Industrial Ethernet Security with HP's Adaptive Network Architecture

Holger Rank
HP Services
ANA EMEA Sales
holger.rank@hp.com

Agenda

- Security Risks for Industrial Ethernet (IE)
- IE + IT Security Strategy
- Security Policies, Processes and Roles
- ANA IE + IT Security Solution
- Summary

Security Risks for Industrial Ethernet

invent

Traditional IT Risks

- Complex IT infrastructures
- Lack in IT documentations incl.:
  - no policies and processes in place
  - no roles/responsibilities defined
  - no escalation and incident management
- IT Infrastructure
  - Viruses
  - Denial of Service Attacks
  - Hacker/Unhappy users etc.
- Controlling
  - no identity handling and management
  - no logging etc.

Industrial Ethernet (IE) Production Plant Risks

- Complex production lines incl. different IE networks, machines, etc.
- Typical not in place:
  - Data security classification
  - Policies, Processes and Roles
  - Escalation and Incident Management
- If one machines stops working, the impact can be for the complete production
- A production stop can damage raw materials, produced goods and the financial impact is high
- IE problems can affect the complete production plants

Industrial Ethernet (IE) Risks

- Soft & hard real time operation requires special protocols
- Connection to the traditional IT
  - No protection against traditional IT / vice versa IE max. FW
  - Specific nonstandard IT Ethernet Protocols like: ProfiNet, Ethernet IP, Ethercat etc.
  - No content screening and user authentication
- Production Machine
  - High productivity pressure – prevents security
  - No virus/content protection possibly for the Programmic Logic Controllers (PLC) or SPS
  - Machine vendor field service – direct access without control
  - No identity management for machine access (employee/repair service)

IE + IT Security Strategy

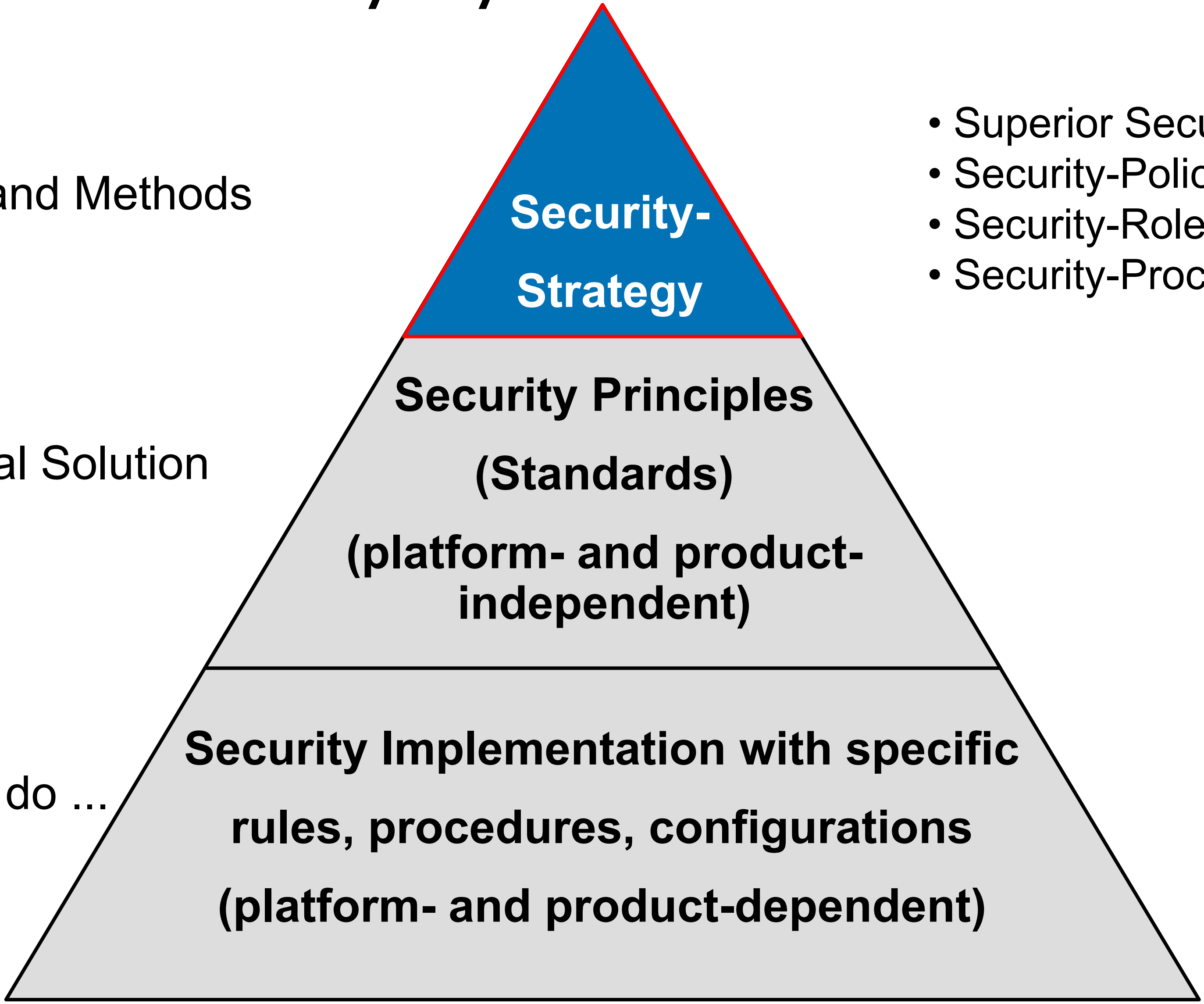
invent

IE & IT Security Pyramid

Goals and Methods

Principal Solution

How to do ...



Security-Strategy

Security Principles

(Standards)

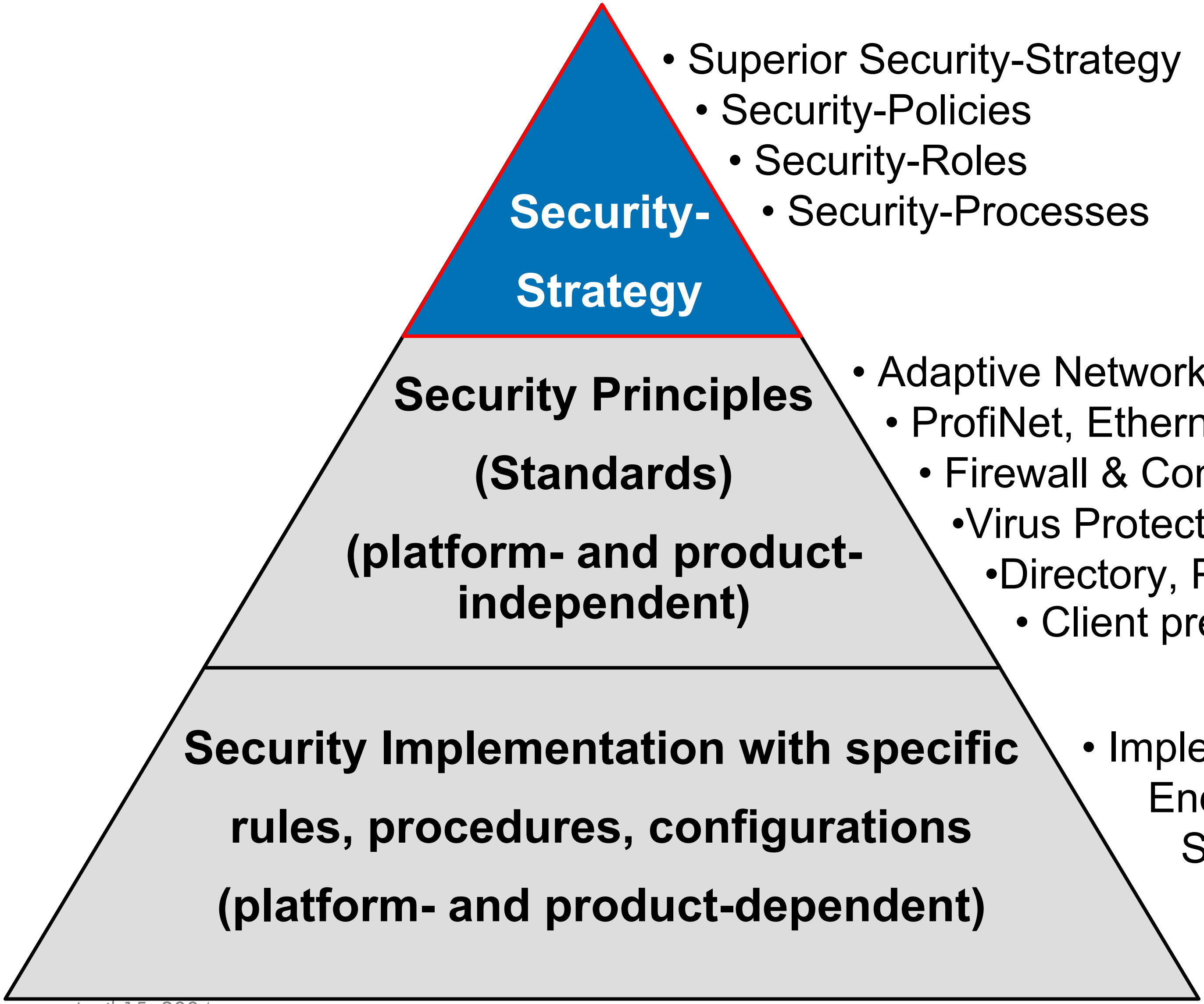
(platform- and product-independent)

Security Implementation with specific rules, procedures, configurations

(platform- and product-dependent)

- Superior Security-Strategy
- Security-Policies
- Security-Roles
- Security-Processes

IE & IT Security Solution Overview



Security-Strategy

Security Principles (Standards) (platform- and product-independent)

Security Implementation with specific rules, procedures, configurations (platform- and product-dependent)

- Superior Security-Strategy
- Security-Policies
- Security-Roles
- Security-Processes

- Adaptive Network Architecture
- ProfiNet, Ethernet IP, Ethercat
- Firewall & ContentScanning Concept
- Virus Protection
- Directory, PKI & LDAP
- Client preScan

- Implementation of a End-to-End IE&IT Solution with ANA

IE & IT Security Strategy, Policies, Processes and Roles

invent

IE&IT Security Strategy

- Defines the security requirements
- Is defined and supported by the executive board for the entire enterprise
- Essential requirement for protection of informations, systems, applications, network and whole production plants and machines
- Gives the IE&IT Security Role owners the rights to protect the company

IE&IT Security Policies

Examples are:

- Password regulation (Passwords)
- Use of external repair service access
- Virus protection (Malicious software)
- Authentication and authorization (Authentication, Authorization)
- Data- and system classification (Classification & Entitlement)
- Use of external access to enterprise (External Network Access)

IE&IT Security Processes

Examples are:

- Security monitoring
- Incident handling and escalation
- Approval handling for repair service access to IE
- Investigation of recently known security risks and vulnerabilities
- Exception handling
- Implementation of security audit

IE&IT Security Roles

IE & IT Security Roles give a answer to:

- Who is responsible for the IT and IE security?
- Who can decide a disconnection of a IE from the IT?
- Who is responsible for the disconnect (technically) ?
- Who can resolve the security problem?
- It defines the objective of the IE&IT Security-Role
- The required knowledge and experience necessary for this IS-Role
- The task and activities, which are derived from the IS-Processes

Adaptive Network Architecture IE & IT Security Solution

Adaptive Network Architecture is

- a **solution**
- **structures** the complete IT infrastructure
- implements **security** and **business** needs
- manages **IT wide compartment's**
- provides a **geographic independence**
- presents the IT in a **virtualized view**
- a **secure** and **auditable** IT wide infrastructure

The components of ANA

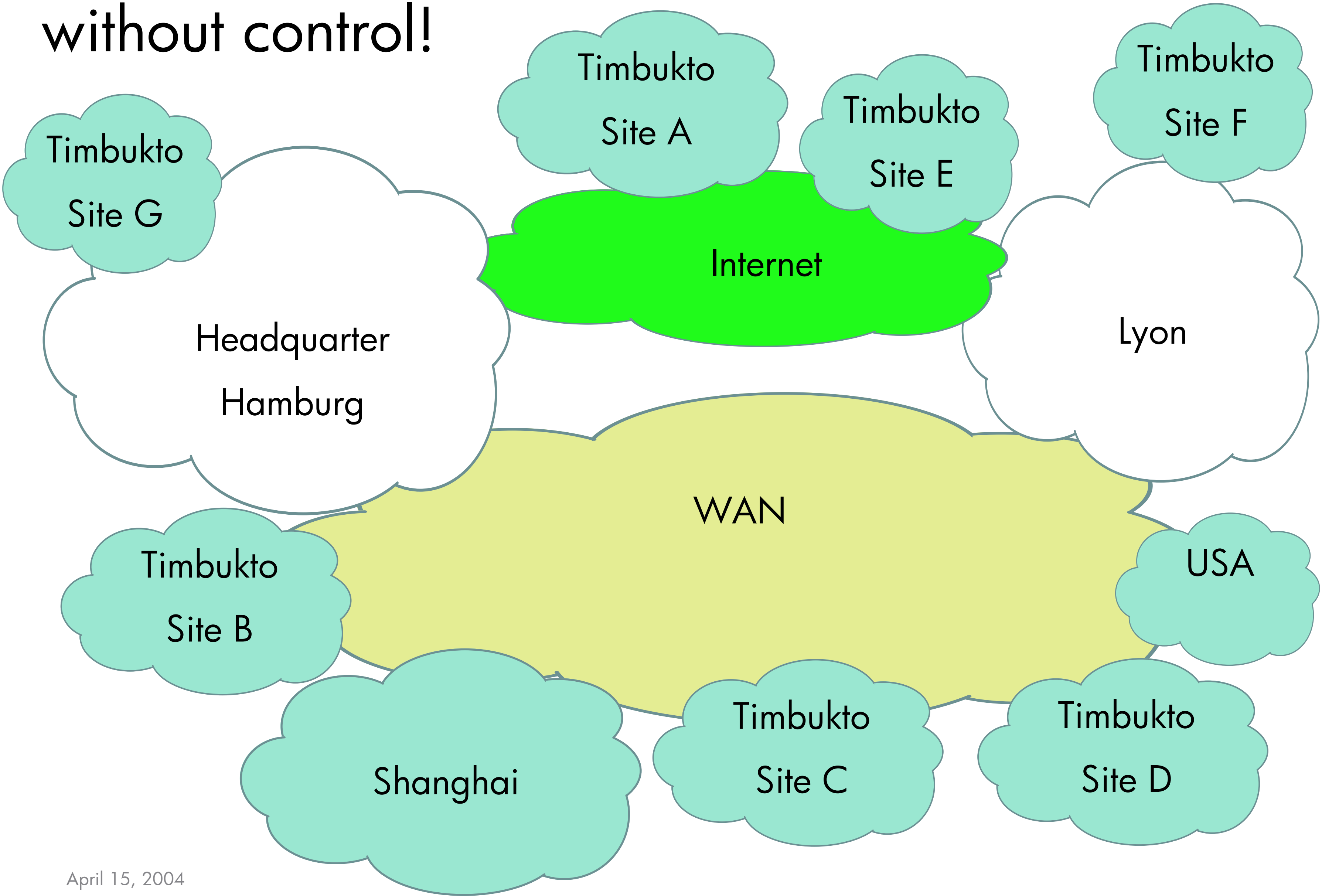
- ANA structures networks into ‘Compartments’
- ANA connects ‘Compartments’ using a ‘Virtual Backbone’
- ANA controls access thru ‘Policy Enforcement Points’
- ANA is using a central ‘Policy Management System’
- ANA leverages your existing IT-, LAN- and WAN-Infrastructure
- Additional Security Solutions like AE, IBNS, Virus protection, IDS, Content Scanning etc.

Practical ANA Security Example

What do we need for a secure IE & IT?

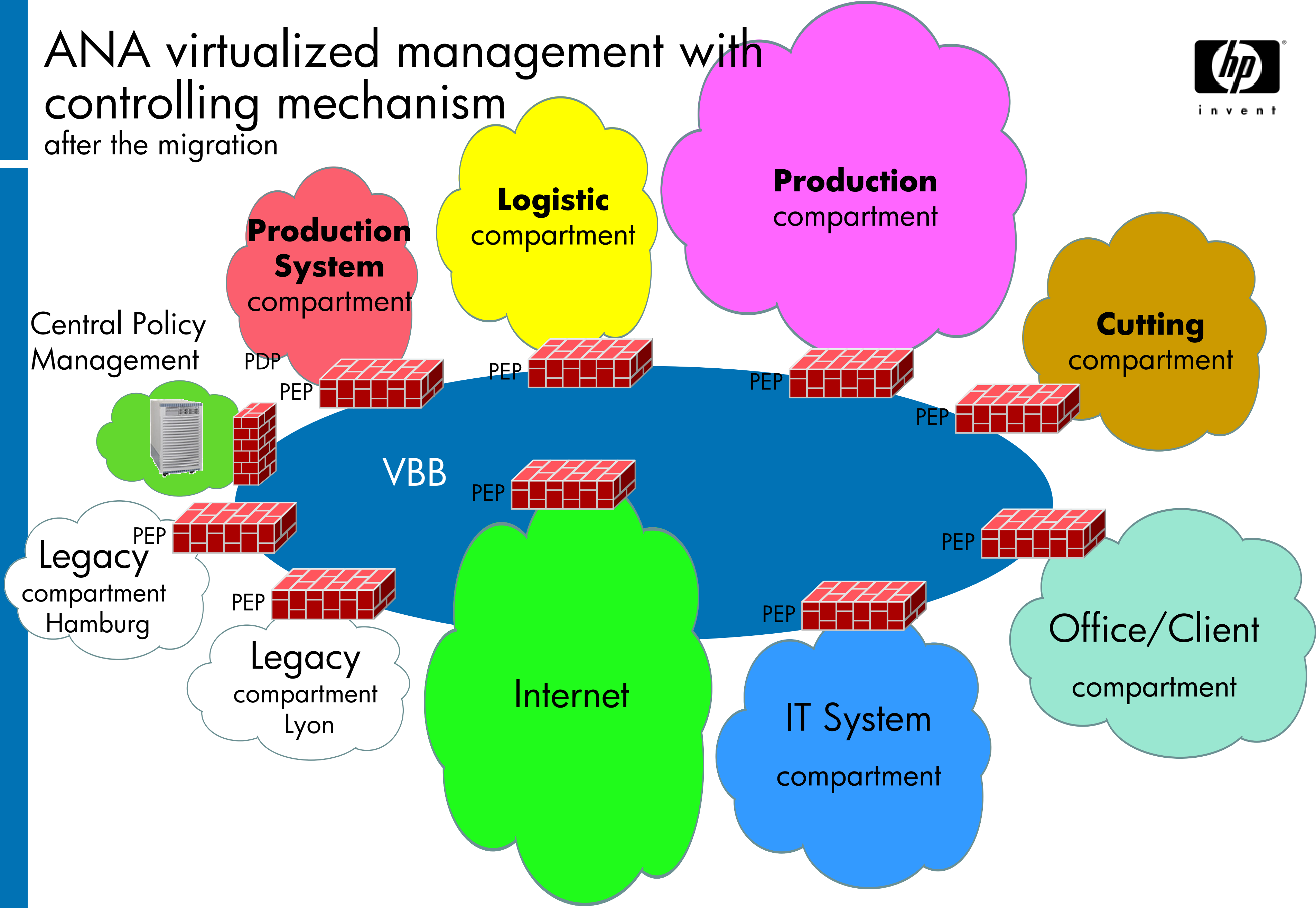
- Policies, Processes and Roles
- Security Data Classification
- Security/Business Compartments
- Security Solutions
  - PEP's (low & high level security)
  - IBNS, IDS etc.
  - Active Directory
  - Virus Protection
- A easy centralized management
- ROI <12 month & real cost savings

Today Network – before ANA without control!

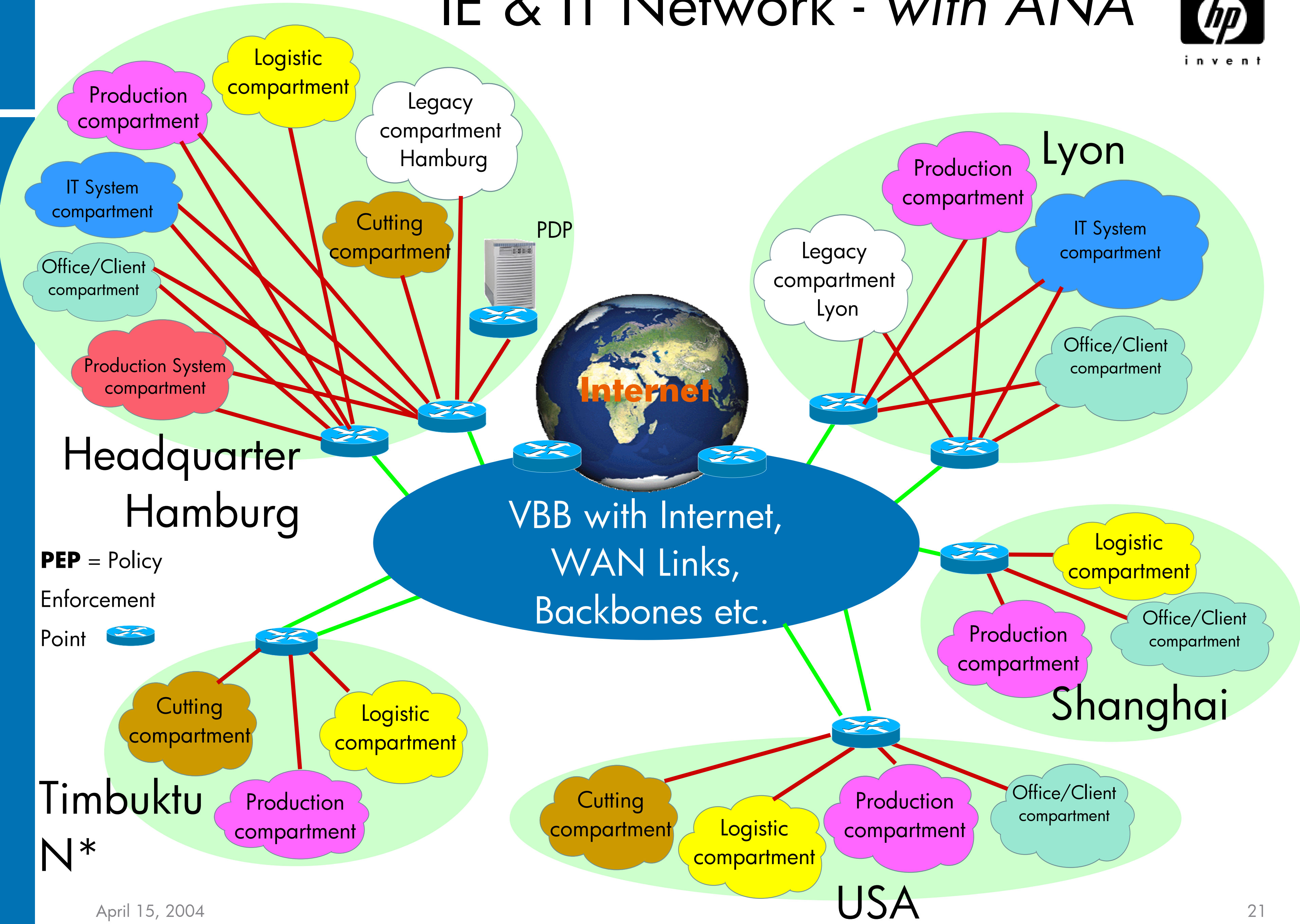


ANA virtualized management with controlling mechanism

after the migration



IE & IT Network - *with ANA*

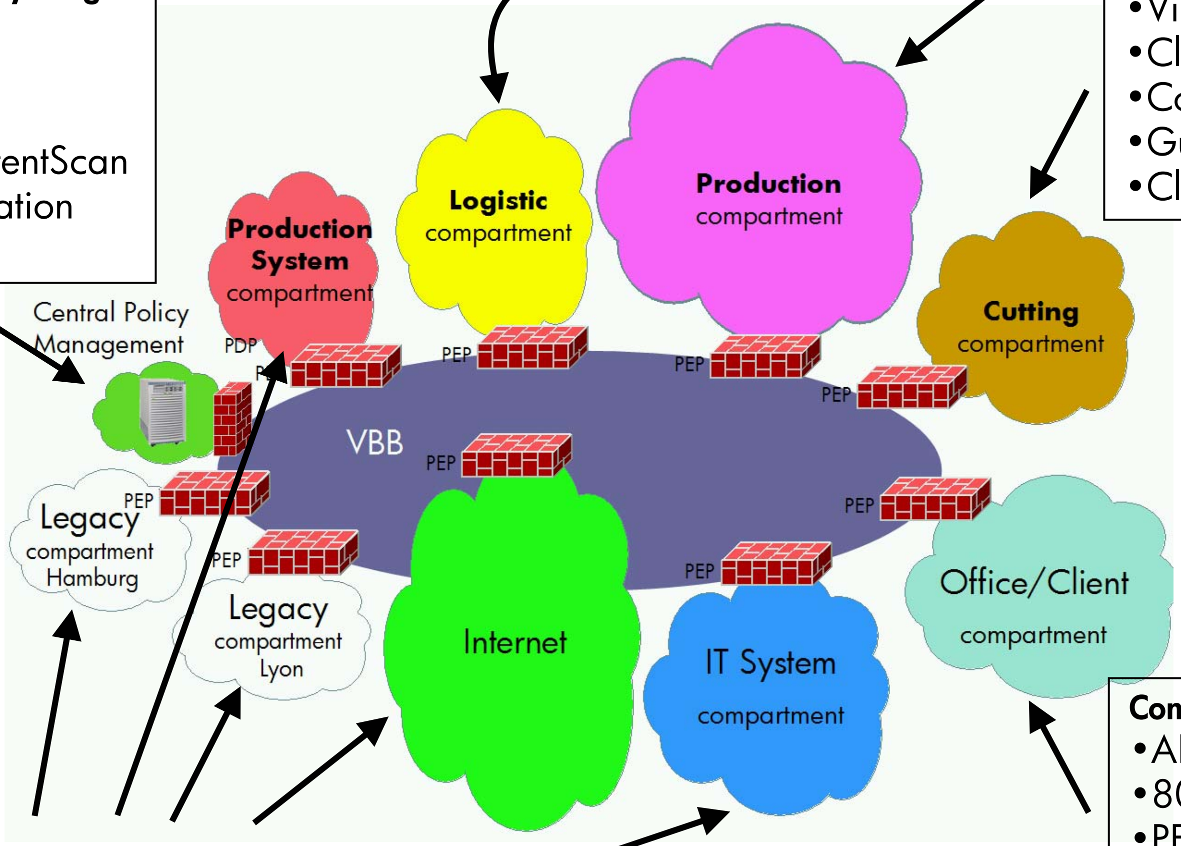


PEP = Policy Enforcement Point

Virtualized management view with ANA & Security Solution’s

after the migration

Compartment Security usage:
- ANA
- 802.1x / IBNS
- PEP’s (Firewall)
- IDS+Virus+ContentScan
- Directory integration
- Single Sign On



Compartment Security usage:
- ANA
- 802.1x / IBNS
- PEP’s Router/Switches/Firewall
- IDS
- Virus&Content Protection
- Client preScan
- Content Scanning
- Guest LAN
- Client Isolation

Compartment Security usage:
- ANA
- PEP’s Router/Switches/Firewall
- IDS
- Virus&Content Protection
- Directory integration

Compartment Security usage:
- ANA
- 802.1x / IBNS
- PEP’s Router/Switches/Firewall
- IDS
- Virus Protection
- Client preScan
- Directory integration
- Single Sign On
- Personal Firewall

Summary

Summary

IE & IT Security means:

- real cost saving and a ROI for security
- rational Policies, Processes and Roles
- secure thinking between IT and IE connections
- a structured IE & IT based on security and business needs
- a secure, standardized, modularized, simple to manage and easy to implement IT & IE infrastructure
- a real security End-to-End management
- a transparent and documented infrastructure
- a auditable secure infrastructure
- trust for working corporate infrastructure and production plants

invent