FACULDADE DE CIÊNCIAS
UNIVERSIDADE DE LISBOA

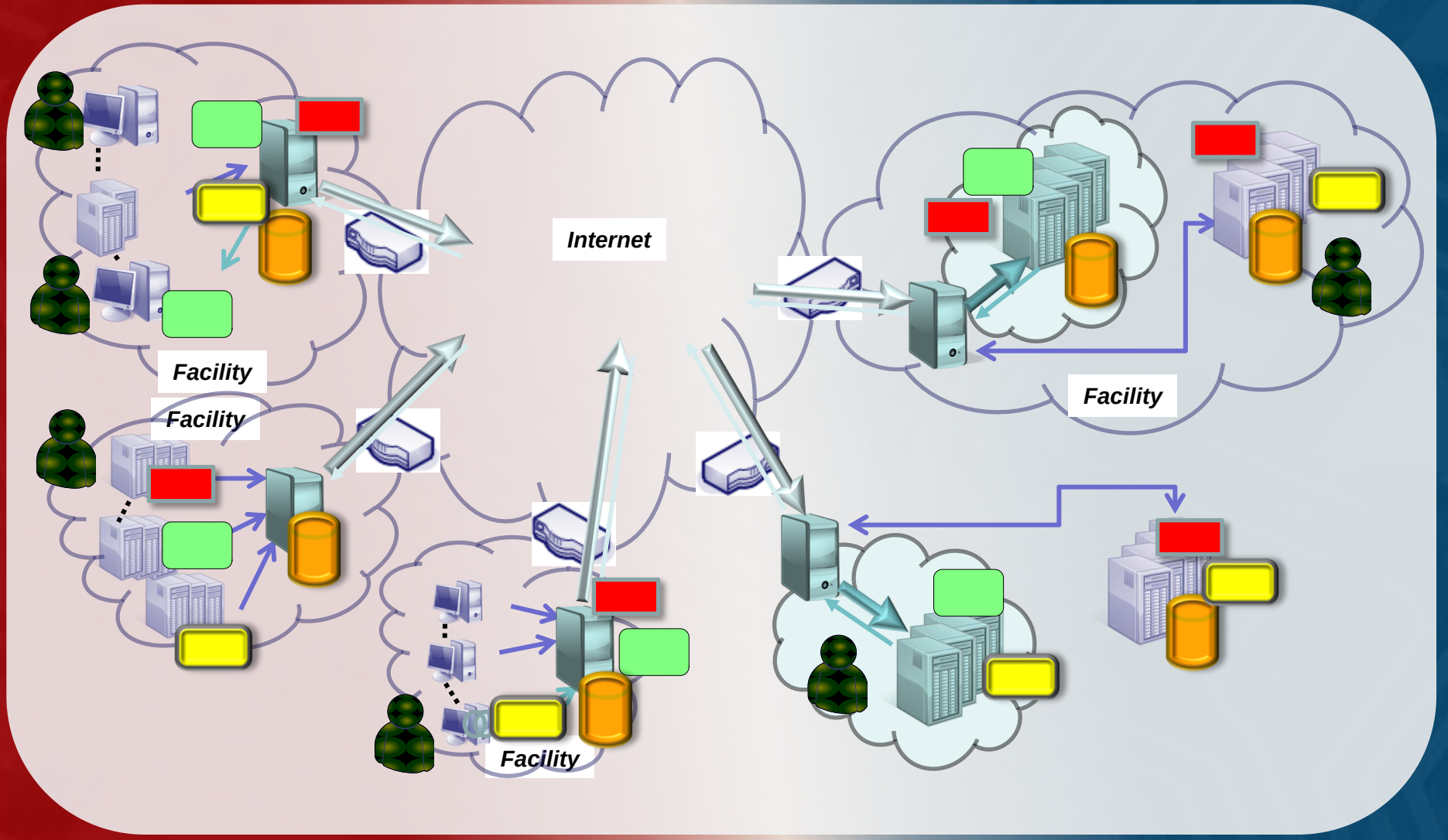
# Are we keeping the security and dependability balance of DevOps in a "cloudified" world?

Paulo Esteves Veríssimo

ULisboa - Faculdade de Ciências - LaSIGE
http://www.di.fc.ul.pt/~pjv

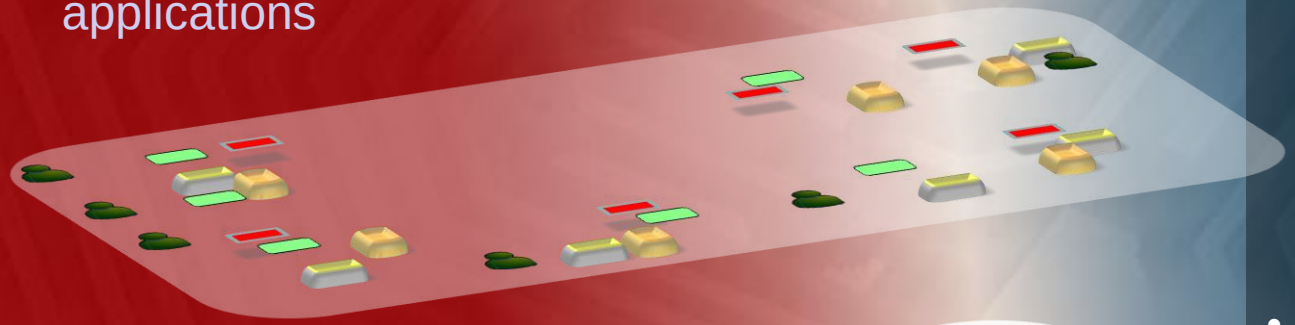
**Research Reports, 66th IFIP WG10.4 meeting**
June 2014

# Classical IT development and operations (DevOps)

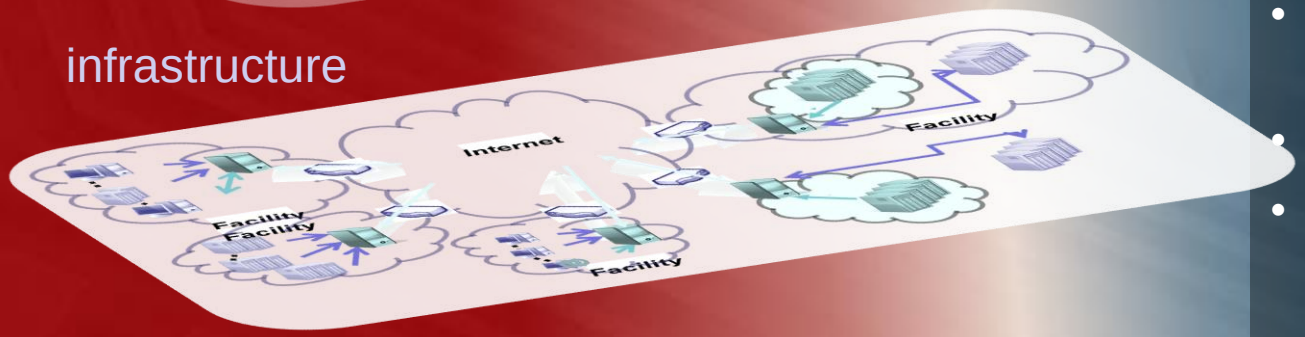


# Security and dependability perspective
## *(classical IT)*

platforms and applications



infrastructure

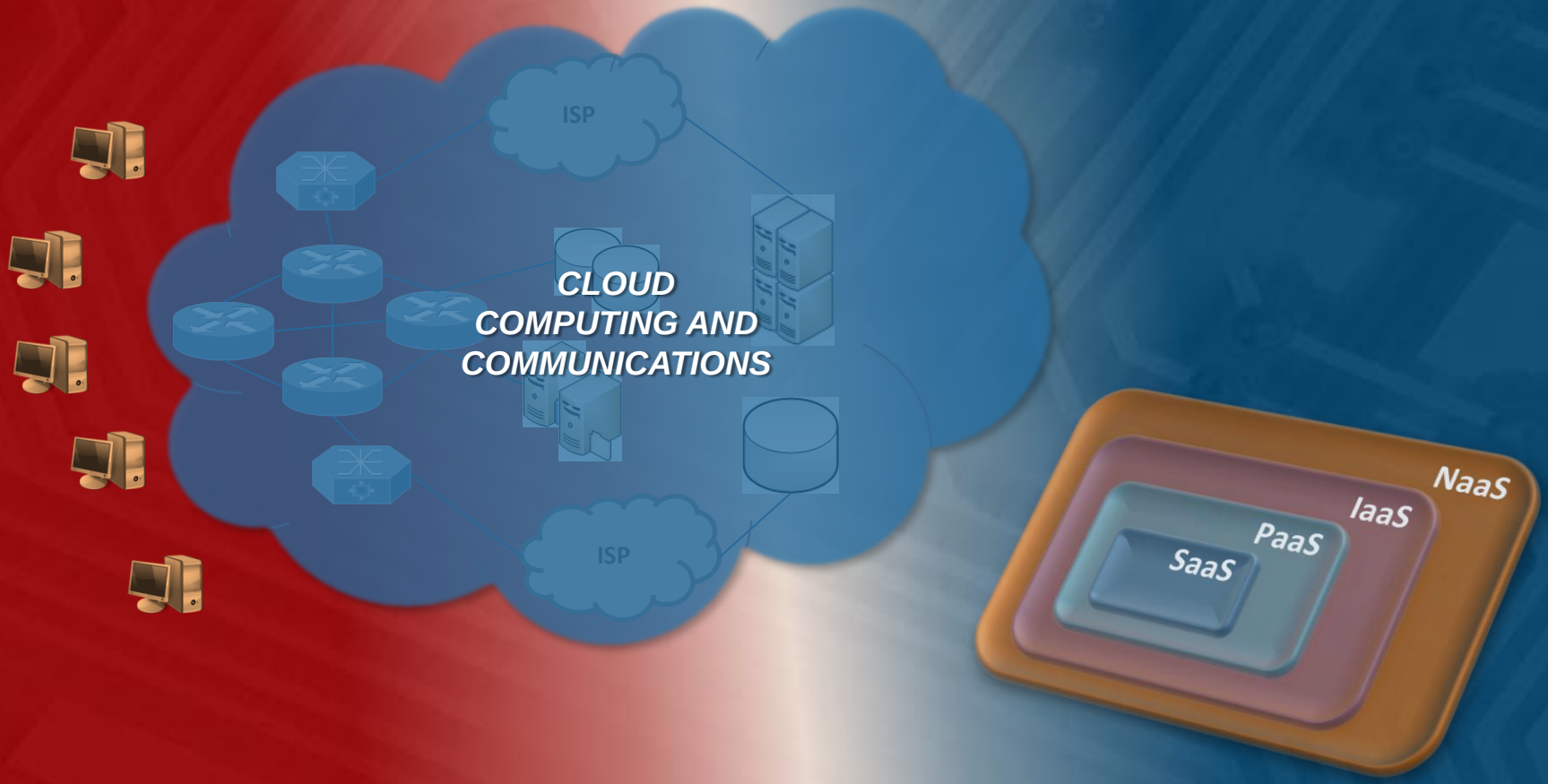



- short-term and dynamic dev/test/deploy cycle
- manageable Sec&Dep
- high separation from infrastructure

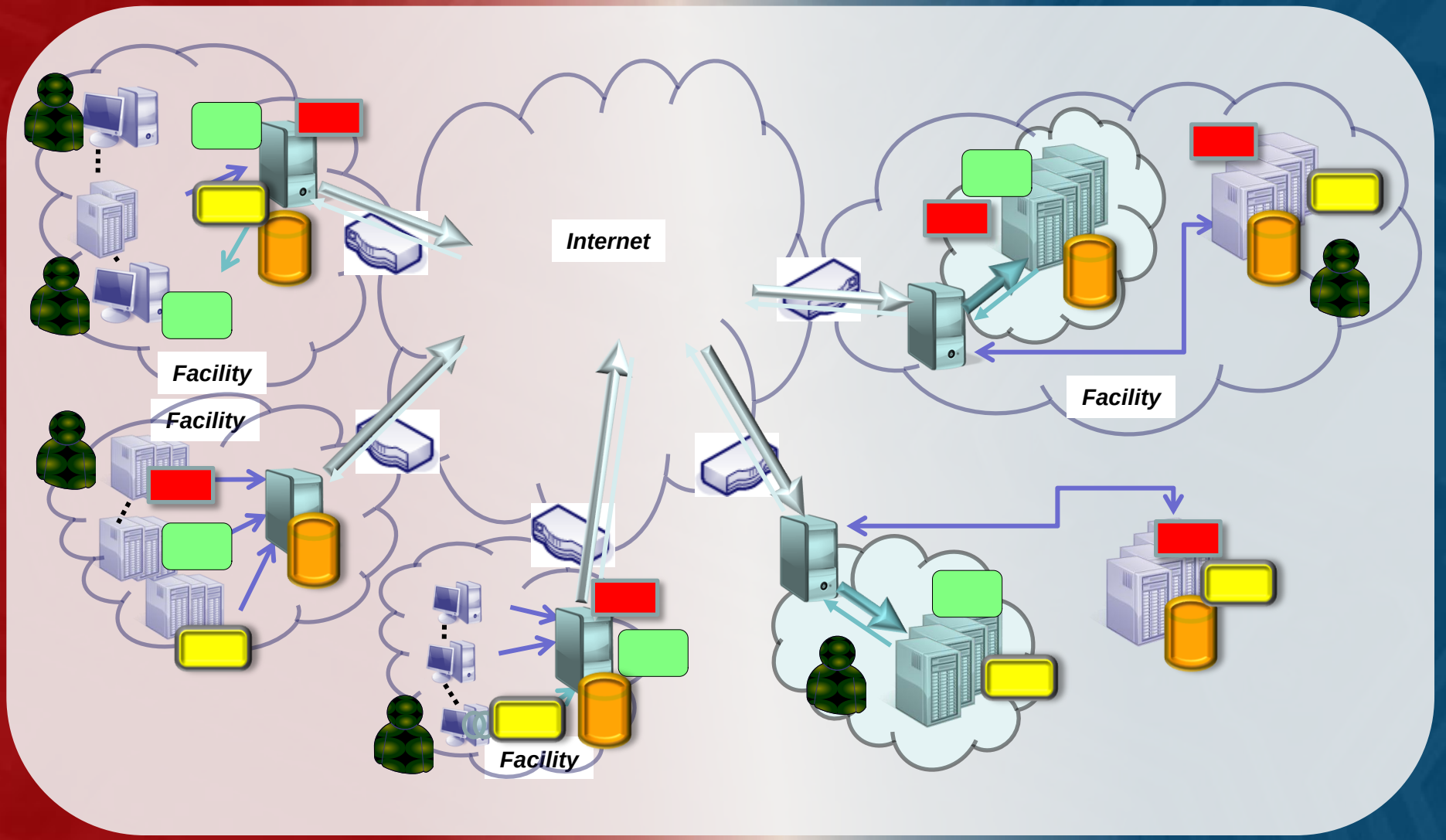
- long-term and stable dev/test/deploy cycle
- good Sec&Dep
- high insulation

# Computing and communications are becoming pervasive commodities

*"buying computing and communications as buying electricity"*



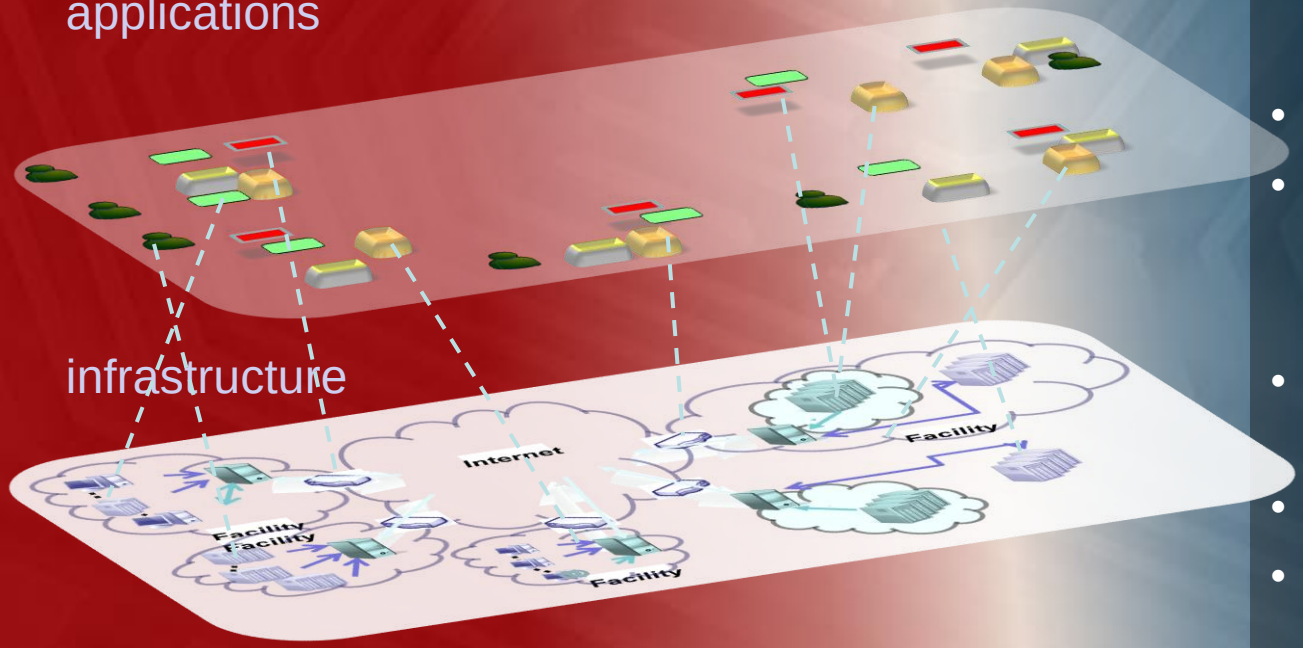
# DevOps in a cloud-oriented IT world



# Security and dependability perspective
## *(classical IT)*

platforms and applications

infrastructure

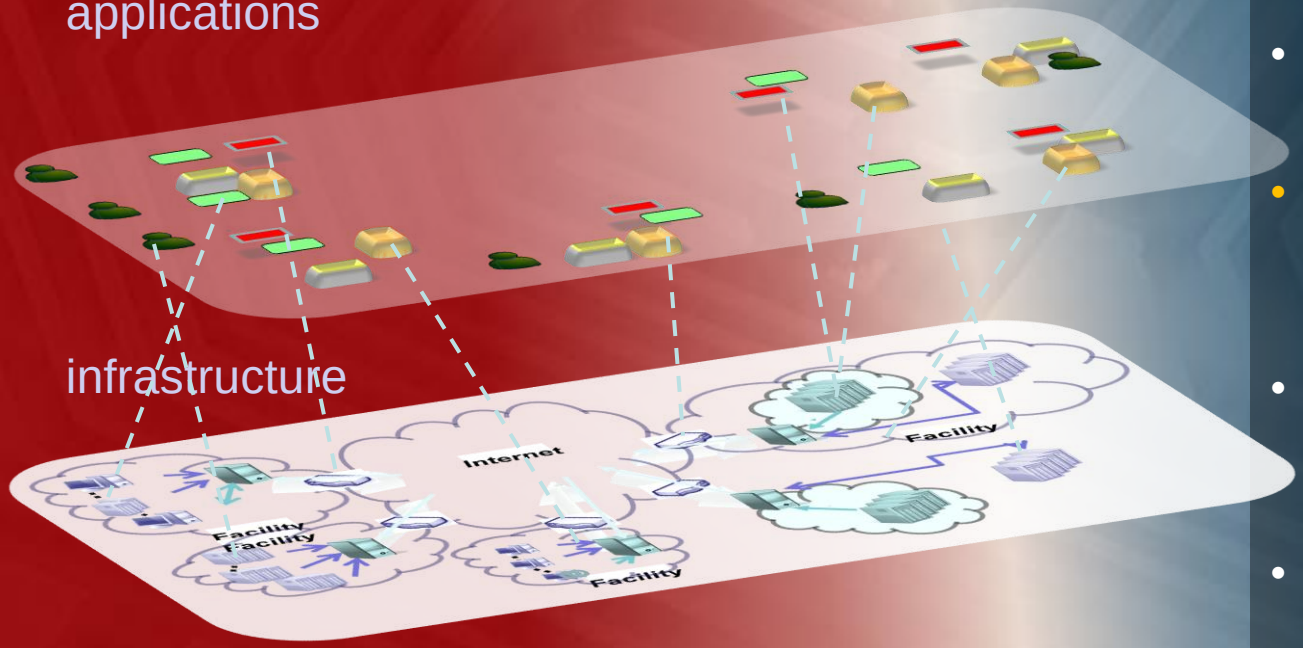



- short-term and dynamic dev/test/deploy cycle
- manageable Sec&Dep
- high separation from infrastructure

- long-term and stable dev/test/deploy cycle
- good Sec&Dep
- high insulation

# Security and dependability perspective
## *("cloudified" IT)*

platforms and applications




- short-term and dynamic dev/test/deploy cycle
- manageable Sec&Dep ?

- weak separation between both layers

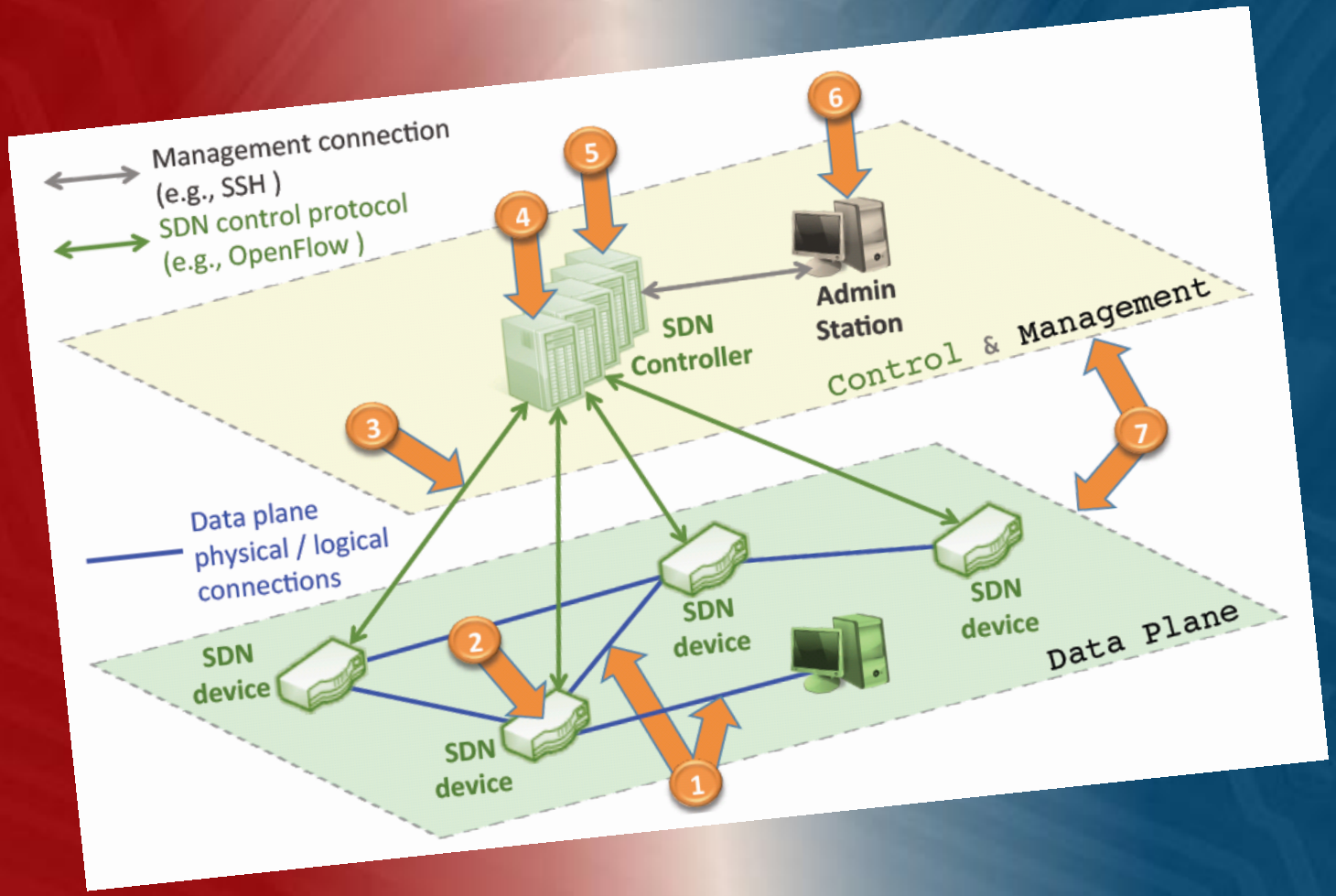
- short-term and dynamic dev/test/deploy cycle
- manageable Sec&Dep ?

# Security and dependability balance has been disturbed

- Fundamentals no longer valid:
  - High uncertainty of both infrastructure and platforms/applications
- Emergence of new vulnerabilities:
  - interference
  - interdependence
- Emergence of new threats:
  - compounded attack surfaces

- Where to look?
  - Virtualization (VMM, etc.)
  - SDNs

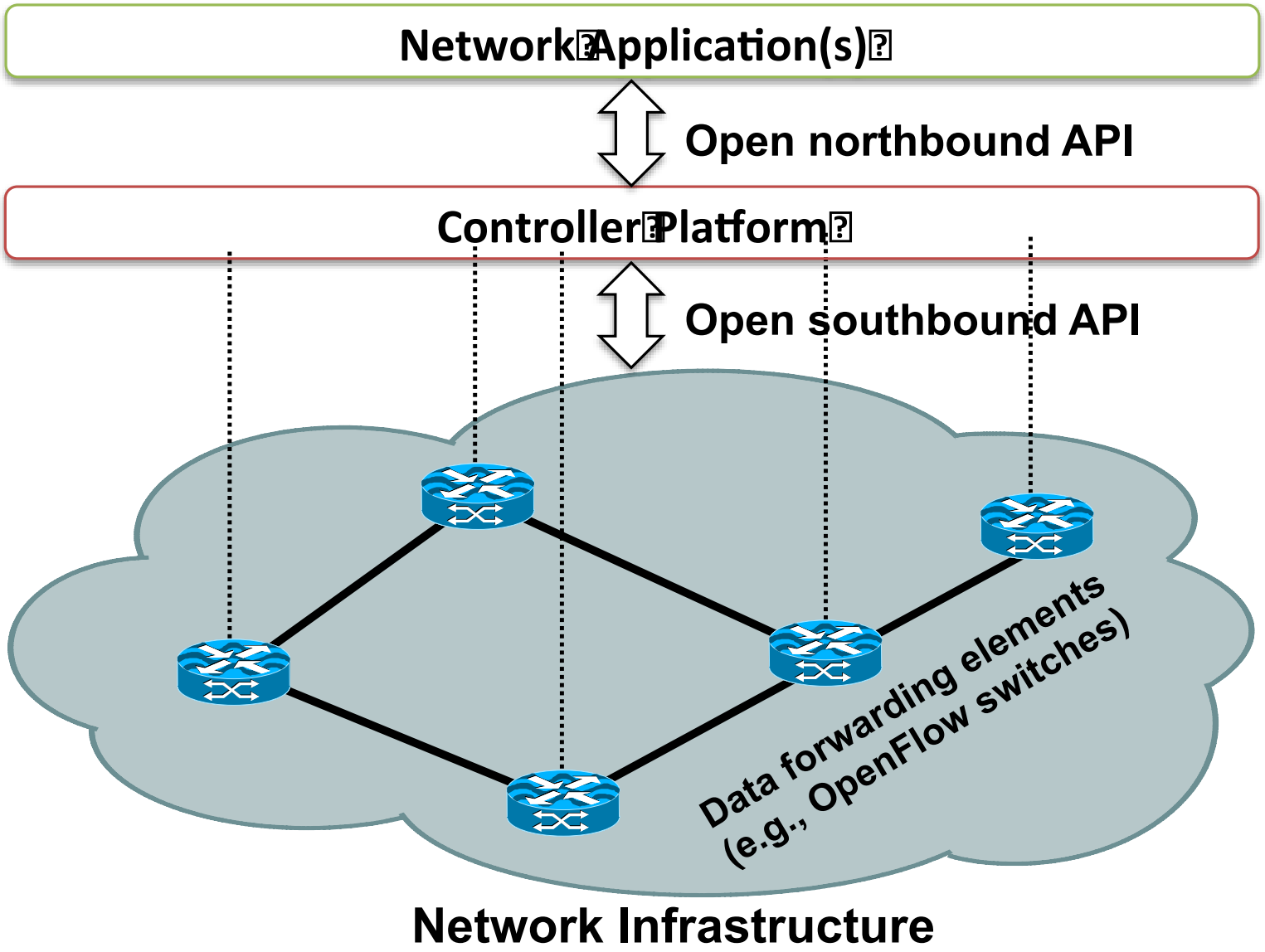
# Threats to SDN systems



# Software-Defined Networks

- Decoupled control and data planes
- Logically centralized controllers
- Programmability
- Openness
- Interoperability

# Software-Defined Networks



# Problem statement

ironically, main causes of concern lie in SDN's main benefits:

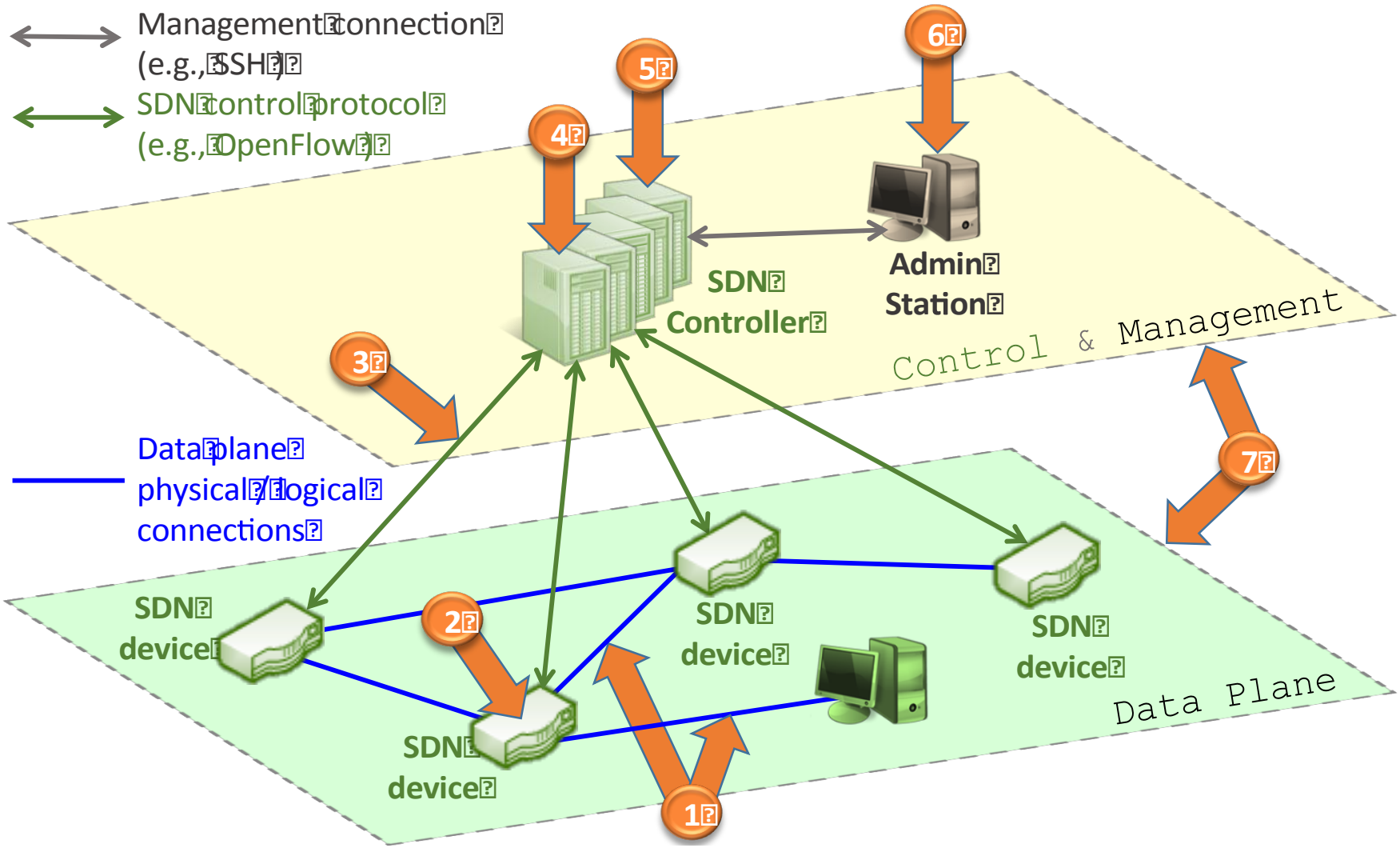
*network programmability and control logic centralization bring in new fault and attack planes*

*which open the doors for new threats that did not exist before or were harder to exploit*

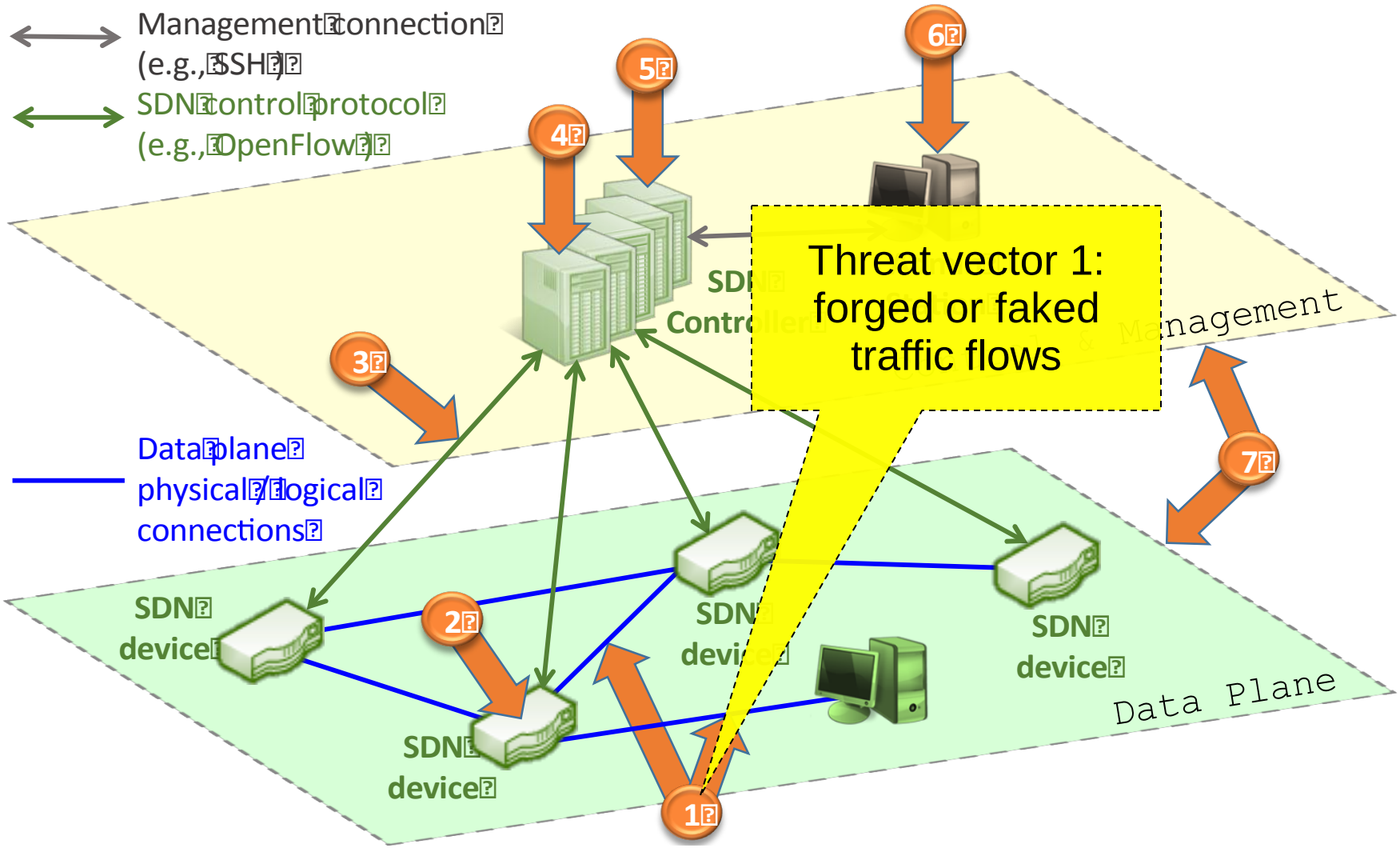
comparatively smaller diversity in SDNs added to high configurability and programmability:

*an attack similar to Stuxnet could have dramatic consequences*

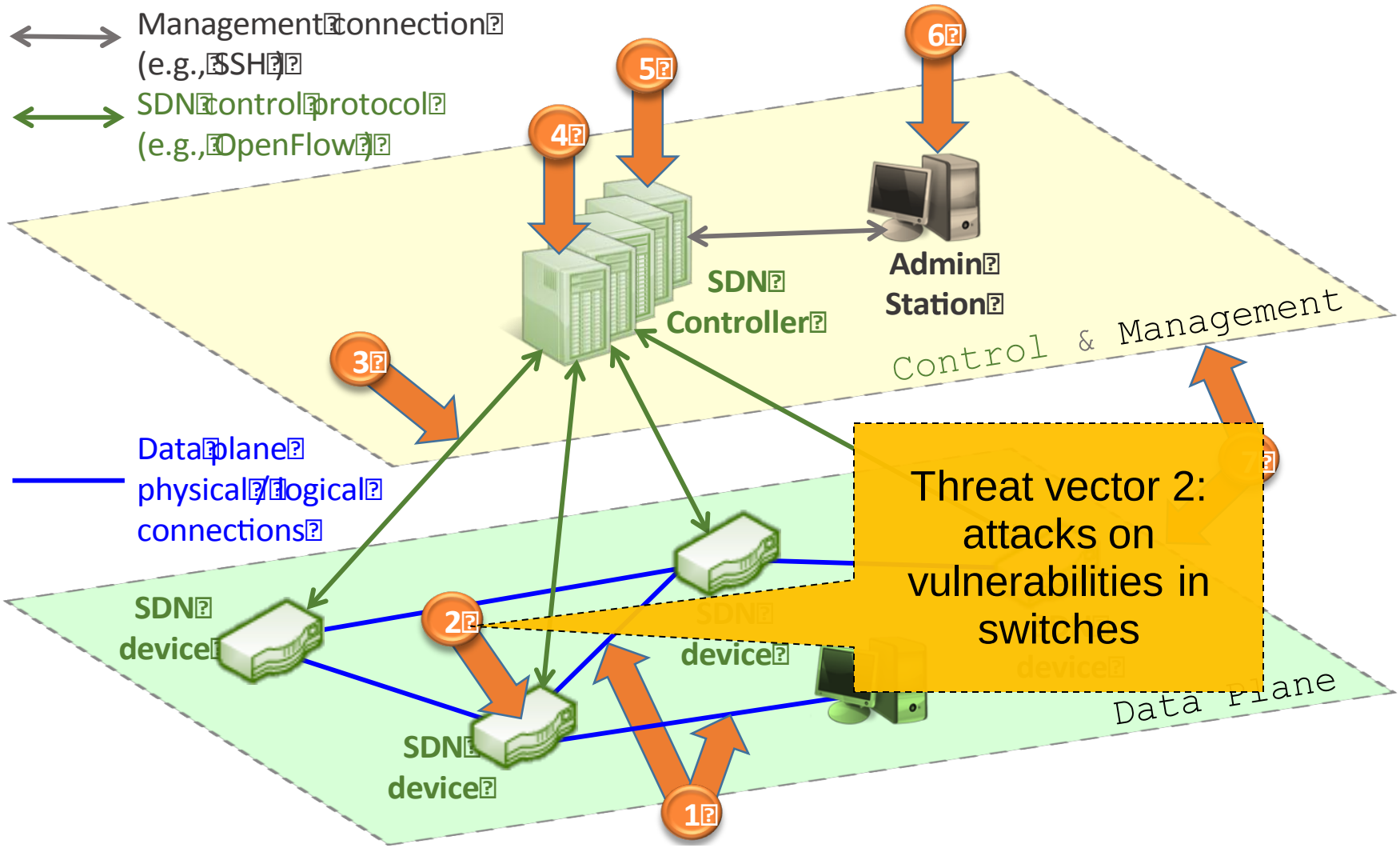
# Threat vectors



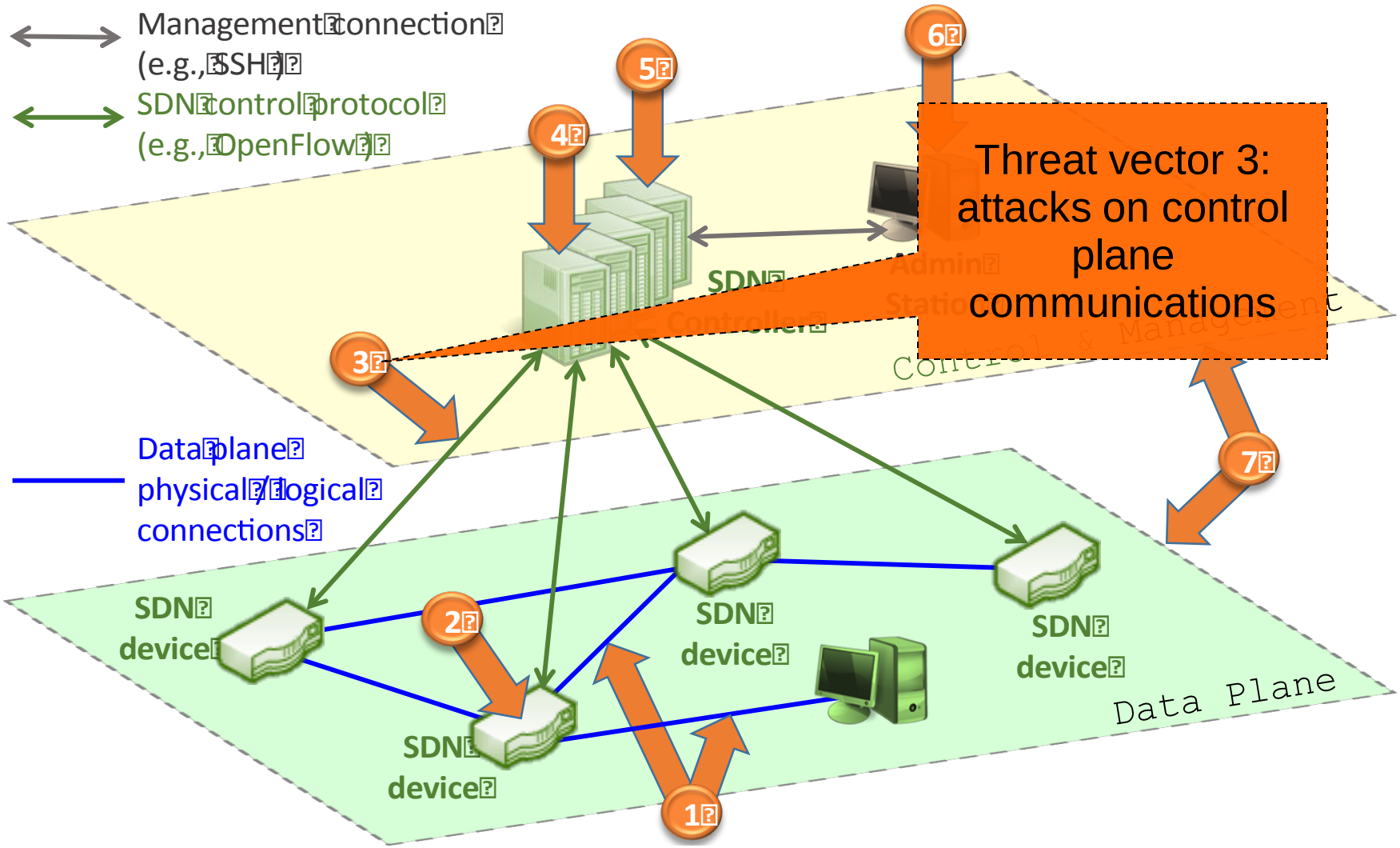
# Threat vectors



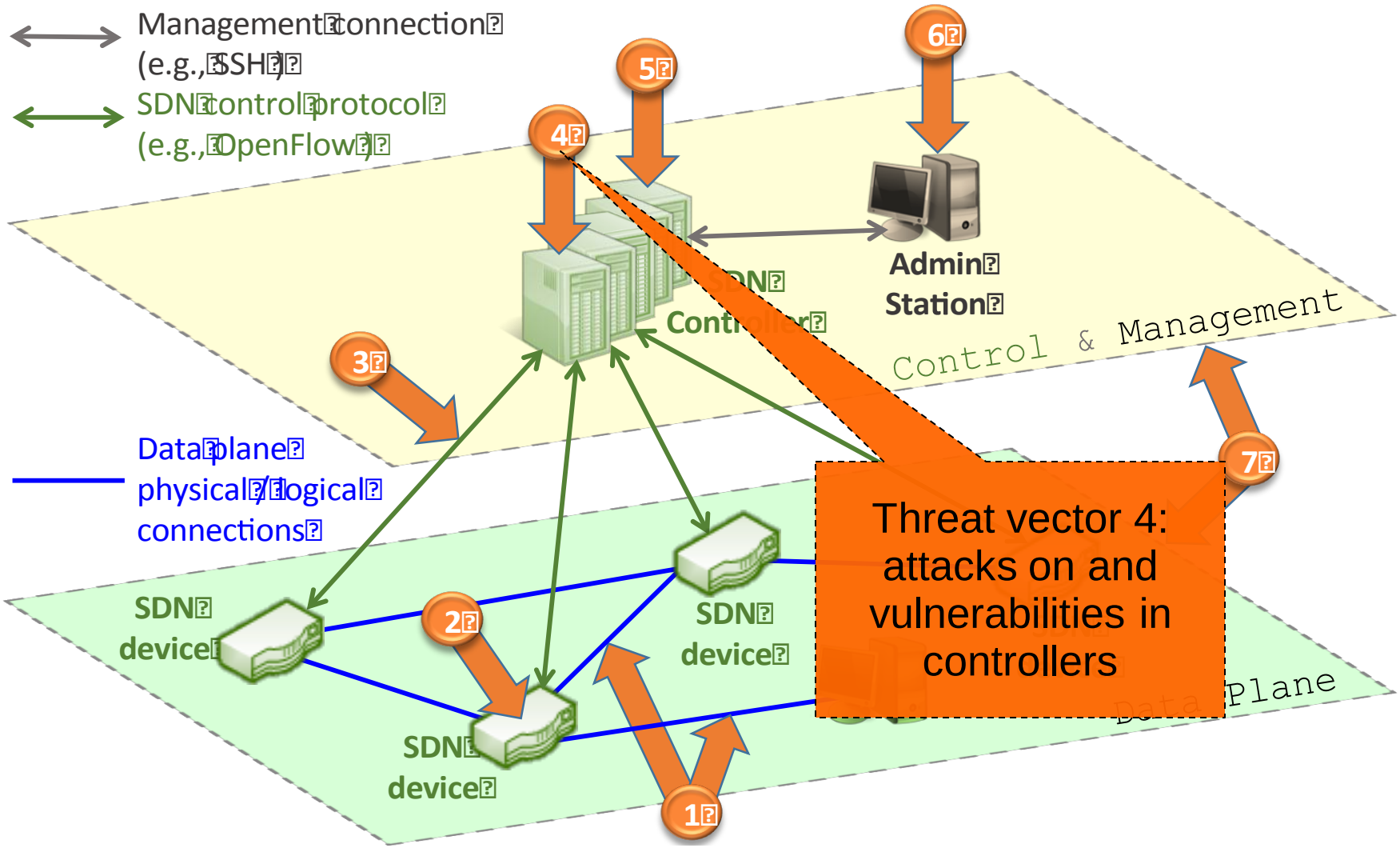
# Threat vectors



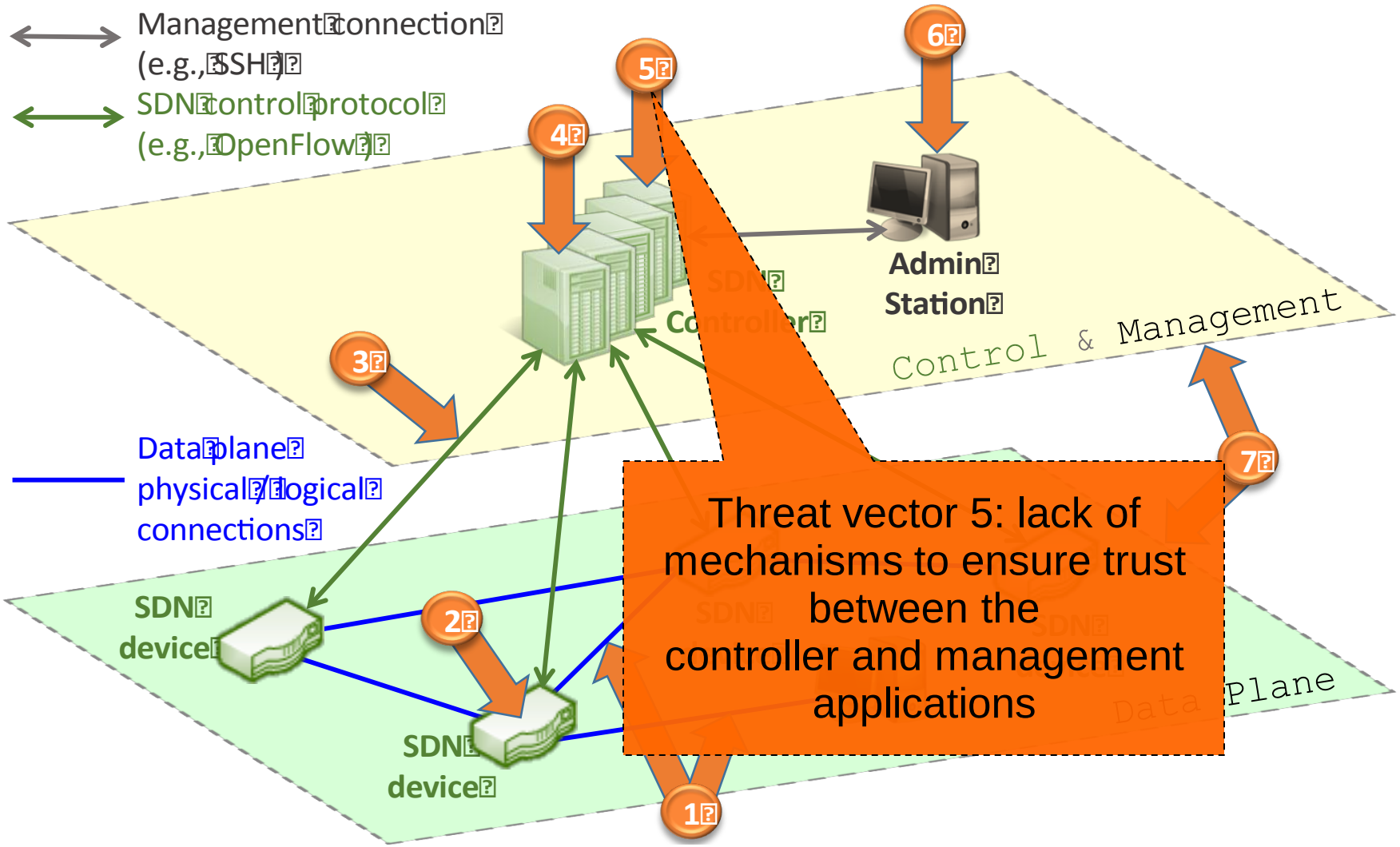
# Threat vectors



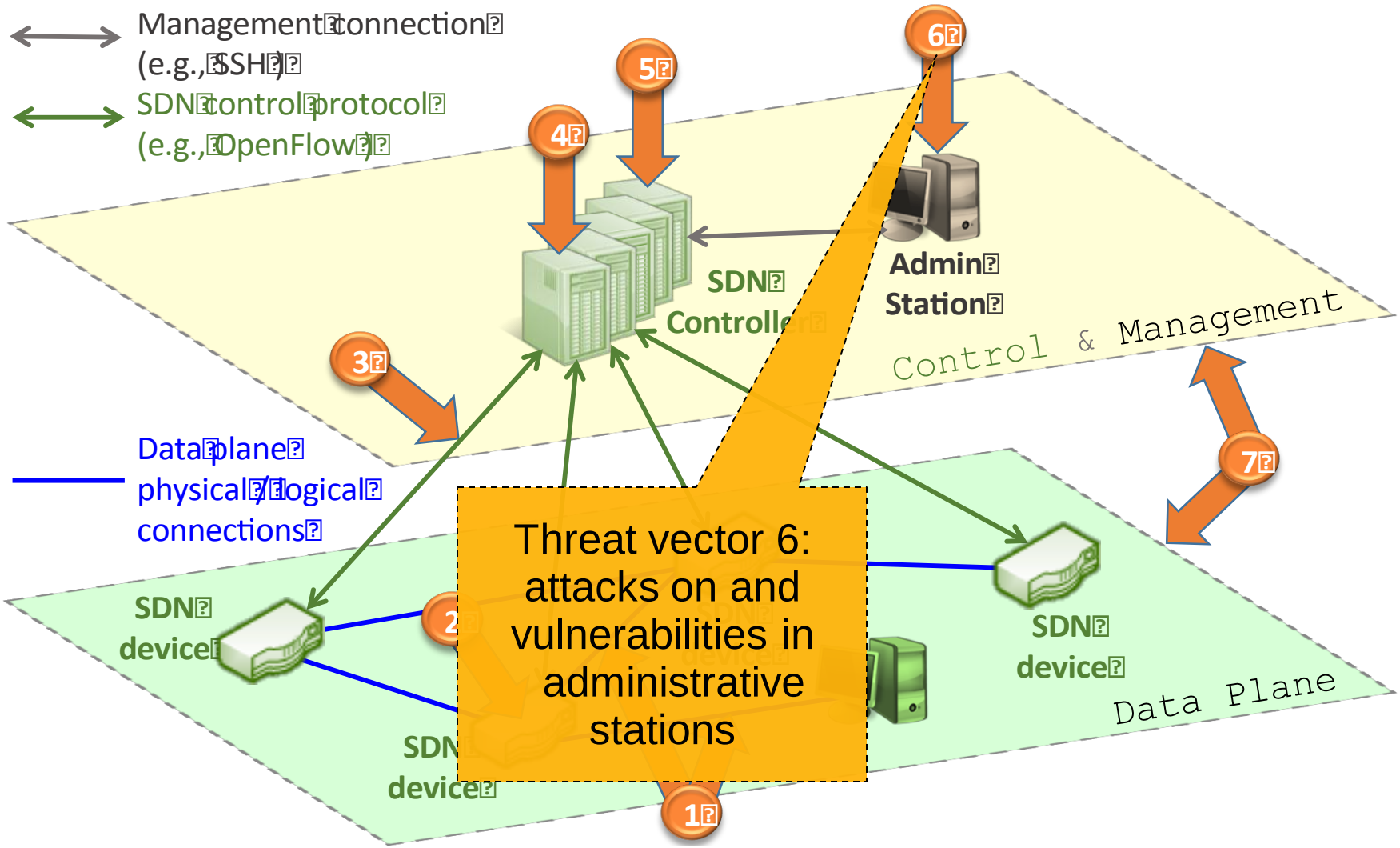
# Threat vectors



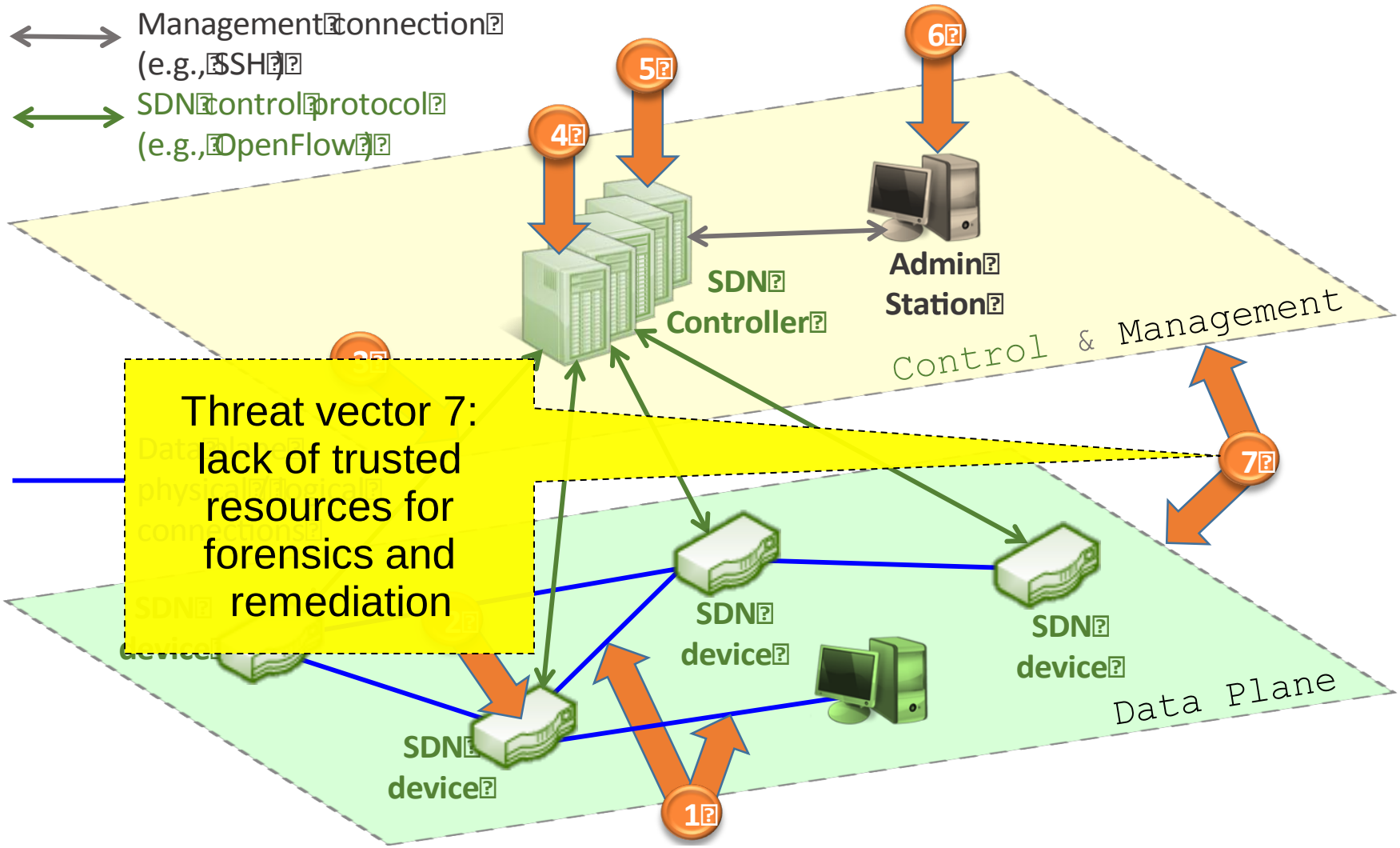
# Threat vectors



# Threat vectors



# Threat vectors

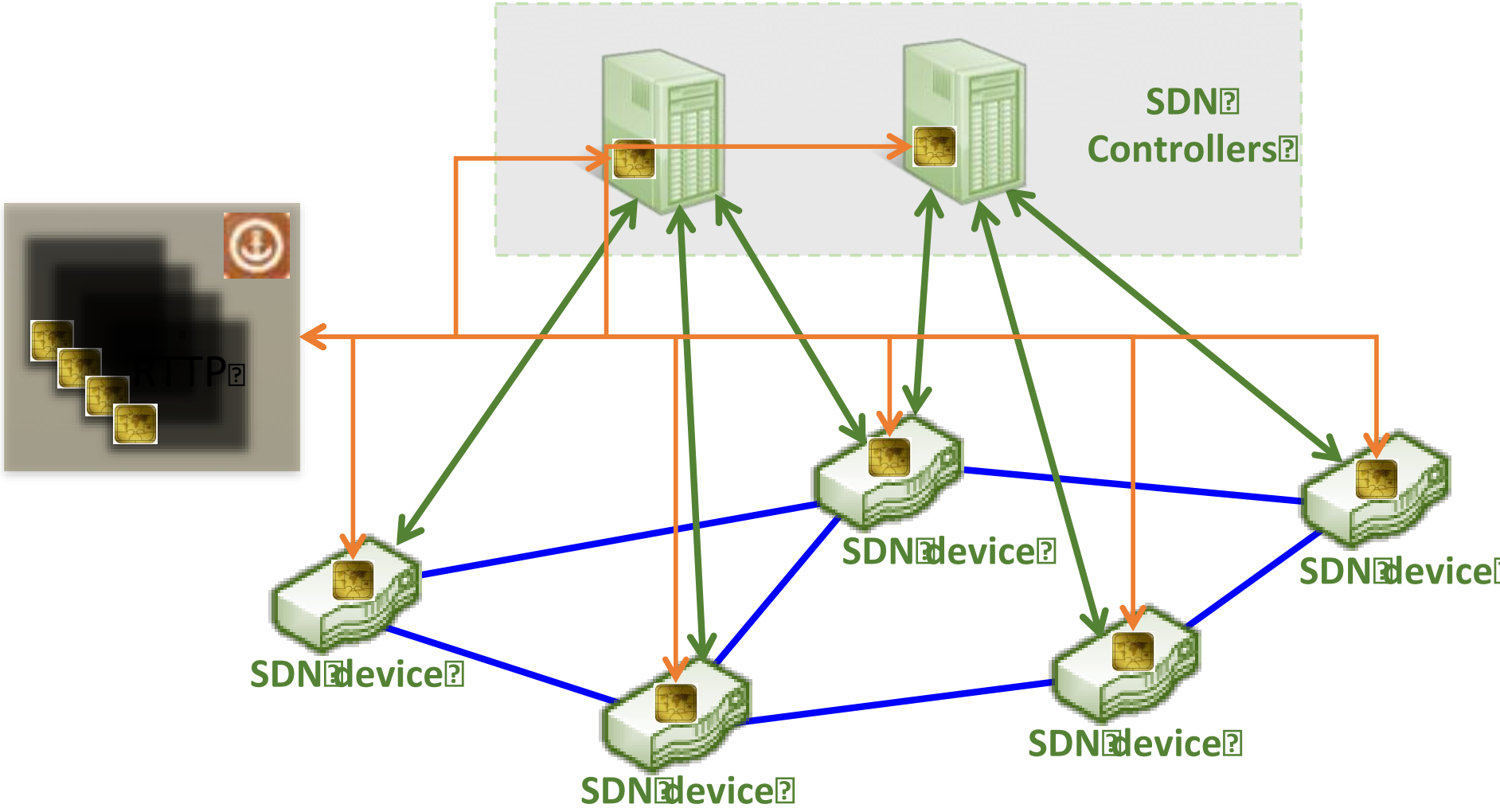


# Threat vectors

| Threat | Specific to SDN? | Consequences in SDN |
|---|---|---|
| Vector 1 | no | can be a door for DoS attacks |
| Vector 2 | no | but now the impact is potentially augmented |
| Vector 3 | yes | communication with logically centralized controllers can be explored |
| Vector 4 | yes | controlling the controller may compromise the entire network |
| Vector 5 | yes | malicious applications can now be easily developed and deployed on controllers |
| Vector 6 | no | but now the impact is potentially augmented |
| Vector 7 | no | it is still critical to assure fast recovery and diagnosis when faults happen |

# Proposed Approach: RTTP

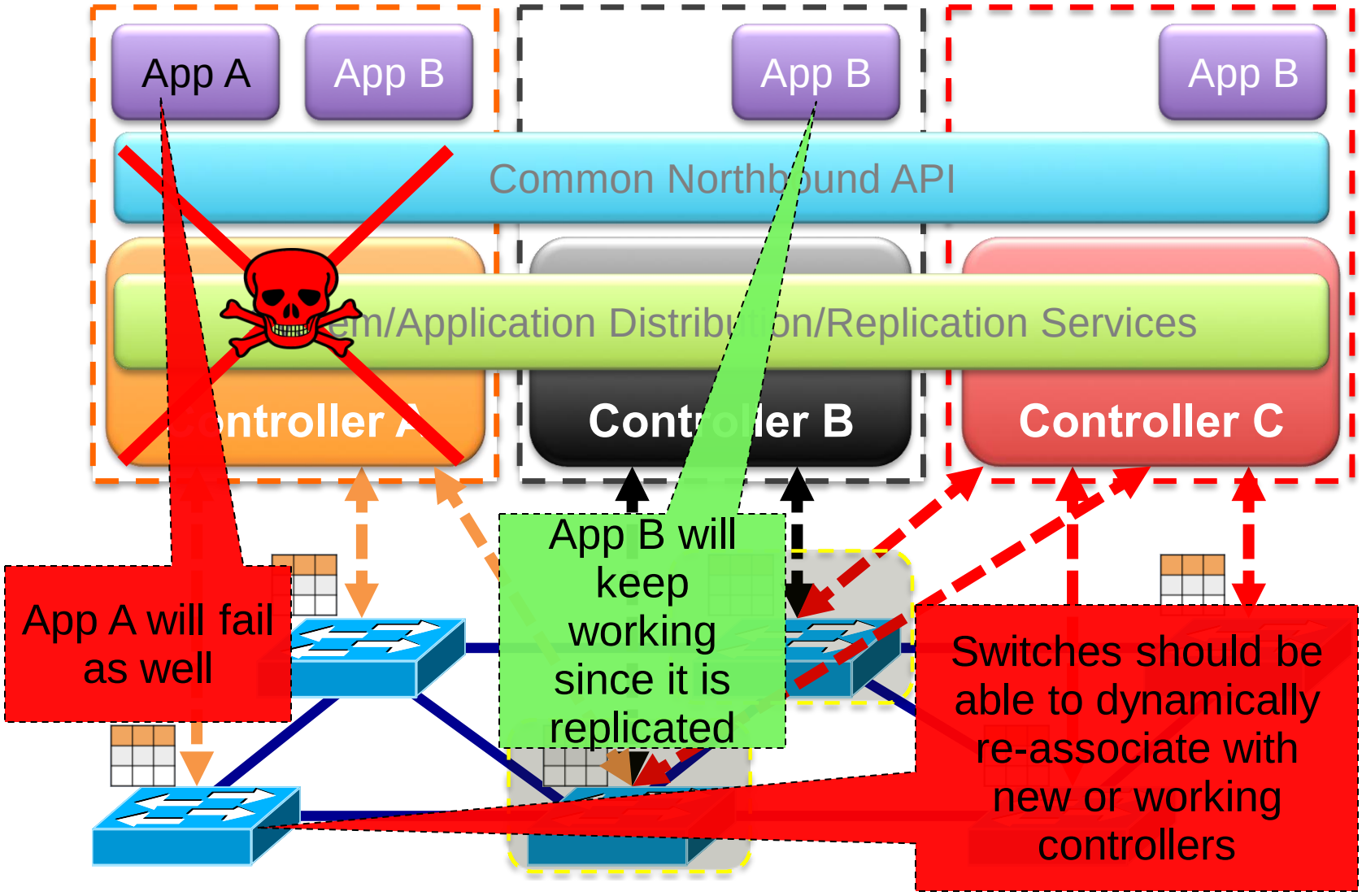
**Resilient and Trustworthy Third Party**



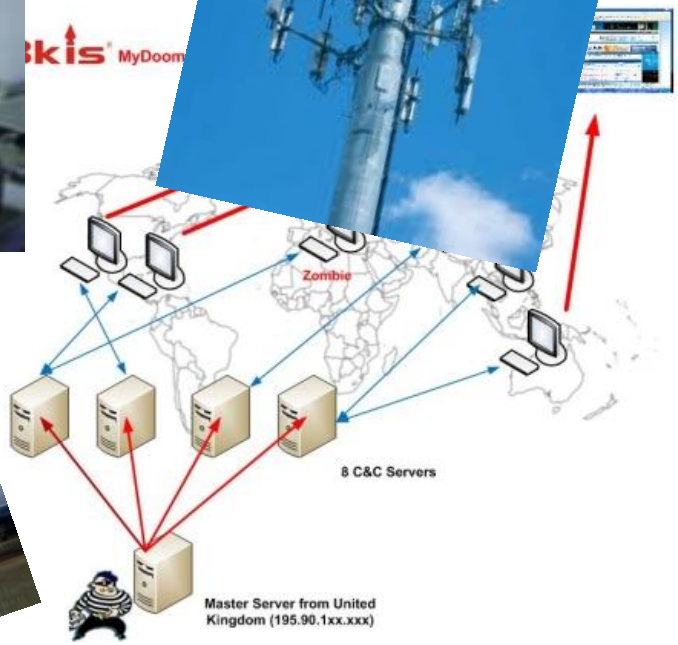
# Security & Dependability mechanisms for SDN

- Replication
- Diversity
- Self-healing mechanisms
- Dynamic device association
- Trust between controllers and devices

# Security & Dependability




www.MyPE.co.za


Zombie
8 C&C Servers
Master Server from United Kingdom (195.90.1xx.xxx)

**Thank You!**