# A study of network vulnerability in embedded devices

T. Sugimoto, M. Ishii, T. Masuda, T. Ohata, T. Sakamoto, and R. Tanaka
Japan Synchrotron Radiation Research Institute (JASRI/SPring-8)

2nd Control System Cyber-security Workshop,
October 11th, 2009, Kobe International Conference Center, Japan

# Overview

- Introduction
- Problems at SPring-8 control system
- Investigation of vulnerabilities in embedded devices
  - One example: motor control unit
- Improvement of reliability
  - Implementation of embedded devices
  - Refinement of network
- Summary

# What is embedded system?

- Instruments with microcomputer for dedicated applications
- Implementations of embedded devices are black-boxed; details are not known by us, especially commercially available devices.
- Network (Ethernet) is used as a field bus of embedded devices.

Network-connected embedded devices are very useful, but there are problems.

# Problems of embedded devices

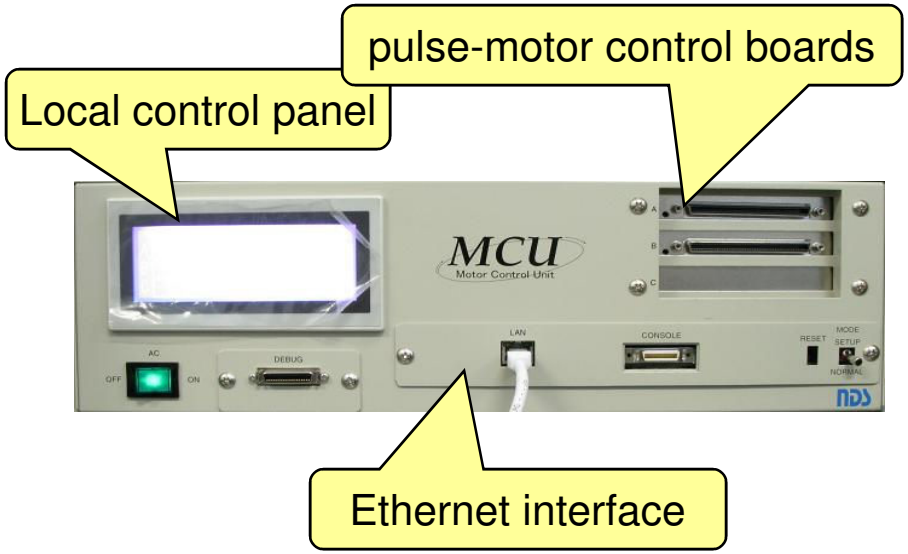
- Many problems of embedded devices had been occurred in SPring-8 control system.
  - Device errors of digital multimeters
  - Session lost of oscilloscopes and multi-channel analyzers
  - Hang-up of moter-control units
- Accelerator operation failures (such as interruption of injection) are caused by these problems.
- Commercially available embedded devices are also used in other facilities;
  - Not only SPring-8, but any facilities may be suffer from these problems.

# Aim of present study

- Improve reliability of network-connected embedded devices
  - investigate vulnerabilities in embedded devices
    - motor-control unit (MCU) was concentrated studied.
  - perform improvement
    - implementation of embedded devices
    - refinement of network system

# Motor-control unit (MCU)

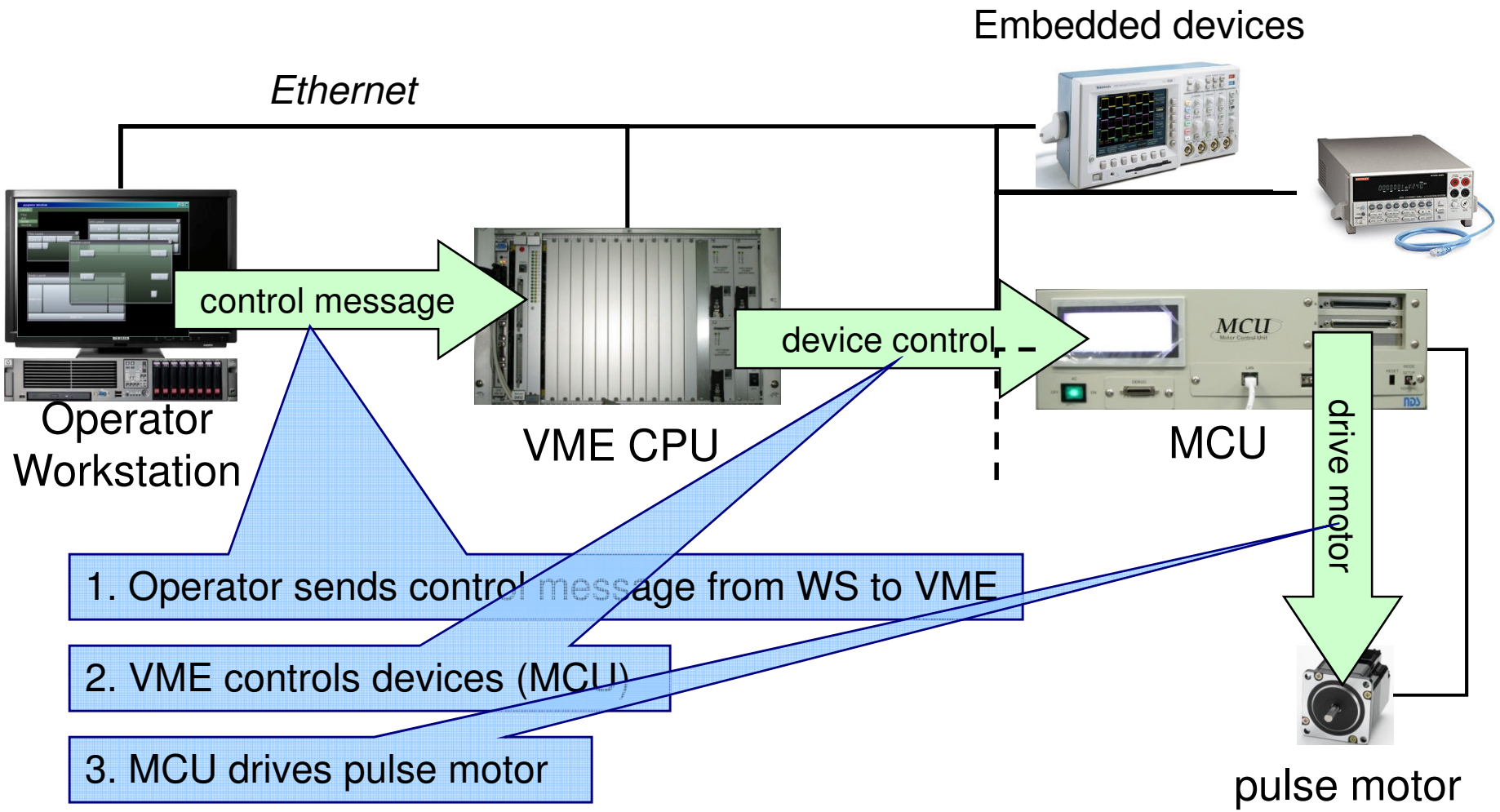
- MCU is one of the most important devices in SPring-8 control system.
  - Many MCUs are used in control system; beam slits, RF phase adjuster and attenuators, and wire-grid monitors.
- MCU is a typical embedded device with limited resources.
  - Real-time operating system (iTRON)
  - Kernel is running on flash memory
  - Fast Ethernet interface (100BASE-TX)



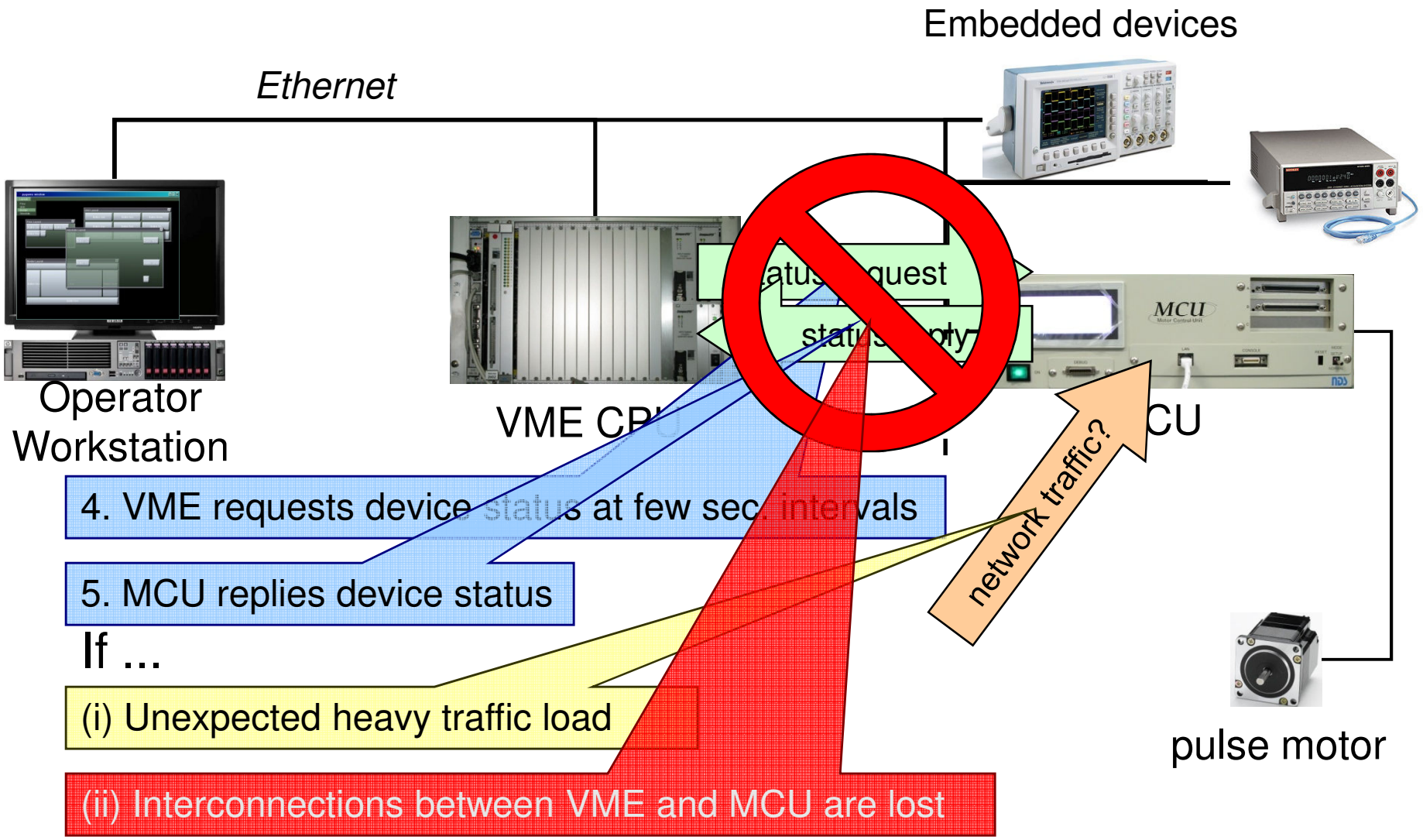

Characteristic specification
- CPU: SH-4 200MHz
- OS: NORTi4 Flash-based system
- Ethernet: 10/100BASE-TX
- Protocol: TCP/IP, socket interface
- Axis: 4-12

# Problems at SPring-8 control system

# Problem in SPring-8 control system



# Problem in SPring-8 control system



# Vulnerability studies on embedded devices

- Vulnerability scans were performed using Nessus* utility.
  - several devices are tested; digital multimeter (DMM), network switch, VME CPU, and motor-control unit (MCU).
  - DMM and MCU, did not pass the test;
    - These two devices are just the causes of SPring-8 operation failures.
  - MCU was hang-up during primitive traffic stress test.
- We performed detail investigations on MCU.

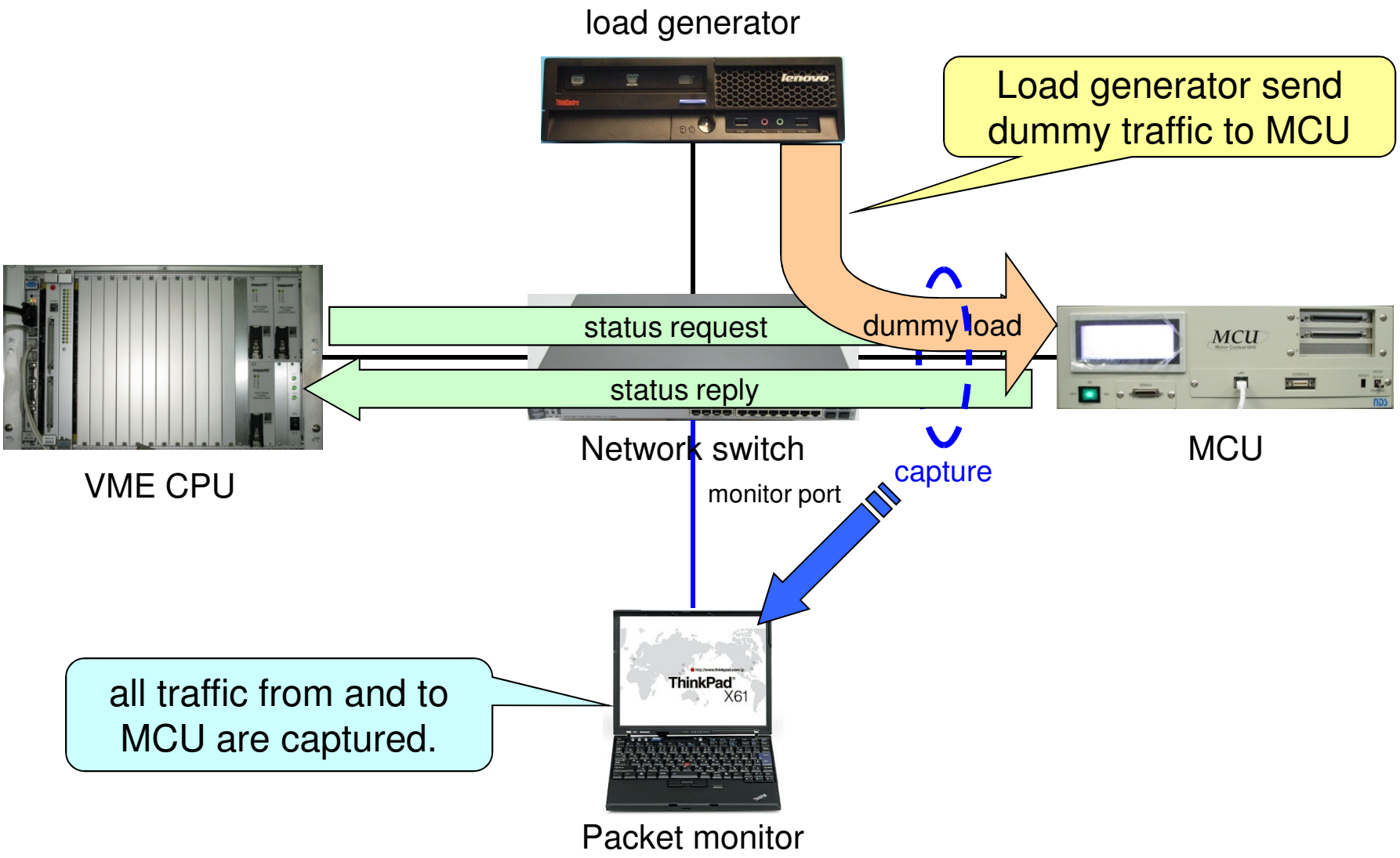
*Tenable Network Security: http://www.nessus.org/nessus/

# Vulnerability studies on motor-control unit (MCU)

- We assumed broadcast traffic affects MCU.
  - Number of nodes have been increased from 300 to 1200 for past 10 years.
  - Broadcast traffic is proportionally increased.
  - Broadcast burst (syslog flooding) have often occurred.
- We investigated relation between broadcast and MCU hang-up.
  - Instantaneous load capability
    - model of broadcast burst
  - Continuous load capability
    - model of generally flown broadcast
- By applying simulated load on MCU, traffic capabilities were measured.

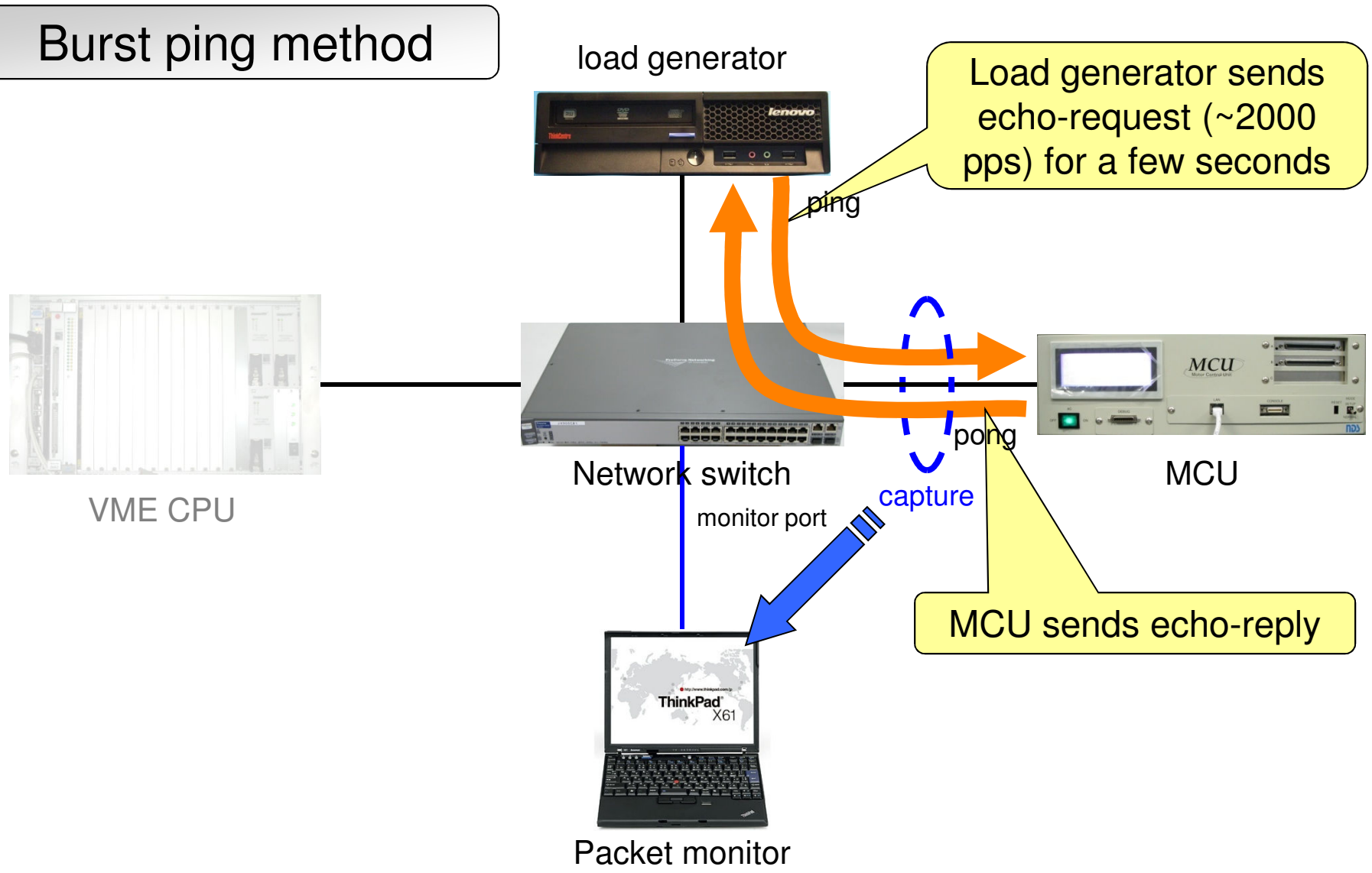
# Details of vulnerability investigation on MCU

# Test bed for vulnerability scan

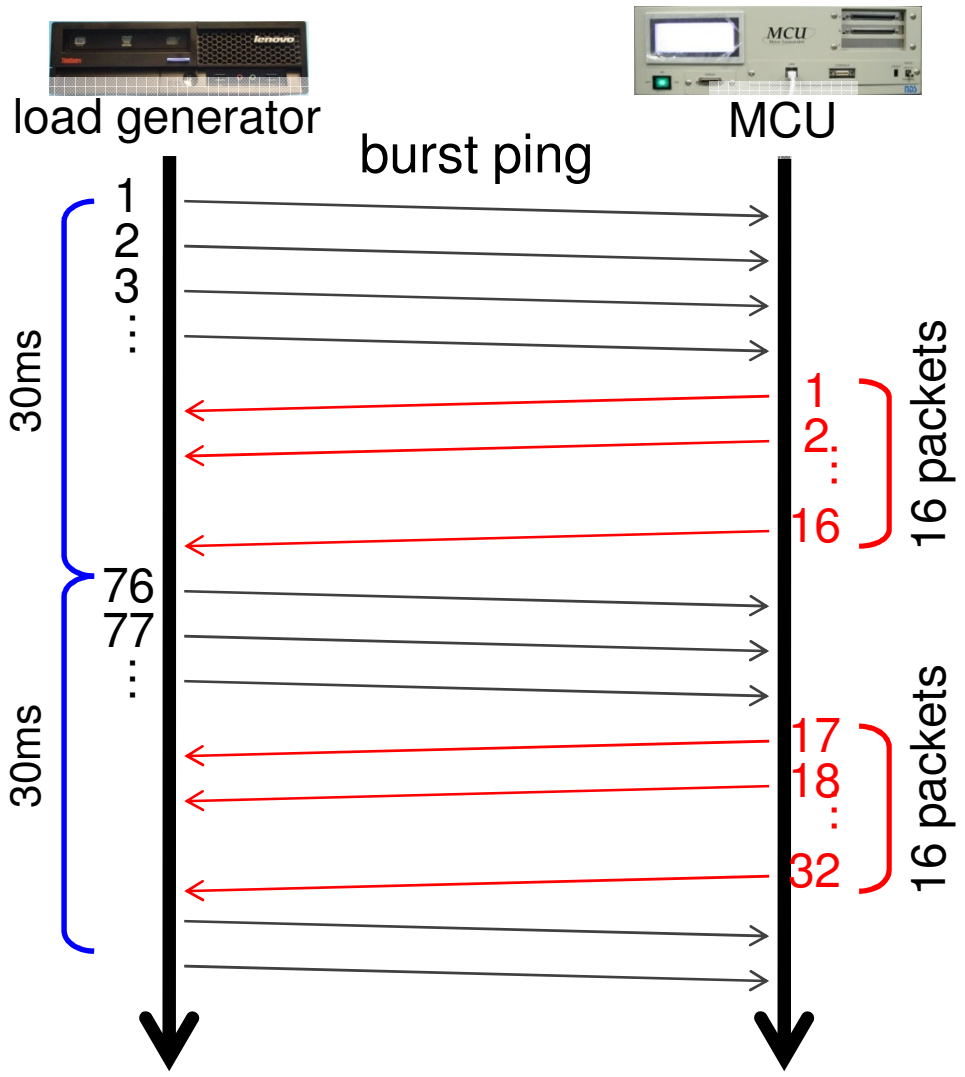


# Instantaneous load capability test

Burst ping method



# Instantaneous load capability test using burst ping




Only 16 packets are processed in 30 msec period.

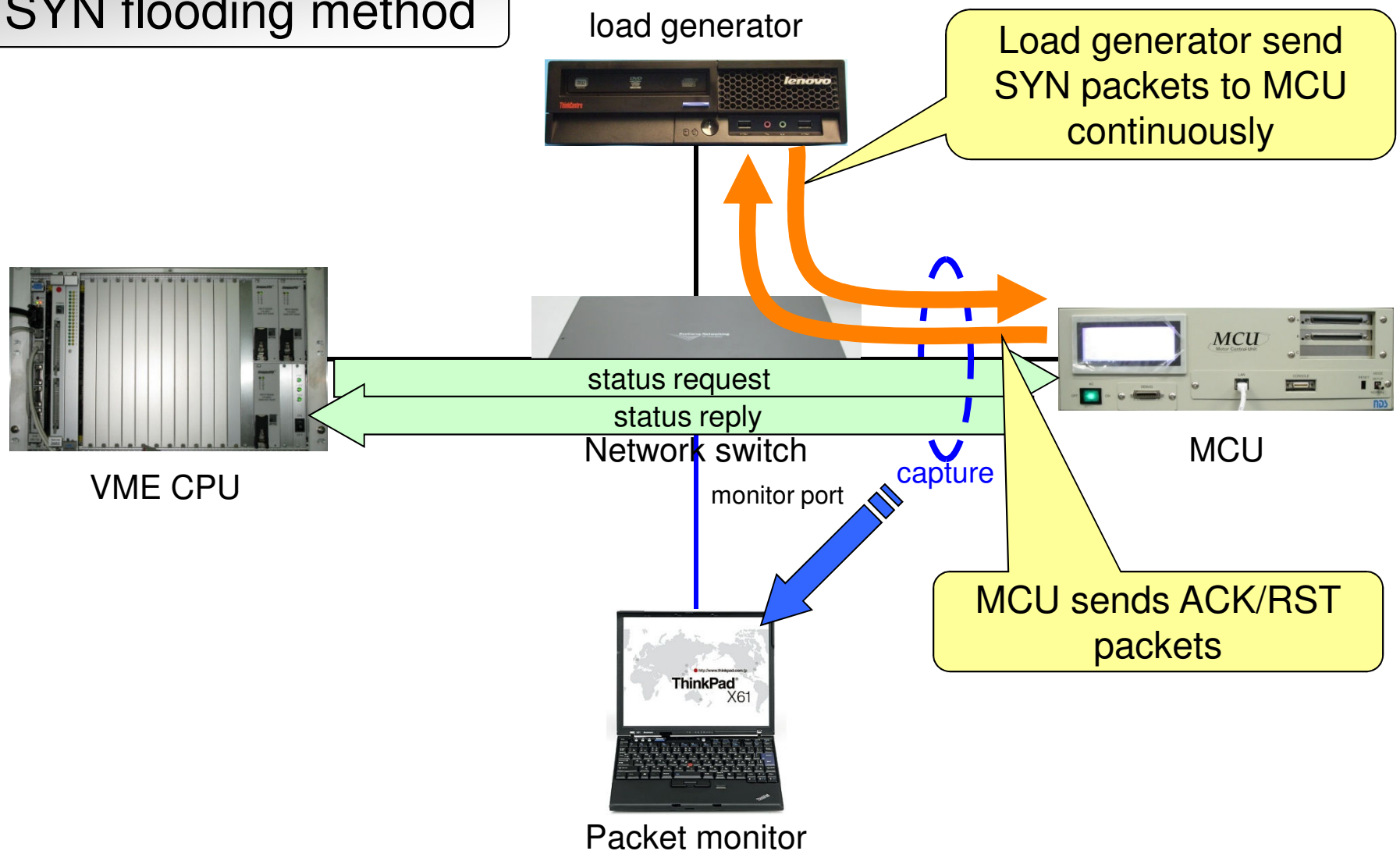
Exceeded packets are stored in buffer, packets are processed in the next period.

If buffer is overflown, packet lost is occurred.

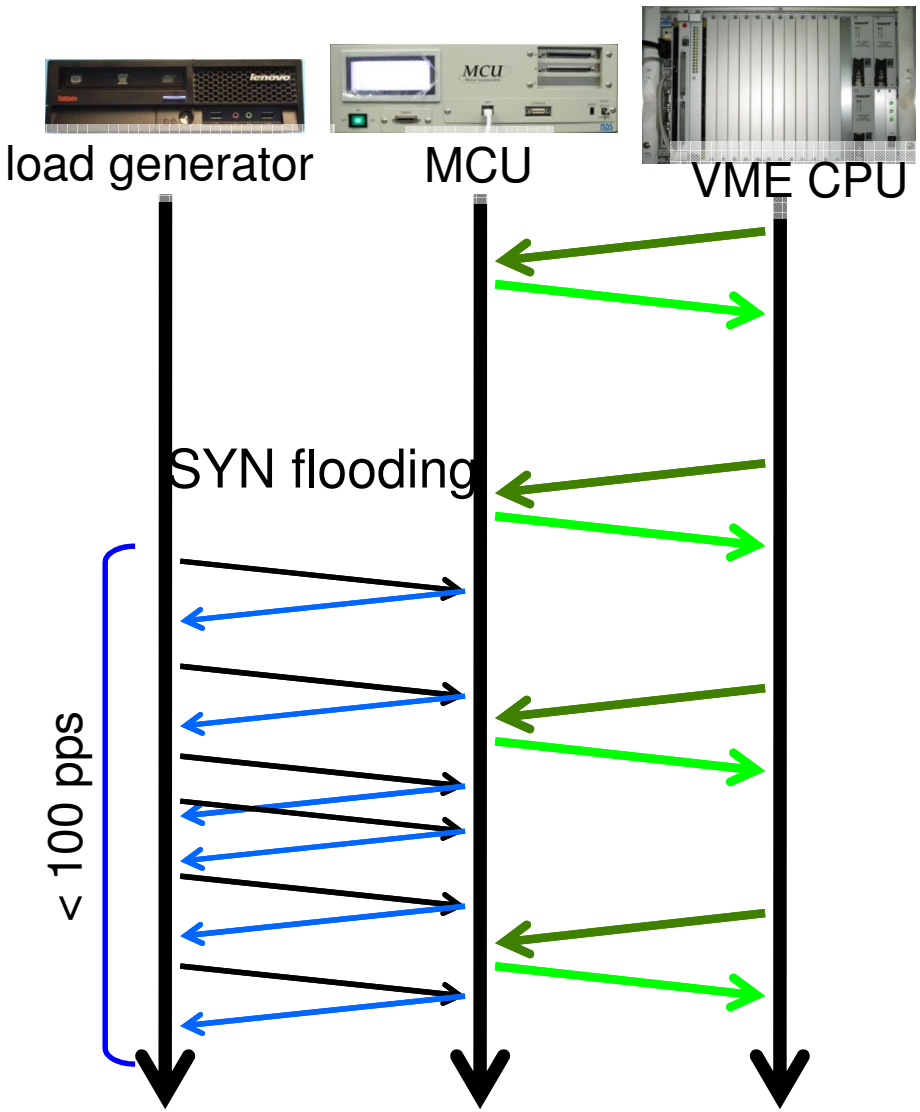
<u>MCU cannot process such a low rate packets.</u>
(16packet/30msec → 533pps)

# Continuous load capability test

SYN flooding method



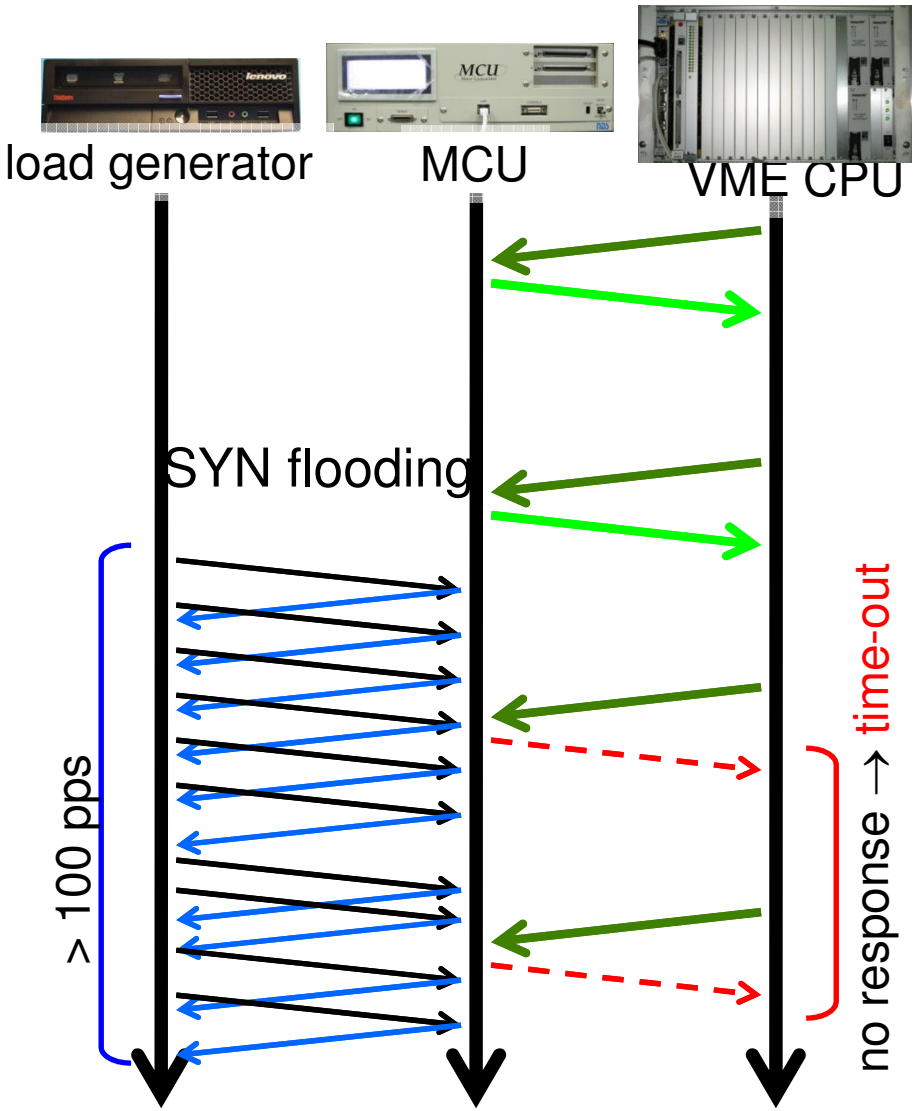
# Continuous load capability test using SYN flooding




Communication packets between VME and MCU are monitored.

If SYN flooding is < 100pps, MCU is no problem.

# Continuous load capability test using SYN flooding




Communication packets between VME and MCU are monitored.

If SYN flooding is < 100pps, MCU is no problem.

If rate exceeds 100 pps, status reply from MCU stopped.
Then connection is timed out, and operation failure is occurred.

<u>Continuous packet > 100pps can not be processed by MCU.</u>

# Results of two vulnerability test

- Instantaneous load capability:
  - 533 pps (← 16 packet/ 30 msec, with 64 byte short ping packet)
    - Overflown packets are dropped.
- Continuous load capability:
  - 100 pps (TCP SYN packet)
    - No reply from MCU, and connection timed out.
  - With detail analysis, not only listened ports, but also closed ports are affected;
    - All packets having destination MAC address to MCU are harmful.

TCP/IP implemetation of MCU cannot endure heavy traffic load

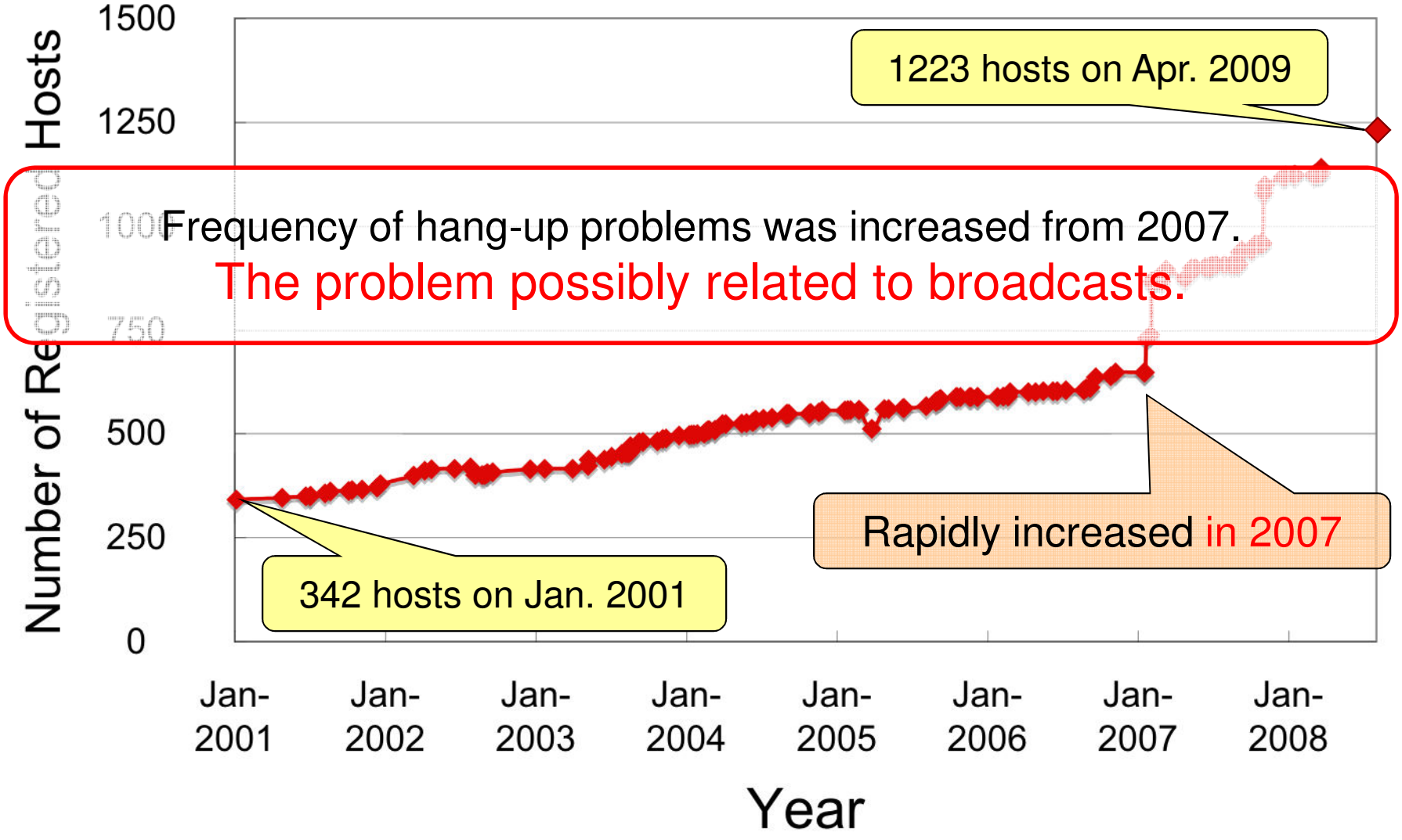
# Examination of heavy traffic load in the actual control network

- We examined traffic flow of control network using sFlow technology.**
  - Many broadcasts flow
    - NIS, Syslog, SNMP Trap, NetBIOS over TCP/IP, NTP, etc.
- We supposed that broadcast makes hang-up problem.
  - Because SYN floods to any closed port are harmful.
  - It is worth investigating correlation between broadcast traffic and hang-up.

- We analyzed number of hosts in our control network.
  - Because broadcast traffic is proportional to number of hosts in L2 network.

** T. Ohata et al., ICALEPCS2009, TUP003, *to be presented*.

# Analysis of relation between hosts and hang-up problem



# Our action to improve reliability of embedded devices in control system

# How to improve reliability of embedded devices?

- We have two approaches.
  - Tune-up of embedded devices
    - MCU must endure more heavy traffic.
    - Other devices may also be tuned up.
  - Refinement of network environment
    - Vulnerable devices should be protected from harmful traffic.

# Tune-up of embedded devices

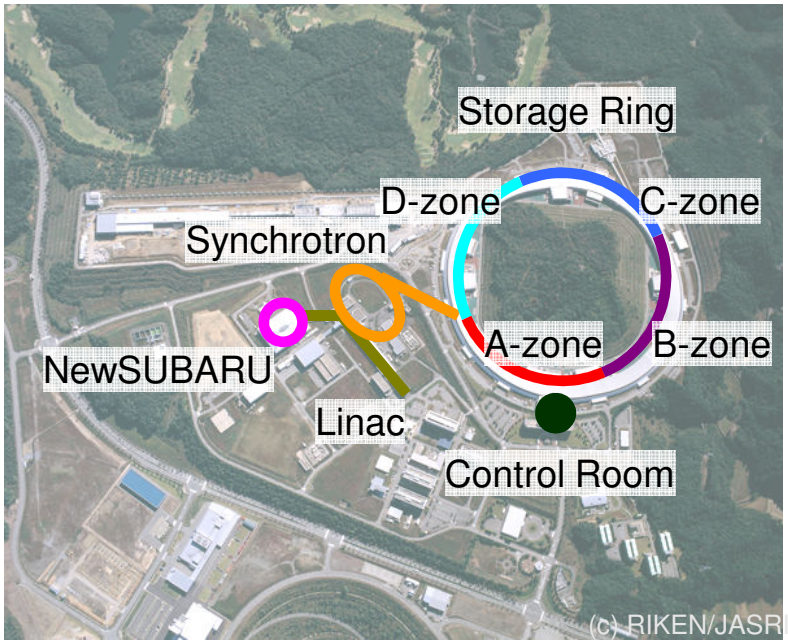
- We considered vulnerability of MCU to be tuned up.
  - Continuous load capability
    - Threshold (100 pps) may be restricted by access speed of flash memory.
    - By substituting RAM-based system instead of flash-based, performance was clearly improved. (> 100pps, no problem)
  - Instantaneous load capability
    - Threshold (533 pps) may restricted by its OS.
      - The OS (iTRON) is running under real-time mode.
    - Using Linux on MCU, MCU endure burst ping more than 2000pps; this is a optional plan.

- We tuned up MCU to overcome continuous load capability.
  - Firmware of MCU was refurbished as RAM-based system.
    - Because broadcast traffic merely exceed 533 pps, but easily exceed 100 pps by syslog flooding from our sFlow analysis.

# Refinement of network environment

- We decided to refurbish control network.***
  - Old SPring-8 control network was /21 single-segment (L2) design.
    - Broadcast domain is too large.
  - New control network is multi-segment (L3) design.
    - Broadcast traffic is dramatically reduced from > 30pps to < 1pps on each segment.

*Segmentation of SP8-LAN*




Now, no trouble on MCU have been reported after the refurbishment.

*** T.Sugimoto et al., ICALEPCS2009 WED006, *to be presented*.

# Summary

- We had many problems on embedded devices.
  - Limited resource (hardware/software) may cause problems.
- We investigated vulnerabilities of MCU.
  - Important devices for SPring-8 control system
  - Vendor's courteous support can be received.
    - We thank Hitz company's cooperation.
- Vulnerabilities on implementation was clearly found.
  - Both continuous and instantaneous load are harmful.
- We took action to improve reliability.
  - Refurbishment of MCU
    - Now, MCU is RAM-based system.
  - Refinement of network environment

- No trouble has been reported on MCU.

# Supplement 1

- We also investigated digital multi meter (DMM).
  - The DMM also had hung up with heavy traffic load.
  - Implementation of the DMM is completely black-boxed.
  - From our investigation, we found the DMM is Windows based embedded device.
- By substituting new firmware received from the DMM vendor, hang-up problem was solved.
  - We suppose that problem is caused by vulnerability on Windows OS.

# Supplement 2

- Oscilloscope
  - Our investigation is not enough to discuss.
  - From preliminary investigation: CPU is very poor.
    - File transfer rate is ~ 10 kbps.
    - ARP learning delays; it takes > 1 sec.

- Multi-channel analyzer
  - OS9 based embedded system
  - Too old to be tuned up

We gave up investigation on MCA.