IFIP WG10.4

Evidence-based Computing
for Dependability
(Demo)

konoha

Kimio Kuramitsu

Yokohama National University

Today's Talks

- **First prototype of our open system framework**
  - Target: Embedded Linux
  - Demo in Embedded Technology 2009
  - Scenario: networked video surveillance system
    - Today's demo are ported on VMWare

- **Experience**
  - toward "open systems"
  - Future direction

Classic View: Dependable OS

- **Dependable OS never crashes**
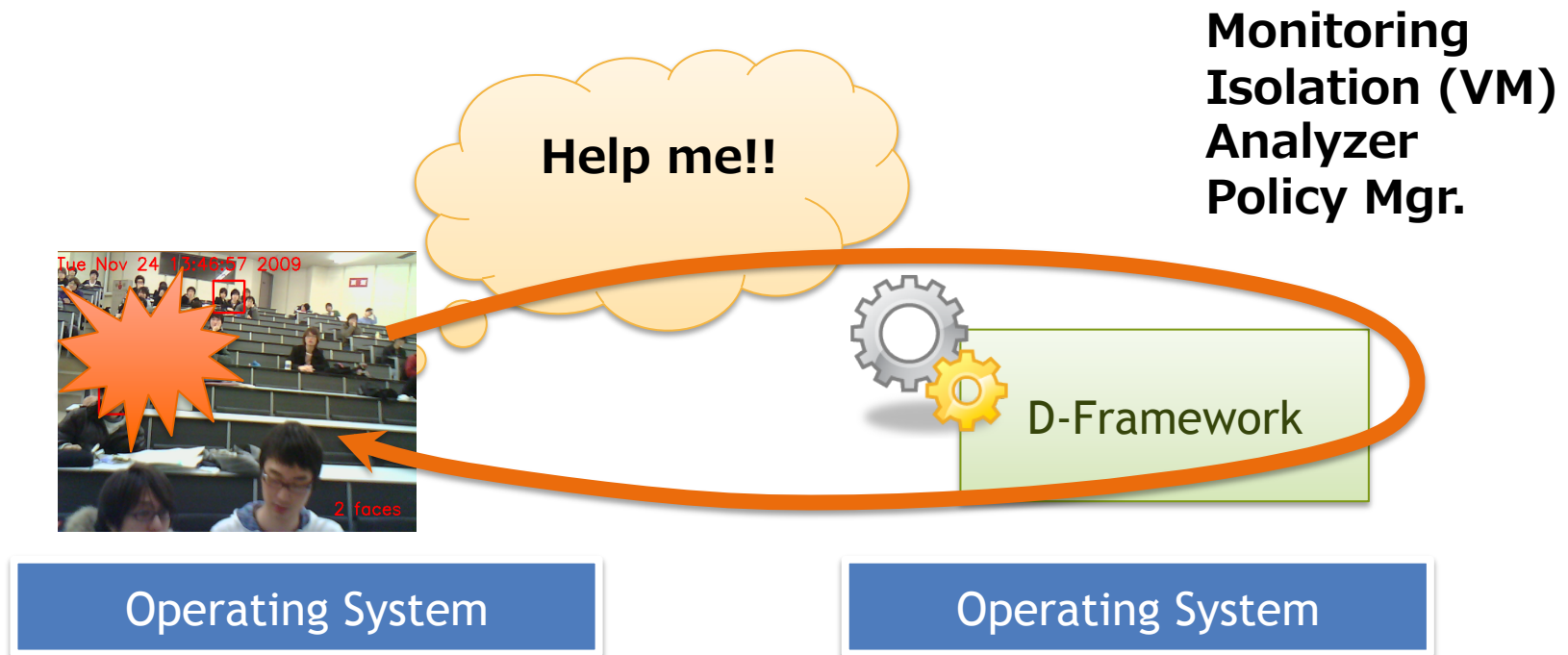- **Applications must handle with external errors (such as I/O errors) by itself**
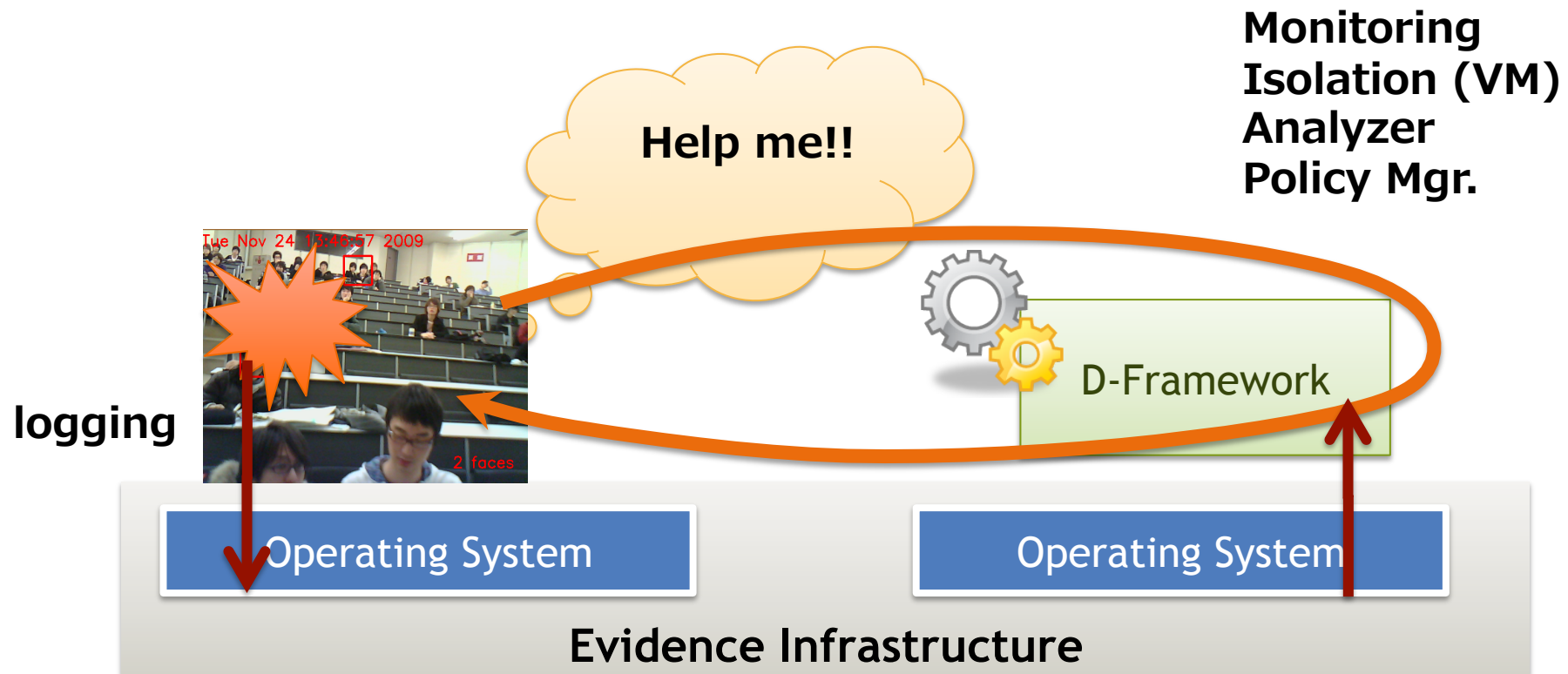
Operating System

Do it yourself

Our View: D-Framework

- **Dependable OS must be dependable**

Help me!!

Monitoring
Isolation (VM)
Analyzer
Policy Mgr.

D-Framework

Operating System

Operating System

Why We Focus on Evidence?

- **Evidence:**
  - digital records of facts: source code, logs
  - "correct" enough to take logical actions

- **Evidences are a key to:**
  - account facts
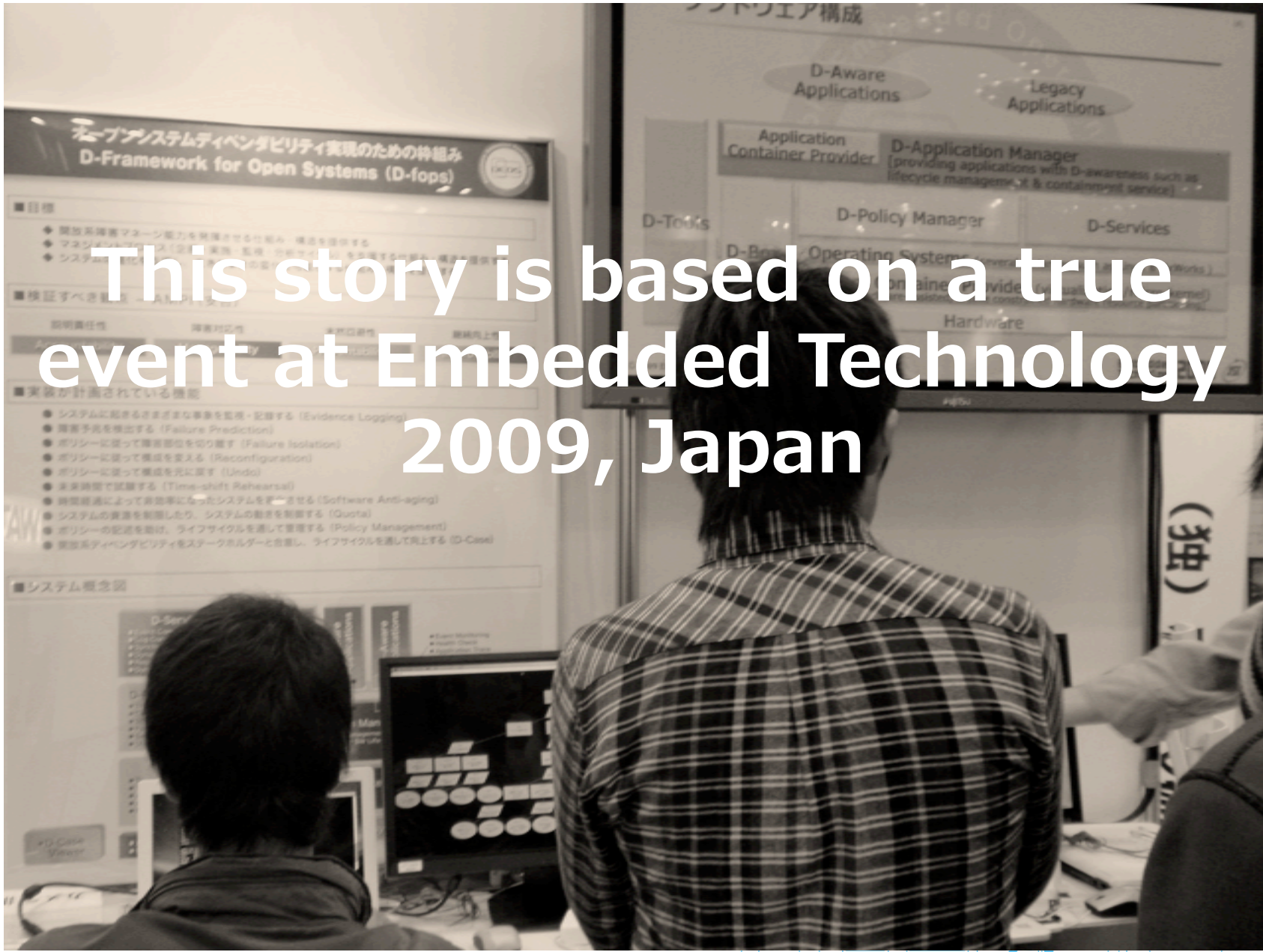 - reestablish agreements
  - correct situations

Today' Demo

developed with

Masahiro Kato, Youtaro Hiraoka, Masaki Goshima
Ken Igarashi, Masahiro Ide, Shinpei Nakata and Me

Goal Structuring Notation,
View of monitored evidences

Monitoring
Injection (Work Up)

Help!!

Framework

Operating System

Operating System

Evidence Infrastructure
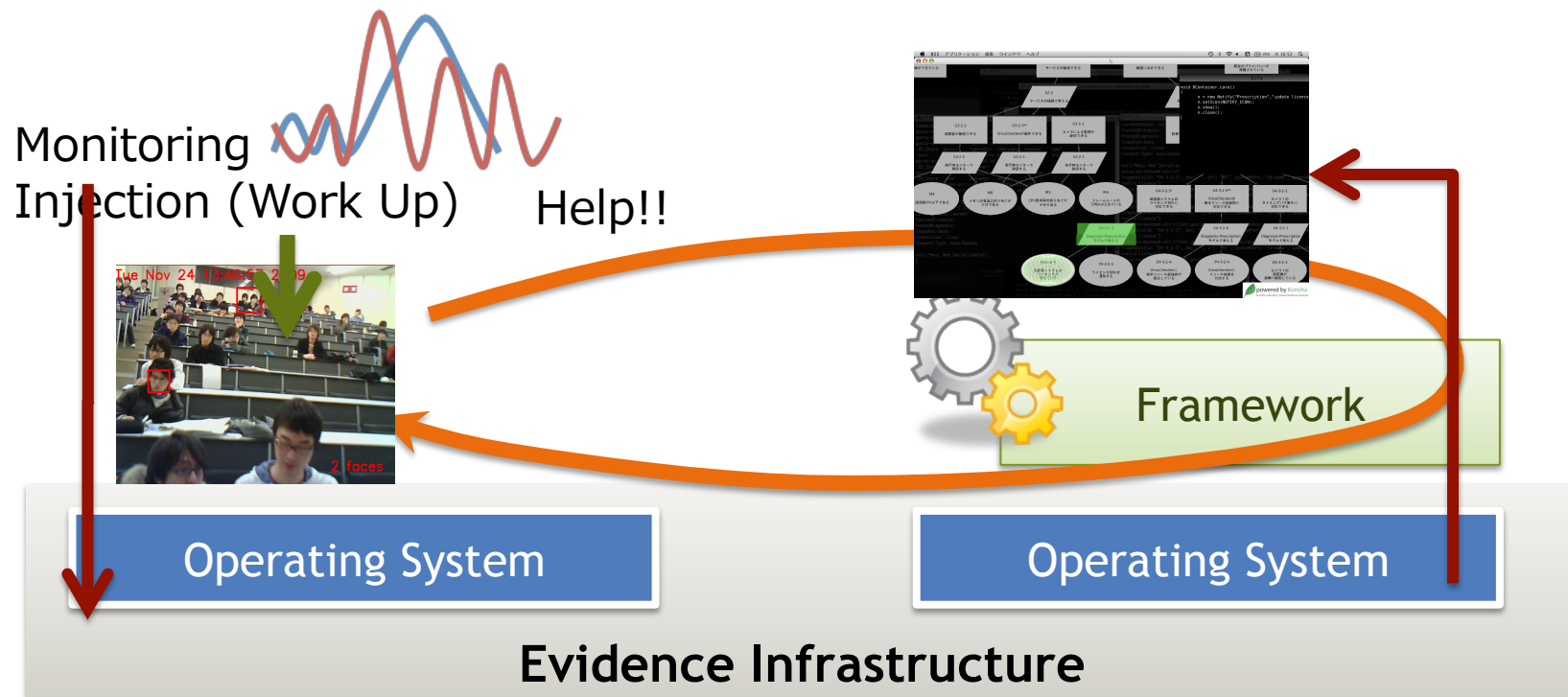
This story is based on a true event at Embedded Technology 2009, Japan

ET2009 Day 1

Yutaka Matsuno, 10:01 am
　いまこんな感じです

Yasuhiko Yokote, 10:03 am
　さすがに１０：０１だとお客さんはいない？？？

 Yutaka Matsuno, 10:01 am
　一人きました
　デモが動いてないです

Yosuhiko Yokote, 11:44am
　ぴーんち！昨日は動いていたのに・・・

Yutaka Matsuno, 11:45 am
　横国の学生さんがいま会場にいっているそうです

ET2009 Day 2

Me,

何だったの？

My Student N

Web Server の起動がうまくい
かなくて通信ができなかったよう
です

Me,

それだけであの大騒ぎなの？

My Student N

DEOSって何がしたいんだったの
でしょうか？

It was a typically student bug

- **My student forgot exception handling. He didn't know what if the server is down.**

```
try {
    in = new InputStream($dcase.server);
    ....

}
catch(IOExeption e) {

}
```
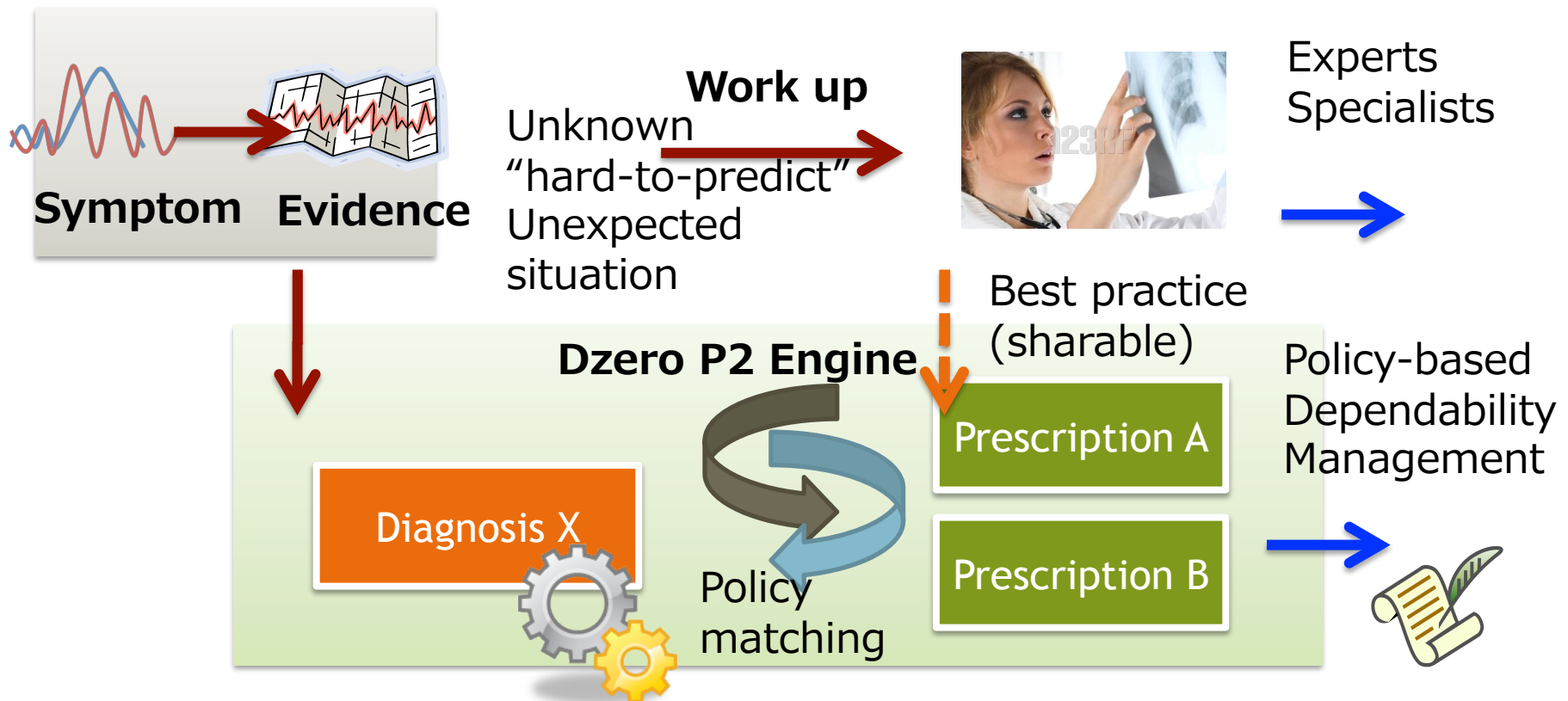
- **No blame on him**
  - "Less experience" could be a good analogy to "unexpected faults" in open systems

Towards Open Systems

- **Failures will happen**
  - Everything is not predictable
  - Vulnerable to unexpected happenings.

- **Accountability is important**
  - Everybody feels anxious, insecure and angry

- **Human experts are needed to recover**

"Open Systems" Management

- **Seamless integration of**
  - Expert intervention for unexpected faults
  - Automated management for expected faults

Symptom **Evidence**

Work up

Unknown "hard-to-predict" Unexpected situation

Experts Specialists

Best practice (sharable)

Dzero P2 Engine

Policy-based Dependability Management

Diagnosis X

Prescription A

Policy matching

Prescription B

Research Directions

- **Evidence technology**
  - collection mechanism and storage
  - standardization

- **Models for evidence**
  - dependability cases
  - policy and fault analysis

- **Language**
  - Describe dependability practices to share and automate

Future Direction

- **All of tools have been implemented in Konoha, our <u>dependable scripting language</u>.**
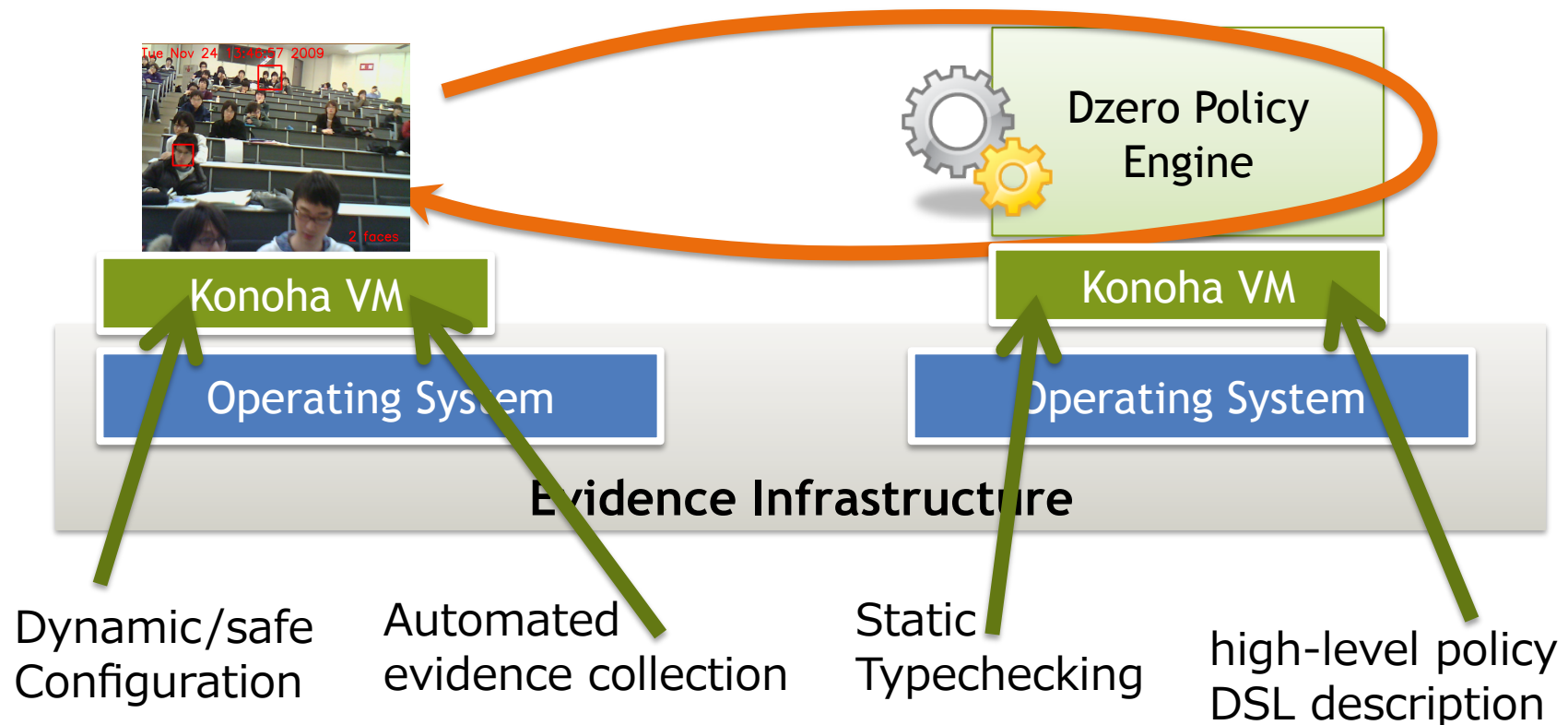
Question?

Kimio Kuramitsu
Yokohama National University
kimio@ynu.ac.jp