MASARYK UNIVERSITY

Surveillance and Monitoring Systems based on Complex Event Processing

Tomáš Pitner
Masaryk University, Czech Republic

BIS 2012, Vilnius, Lithuania, May 23rd

Surveillance and Monitoring Systems

- The monitoring system **continuously**
  - **collects** data from the monitored environment,
  - evaluates this data and **events** that are essential
  - takes the user's **attention** to important events,
  - or is able to respond **automatically**.

Surveillance and Monitoring Systems

- TARGET
  - Used to monitor the operation of various objects
- SCOPE
  - From a single application, computer, or other device
  - Upto large infrastructures
- USERS
  - They help routine operators as well as strategic management

Surveillance and Monitoring Systems

- PURPOSE
  - *Check functionality* - detect faults
  - *Monitor reliability* – discover, prevent outages
  - *Protect* - find external and internal threats
  - *Explore what could not be modelled* - unusual behavior
  - *Save by discovering frauds* - even when not obvious
  - *Optimize* - tune the operation
  - *Measure performance* – real-time KPIs

Surveillance and Monitoring Systems

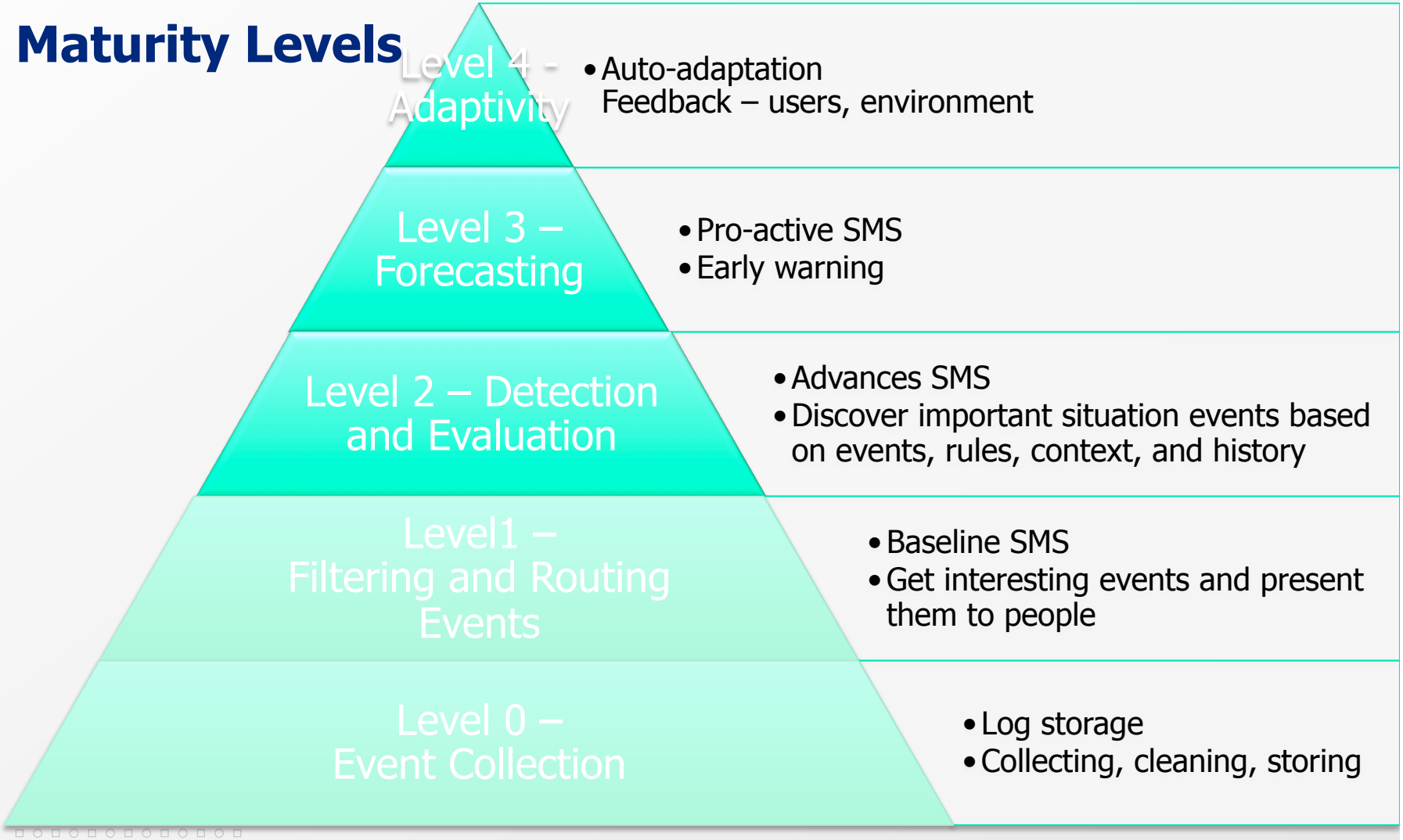
- BENEFITS
  - See the current situation **immediately**
  - **Aggregated** and **visualized** form
  - Measure **KPI** in real-time
  - Standard behavior **profiles** (devices, systems, people)

  - Ensure business **rules compliance**
  - Guarranty **SLAs**

Surveillance and Monitoring Systems

- IMPROVE THE SYSTEMS
  - Shorten the (incident, event) **detection time**
  - Reduce the time to **discover the cause**
  - Make the **intervention** more effective
  - **Reduce staff costs**, require less qualified personnel

Maturity Levels

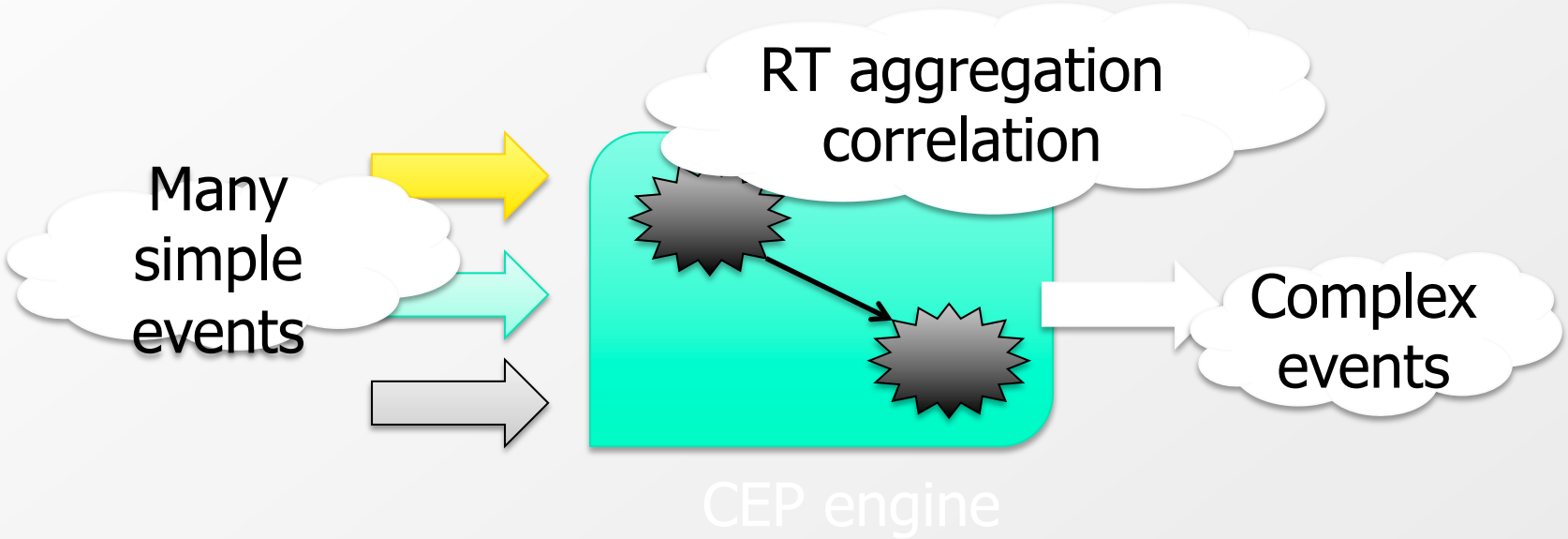


Technology Requirements

- Various domains and data origin
  - Measurements
  - Logs
  - Lower-level systems
- Large data volumes in realtime
  - 10k+ events per sec
- Context, correlation, adaptation

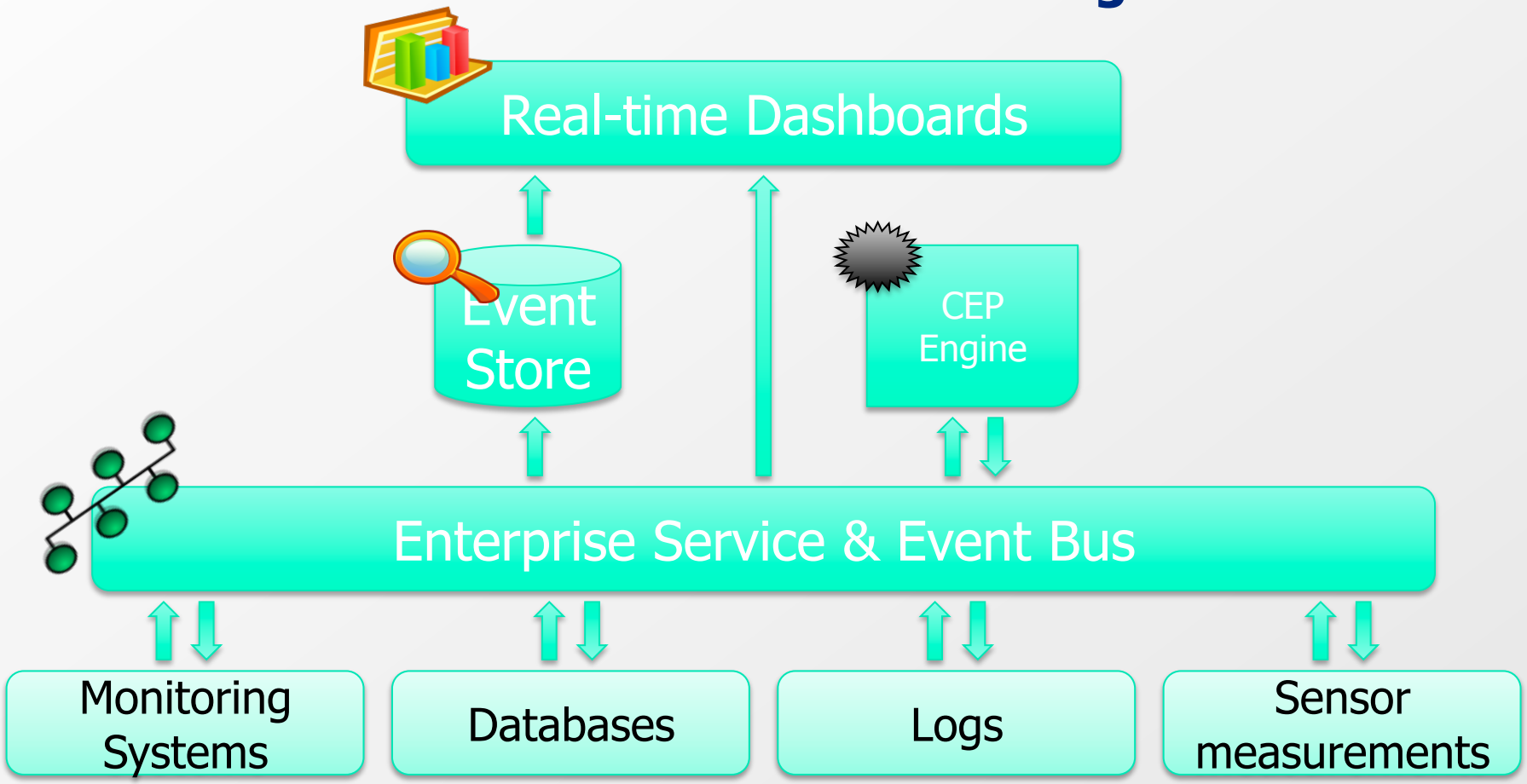
- **How to achieve it ?**

Complex Event Processing Technology



- Real-time (or near RT) fast data flows
- Behaviour pattern detection
- Fraud detection, smart-grids, logistics, telco

CEP-based Surveillance and Monitoring Center



Further Outline of the Talk

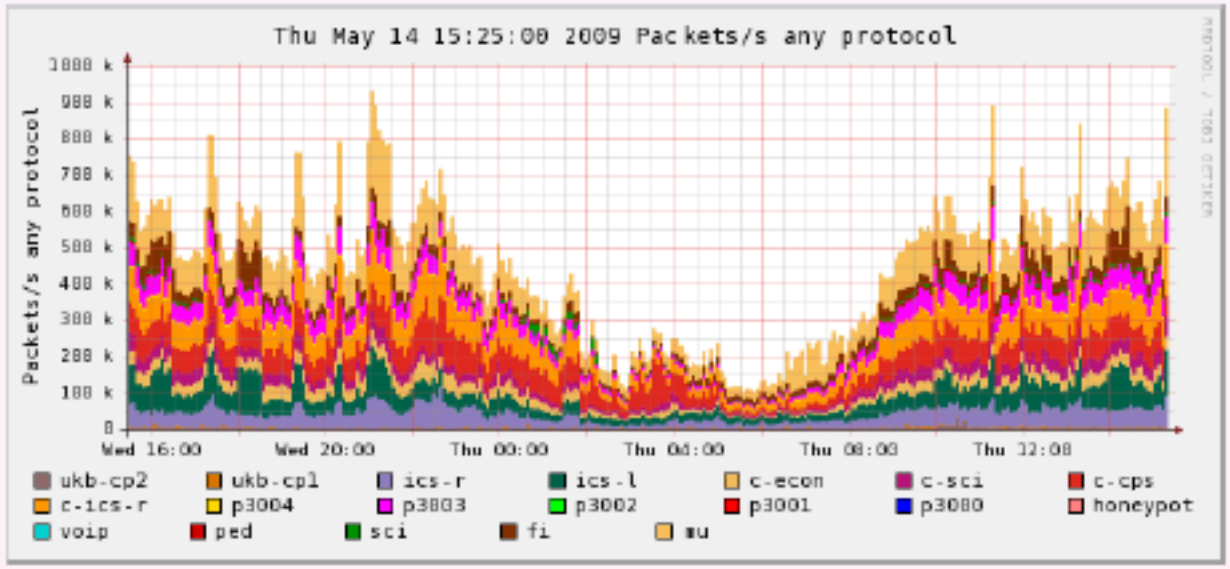
- Domains
- Technology
- Applications
- Partners

Application Domains

- Computer network security
- Facility management
- Fraud detection in large enterprises / sales networks
- Computing resources, Clouds
- Complex technological blocks
- Industrial production
- Smart grids, power networks
- Precise agriculture

Computer network security

- Based on Netflow monitoring
- Complement to host-based approach
- Instead of restrictive policies
- The only way in open, research institutions

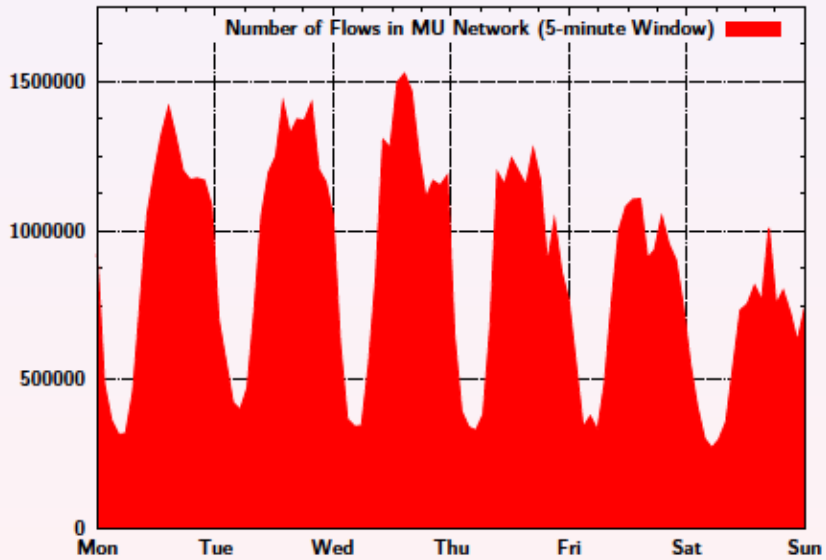


Case of Masaryk University

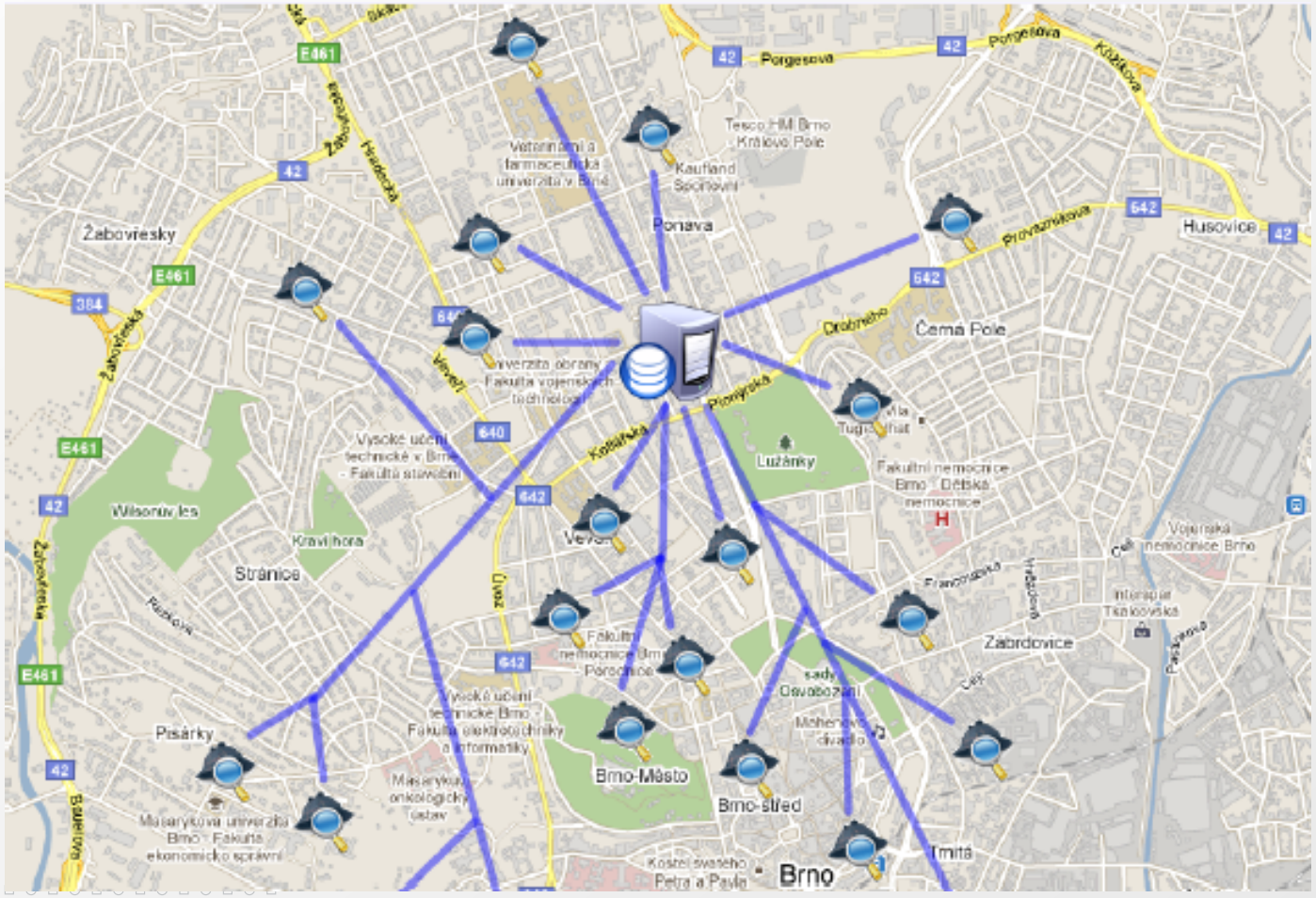
- 9 faculties: 200 departments and institutes
- 48,000 students and employees
- **15,000 networked hosts**
- 2x 10 gigabit uplinks to CESNET (NREN)

Interval	Flows	Packets	Bytes
Second	5 k	150 k	132 M
Minute	300 k	9 M	8 G
Hour	15 M	522 M	448 G
Day	285 M	9.4 G	8 T
Week	1.6 G	57 G	50 T

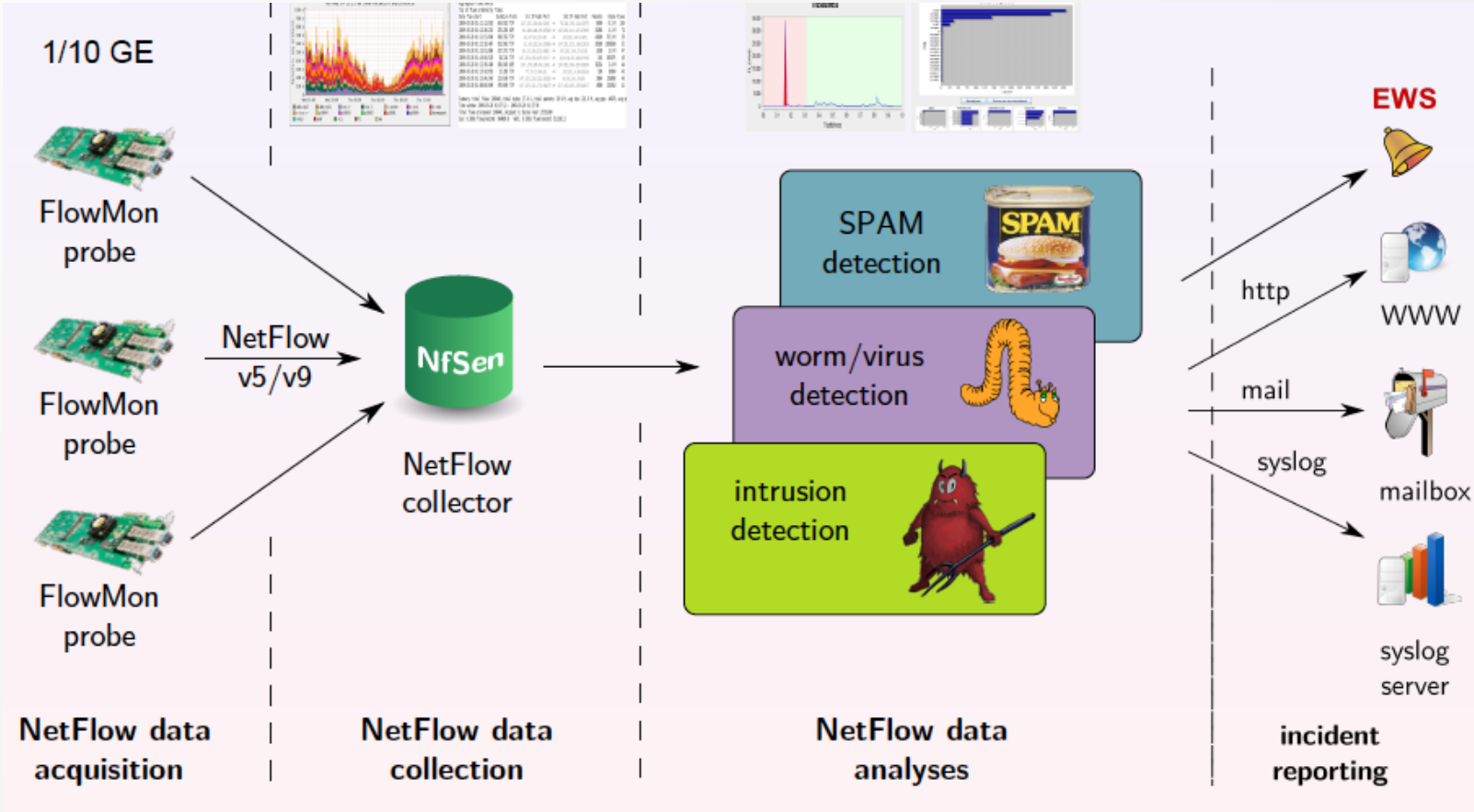
Average traffic volume at the edge links in peak hours.



Hierarchical nature



CEP-based Analysis and Other Processing



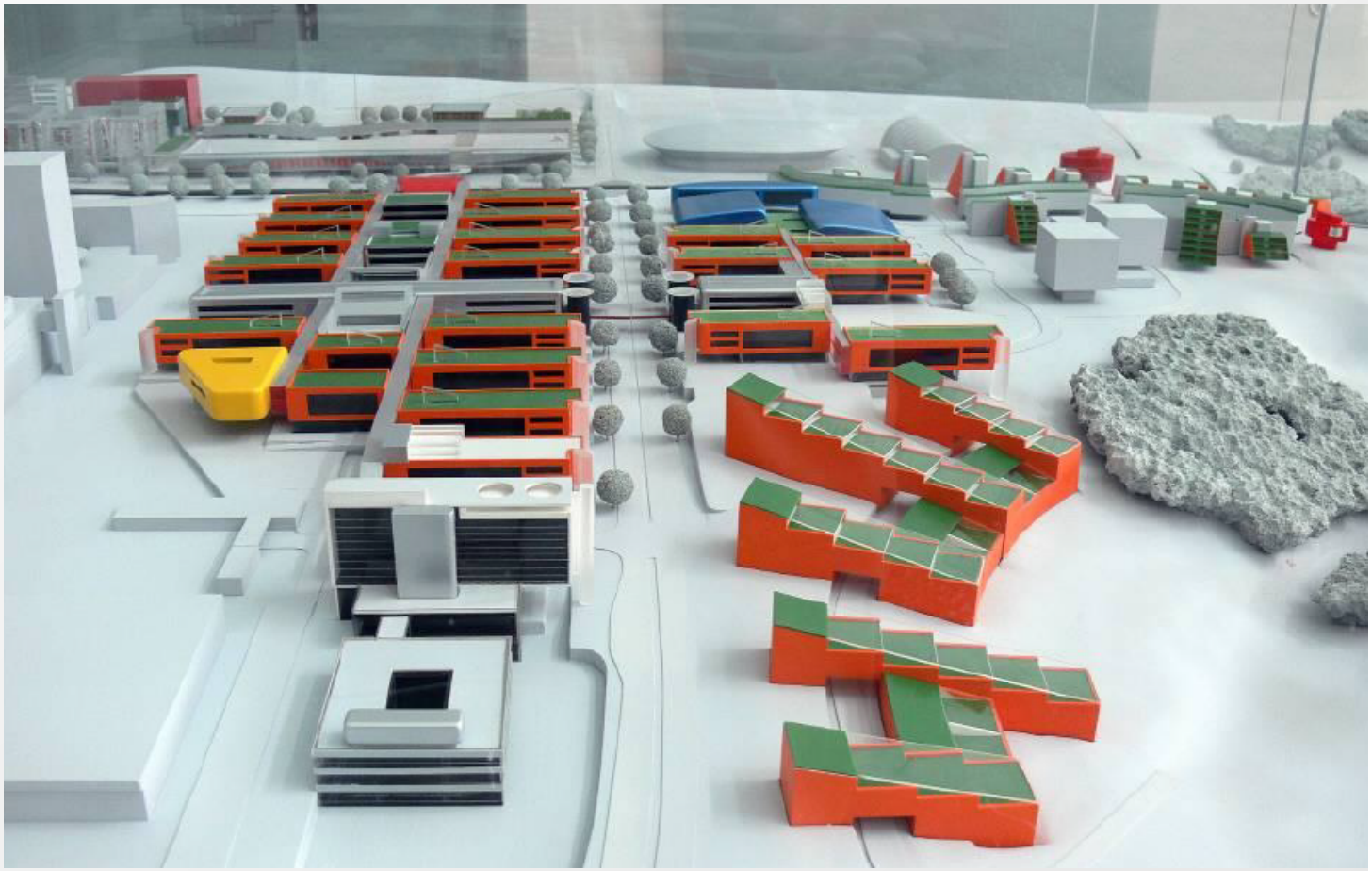
Facility management

Facility management

- WHY SO INTERESTING (in general and for us)?

- Masaryk University
  - 9 Faculties, 40000+ students, 4500+ staff members
  - 250+ buildings (150 own), 20500+ rooms
  - 350000+ m^2
  - Campus of Masaryk University, the largest in CZ
  - Technological equipment in newer buildings

Facility management @Campus of Masaryk Uni



Facility management / What is observed?

- 30+ buildings at Campus, 100000 m^2
- Heating, cooling, air conditioning, moisturizing
- Security: fire detectors, access control, cameras
- Other: audiovisual equipment, lighting, power supply, waste management

- **Building monitoring system**
- 100k records / day
- Alerts, Visualization

Fraud detection

- Applied for fuel-fraud detection at a gas-station network
- Many events from various domains
  - Accounting/billing
  - Fuel level in tanks
  - Volumes sold
  - Volumes supplied
- Saves dozens of M CZK annually for a moderate-size chain

Computing resources, Clouds

- All old-hat problems (grids) and many new ones
- Multi-tenancy
  - IaaS (machine provider)
  - PaaS (platform provider)
  - SaaS (app provider)

- Make it simple, easy to integrate
- Secure (the players should be isolated)
- Keep overhead low

Industrial Production

- Monitoring enhancement for production information system PHARIS

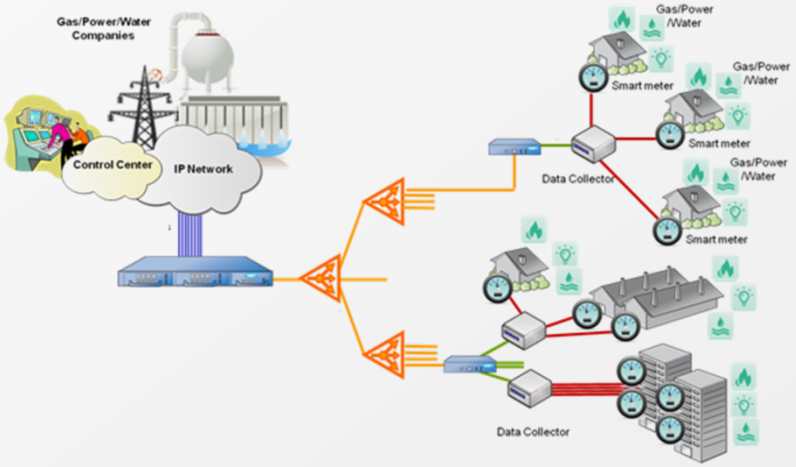
Industrial Production – What is monitored?

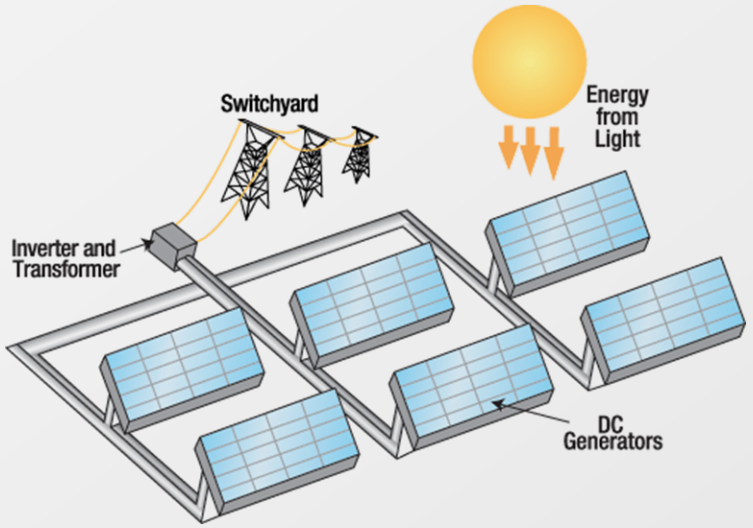
- Machines
  - Number active/working, cycles done
  - Operators, logins
  - Operations performed on machines
  - Reactions to events

  - Derive the machine cycle profiles
  - Detect faults, anomalities

Energy Production and Distribution, Smart-Grids

- Monitoring large smart-meter networks
- Monitoring and controlling alternative energy sources





Example in Smart-Grids

- Large smart-meter infrastructure
  - milions of smart-meters in CZ
- What we know?
  - Status (consumption) every 15 min
  - Outages, failures at SM or communication
  - Switch-off
  - Unauthorized manipulation

Example in Smart-Grids: The Size

- Magnitude of up to 10 M smart-meters
- 10 TB of raw data
- 15 mins time frames important for some processing
- Legacy analytical apps

- New apps not just for smart-grids but also for smaller infrastructures/suppliers

Rounding up...

Achieving higher SMS levels:

Level 0 – collecting data
Level 1 – basic patterns
… all for most legacy SMS … **but we need**:

Level 2 – advanced
Level 3 – predictive
Level 4 – adaptive

Rounding up...

- CEP-based monitoring
  - Large-size, large data volume apps
  - CEP allows down-sizing, supports hierarchical structure
  - Recursive processing (low- and high-levels together)
  - Multi-domain nature
  - Context-aware monitoring
  - Identification of common patterns

MASARYK UNIVERSITY

Thank you for your attention!

Questions? At any time to

tomp@fi.muni.cz

Tomáš Pitner
Masaryk University, Czech Republic