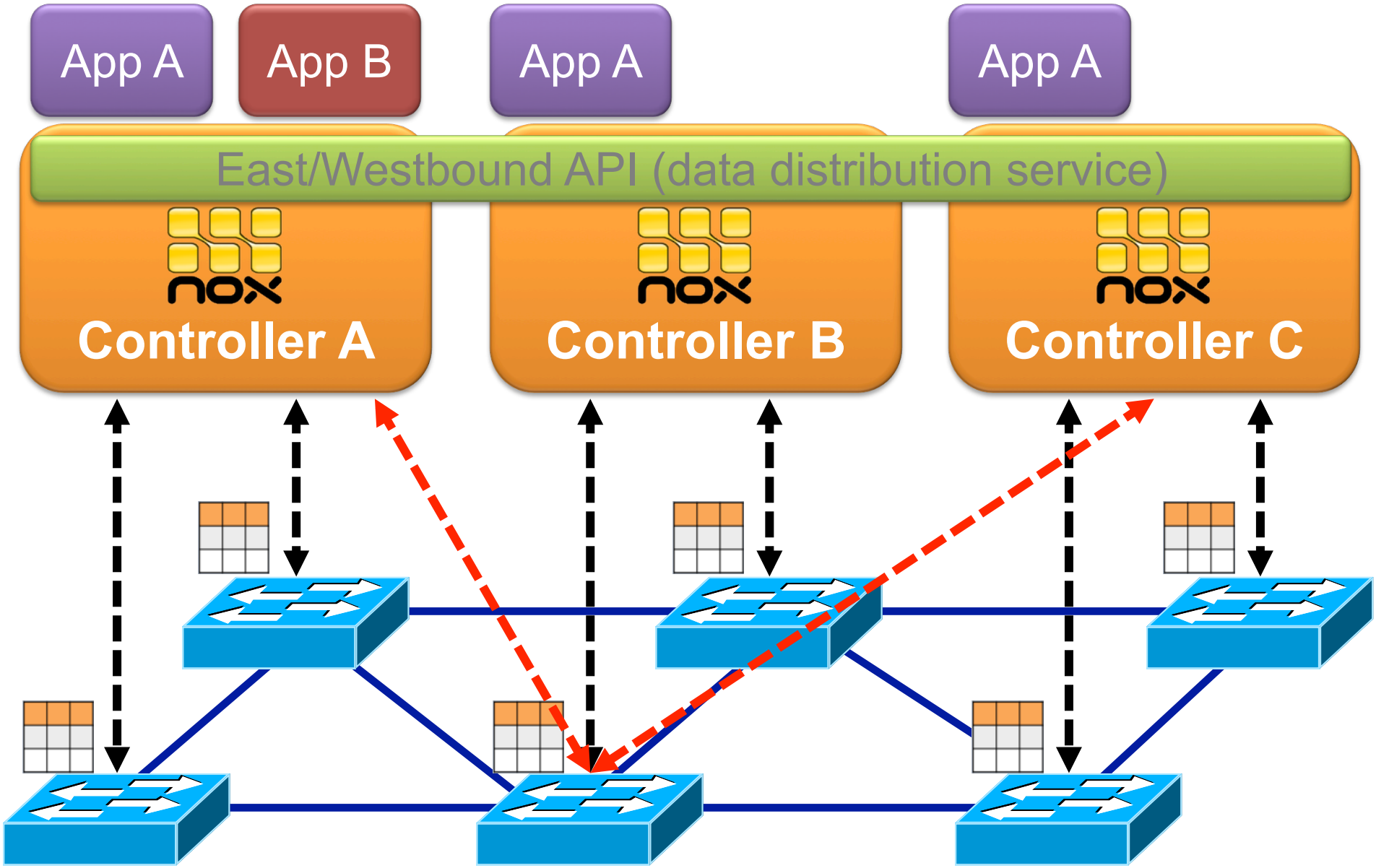
Master-slave controllers



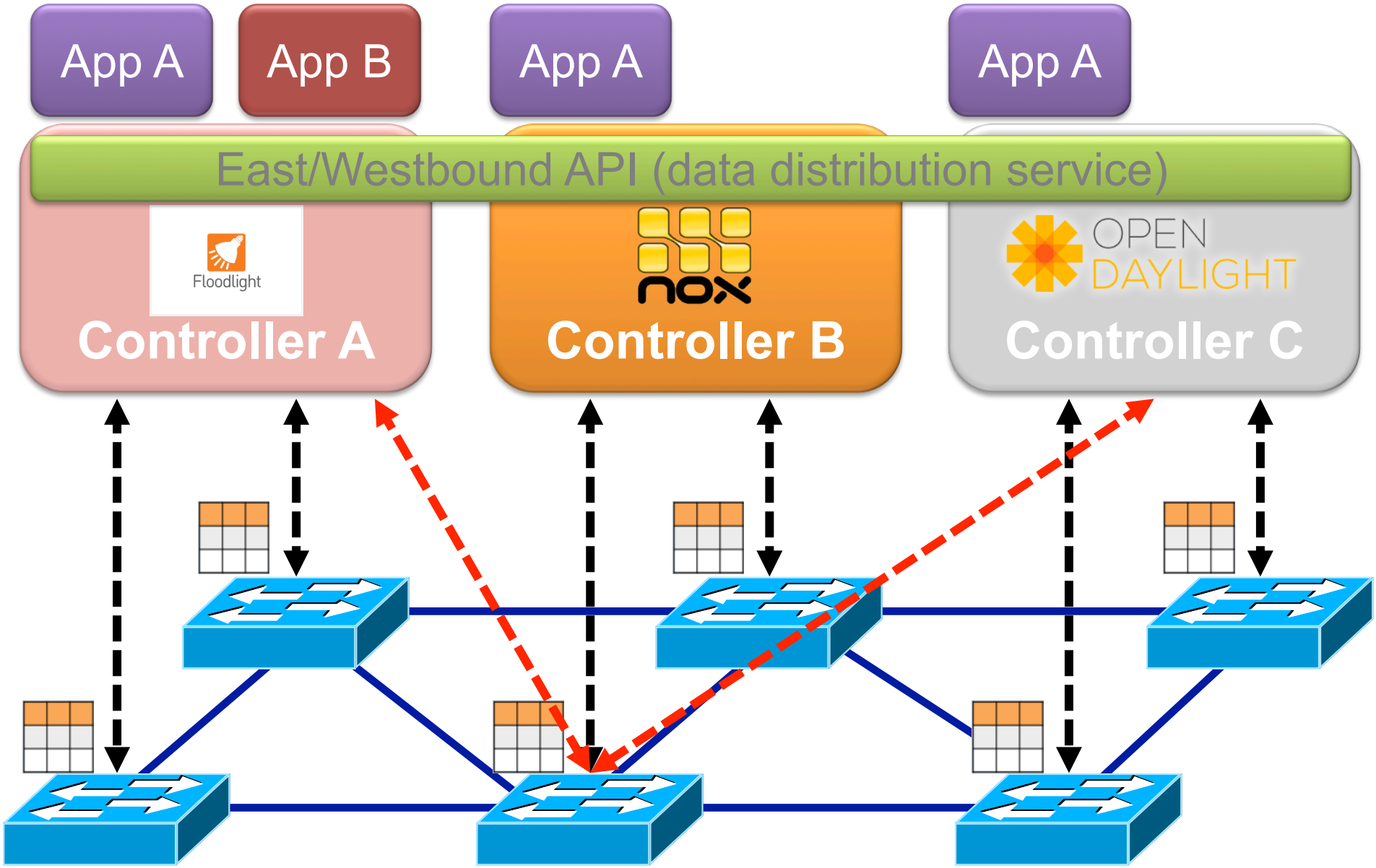
(Aside: [strong] consistency matters)

- Inconsistencies may lead to
  - network loops
  - security issues
  - …

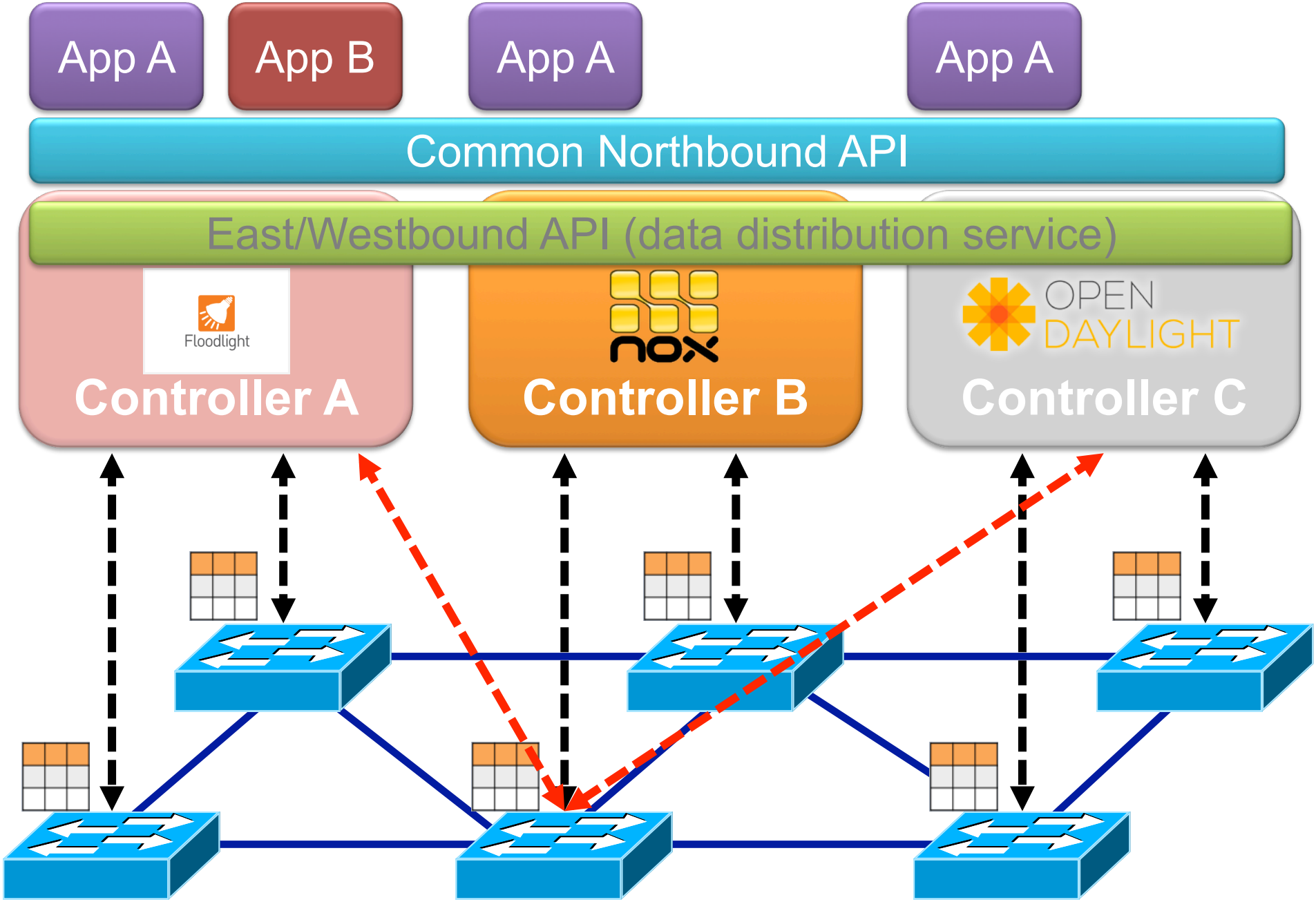
One single app instance (App B) can now configure the whole network



Adding diversity



Adding diversity



Outline

Main threat vectors in SDNs

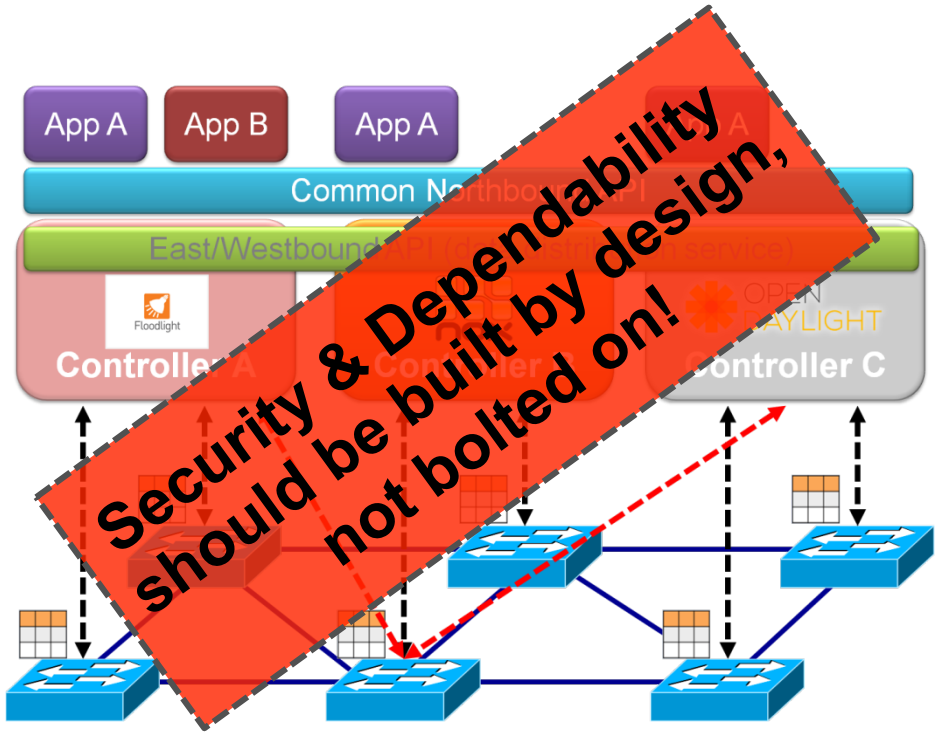
Security & Dependability by design

Final remarks

Our main message

- SDNs bring a very fascinating dilemma
  - an extremely promising **evolution of networking** architectures

    versus
  - a dangerous increase in the **threat surface**.



Check our HotSDN 2013 paper (click link to download)

ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN)

- Diego Kreutz, Fernando M. V. Ramos, Paulo Veríssimo.
  Towards Secure and Dependable Software-Defined Networks.

fvramos@fc.ul.pt
http://www.di.fc.ul.pt/~fvramos/