



SECURING AGAINST INTRUDERS AND OTHER THREATS
THROUGH A NFV-ENABLED ENVIRONMENT
[H2020 - Grant Agreement No. 700199]

Il progetto SHIELD: modern network-based cybersecurity

Antonio Lioy

Politecnico di Torino – Dip. Automatica e Informatica

lioy@polito.it



ubiwhere



POLITECNICO
DI TORINO



Telefonica

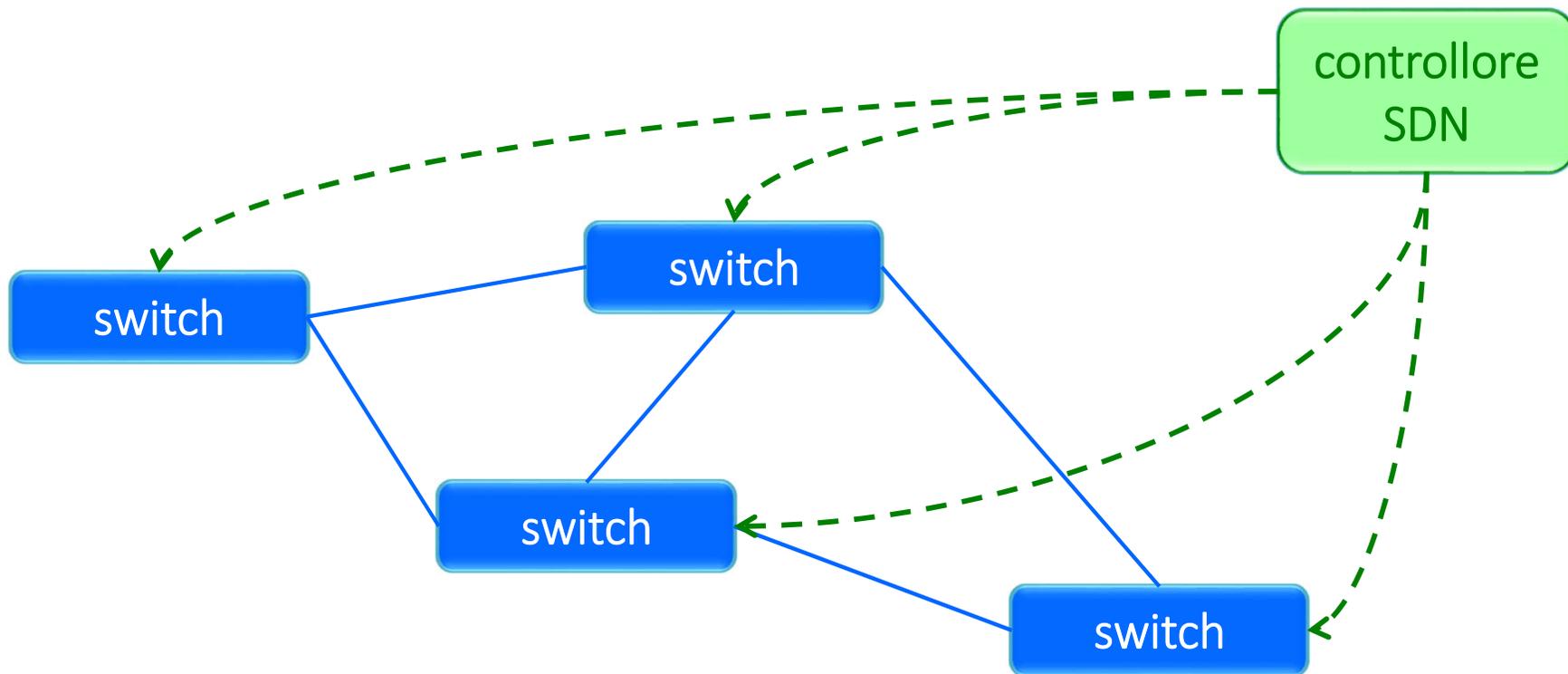


Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri



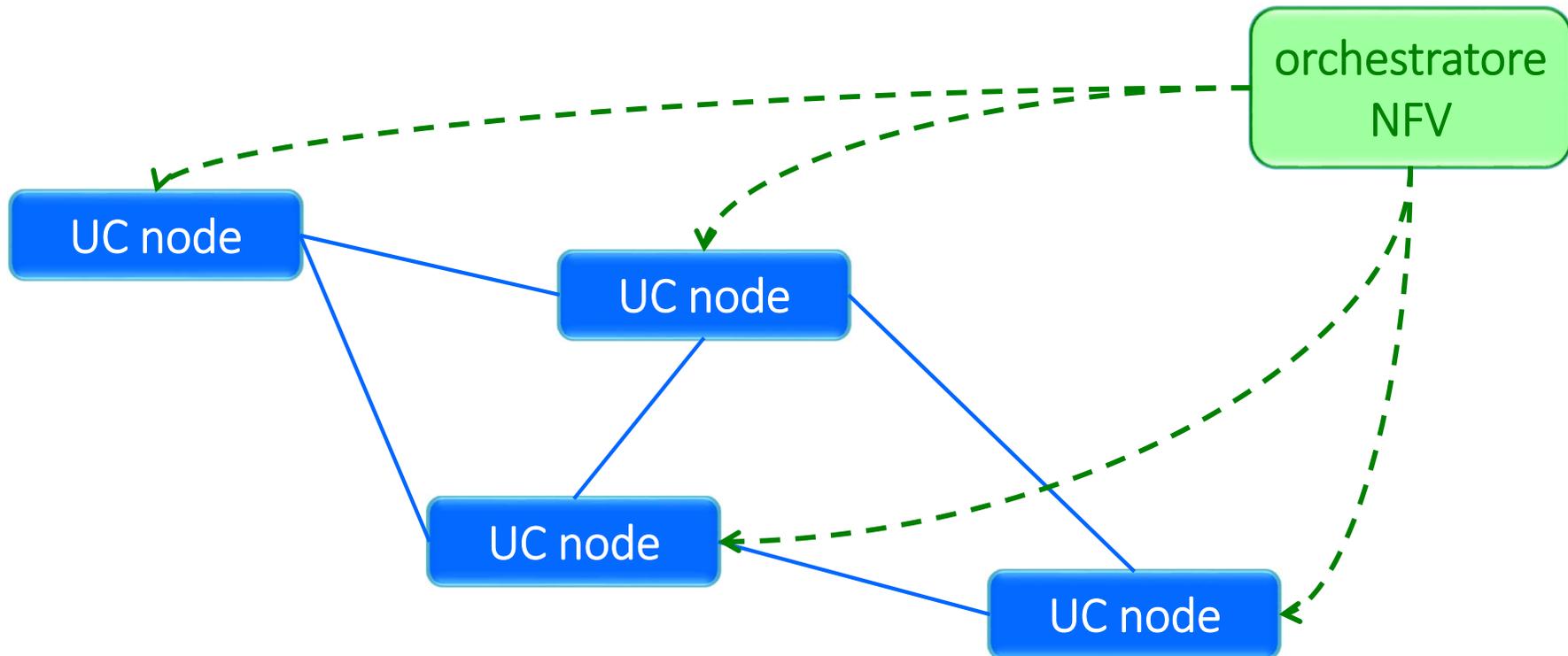
SDN e NFV – innovazione nelle reti

- SDN = Software-Defined Networking
 - separazione tra data-plane e control-plane
 - percorsi di rete definiti da un controllore di rete (molto) intelligente

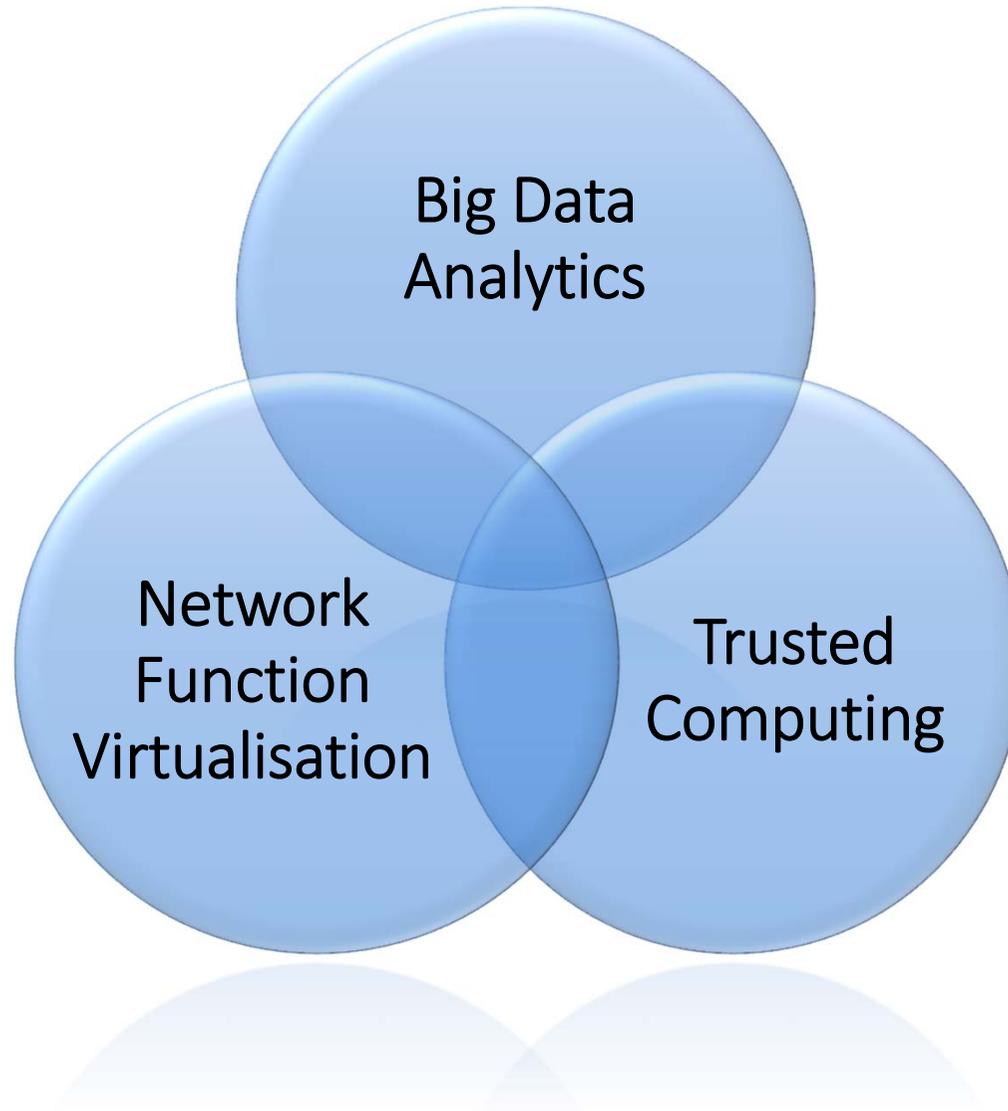


SDN e NFV – innovazione nelle reti

- NFV = Network Function Virtualization
 - non più nodi di rete "dedicati" (es. switch, router, firewall, IDS)
 - nodi Universal Computing (UC) = RAM, CPU, NIC, disco (poco)
 - funzioni configurate (e riconfigurate) come necessario

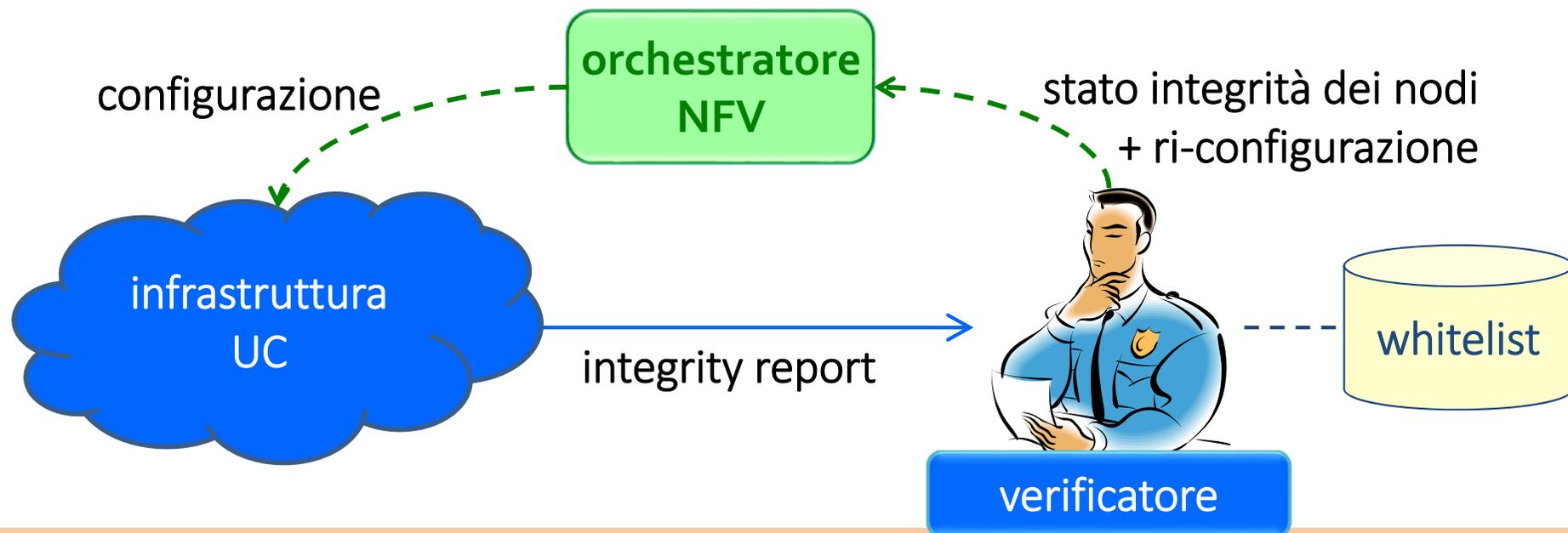


I concetti base di SHIELD



Trusted computing – dal cloud alle reti SDN/NFV

- piattaforma hardware basata su TPM (Trusted Platform Module)
- processo recursivo "misura-e-poi-esegue"
- misurazione di:
 - tutto il software eseguito (BIOS, boot, SO, applicazioni)
 - tutte le configurazioni (es. routing, filtraggio)



Machine learning + big data analytics per cybersecurity

- molti strumenti ma poco o niente open-source
- DARE = Data Analysis and Remediation Engine
 - informazioni dall'infrastruttura SDN/NFV
 - elaborazione con strumenti open-source
 - console di monitoraggio
 - reazione tramite configurazioni "astratte"
 - indipendenza dall'orchestratore
 - indipendenza da specifiche Network Security Function (NSF)



SHIELD in sintesi

- infrastruttura sicura, fidata e flessibile (SDN, NFV, Trusted Computing)
- machine learning e big data analytics per monitoraggio e reazione
- tre casi applicativi base:
 - un ISP **per proteggere la propria infrastruttura** (riducendo costi e complessità di gestione)
 - un ISP **per offrire SECaaS (Security-as-a-Service)** ai propri clienti
 - un'agenzia governativa (nazionale o internazionale) o un gruppo di interesse **per monitoraggio delle reti**



SHIELD - milestone

- framework rilasciato come open-source
- alcuni elementi proprietari (es. analytics engine)

SHIELD alpha version
(componenti base)
Settembre 2017

SHIELD beta version
(integrazione base)
Settembre 2018

SHIELD release finale
(post-validazione)
Febbraio 2019



SHIELD - dati essenziali

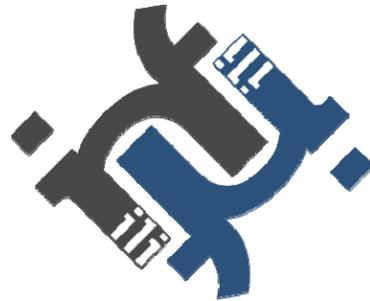
- progetto H2020, programma "Secure Societies"
- 11 partner
- durata Set'16 – Feb'19
- budget 4.56 M Euro



SHIELD – partner del consorzio



**Hewlett Packard
Enterprise**



Agencia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

ubiwhere



Il progetto SHIELD

SHIELD – contatti



<https://www.shield-h2020.eu/>



@shield_h2020



SHIELD EU Project



info@shield-h2020.eu



SHIELD has received financial support from the European Commission under Grant Agreement No. 700199



Il progetto SHIELD