Applying Linux to the Social Infrastructure BoF

Noriaki Fukuyasu, Linux Foundation
Yoshitake Kobayashi, Toshiba

Embedded Linux Conference 2015
23-25 March 2015

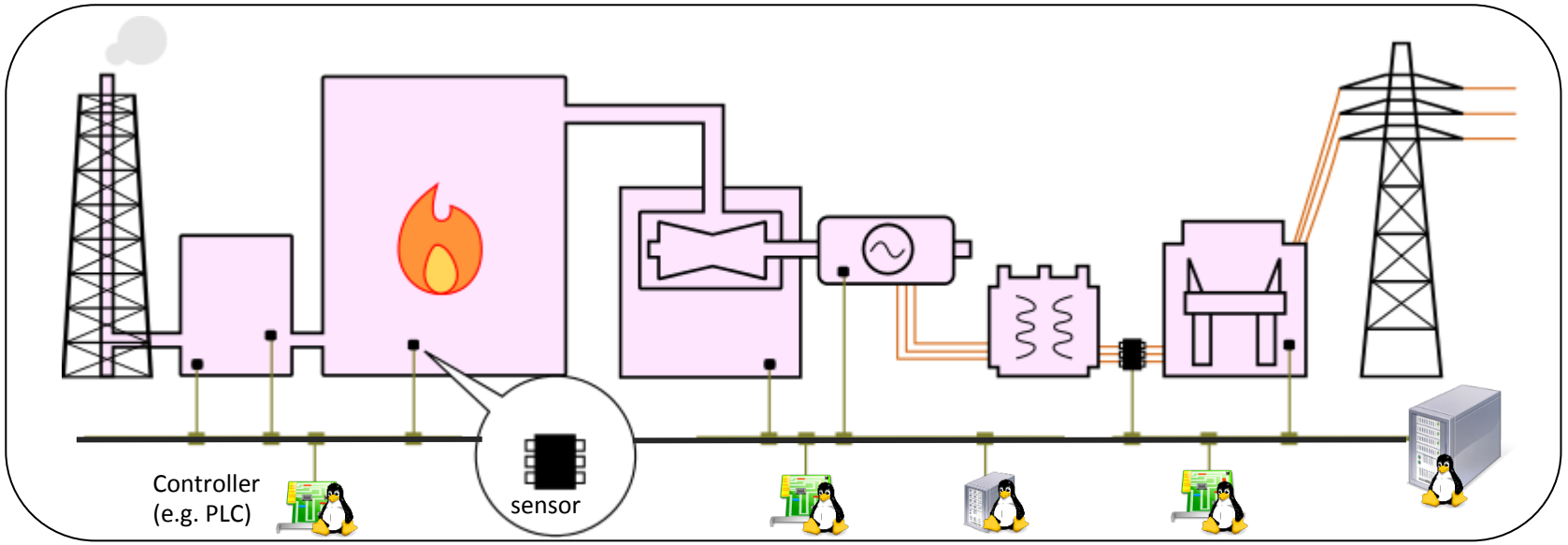
“Social Infrastructure Systems”?

- The systems which are used to run our “Society”.
- This should include the systems such as:
  - Entergy Infrastructure (Power Plants, Power Distributions)
  - Public Transportations (train, airports etc)
  - Road Management (toll gate management etc)
  - Earth monitoring
  - Communication Infrastructure

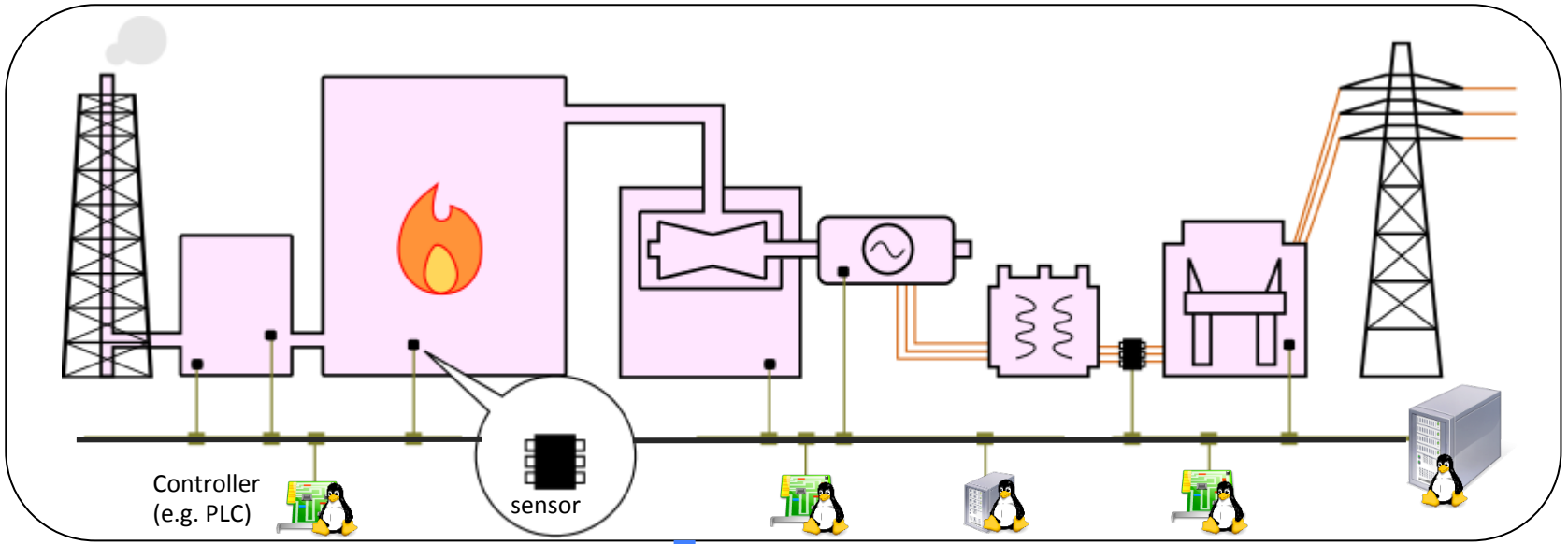
Today' Goal

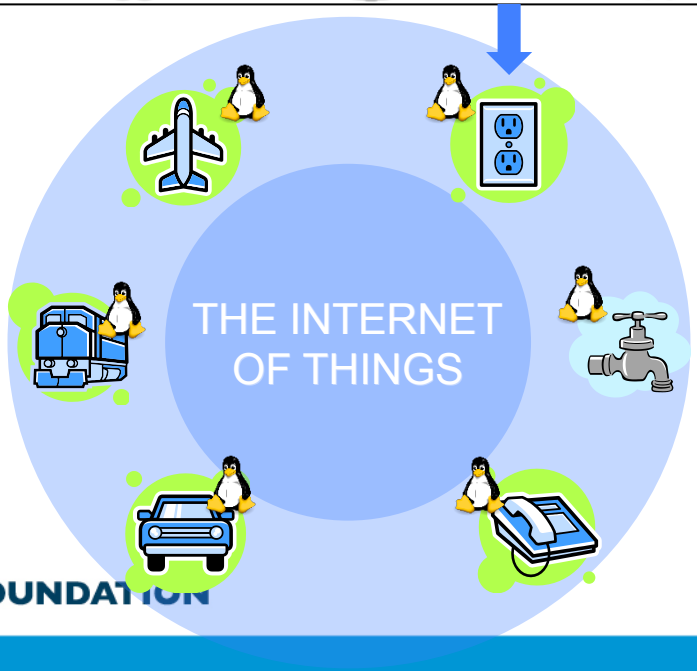
- Would like to share opinions with audience about the "future" of social infrastructure systems (= SI systems)
- Would like to hear about the "requirements" for SI systems.
- Would like to recruit companies/developers who want to work with us in this area.

Typical SI systems today: STAND ALONE



Typical SI systems Future: CONNECTED





Problem statement

The CONNECTED SI systems causes the following issues:

- Security
- Safety
- Functions

Problem statement

The CONNECTED SI systems causes the following issues:

- Security
- Safety
- Functions

The industry need to solve the issues if we wish to continue to use Linux for SI systems

What we want!

- Same level of quality, security, safety, performance and functionality with connected environment.
  - Quality: Well tested
  - Security: Internet Security etc.
  - Safety: Certification
  - Performance: RT constrain
  - Functionality:

- We want to maintain for a long time (more than 15 years).

Where we are at?

- Some companies already start working to try to understand more about these issues, hoping to solve them collaboratively in a future.
- The initial works are focused on:
  - Requirements Correction
  - Partner recruitment
- Today we would like to share some of the results of our initial works.

Our Goal:

- Develop **REFERENCE IMPREMENTATION/ META-DISTRIBUTION (*)** for SI system collaboratively.
- We are hoping to launch this project within CE Working Group at the Linux Foundation.

(*)
Reference implementation/Meta-Distribution may include:

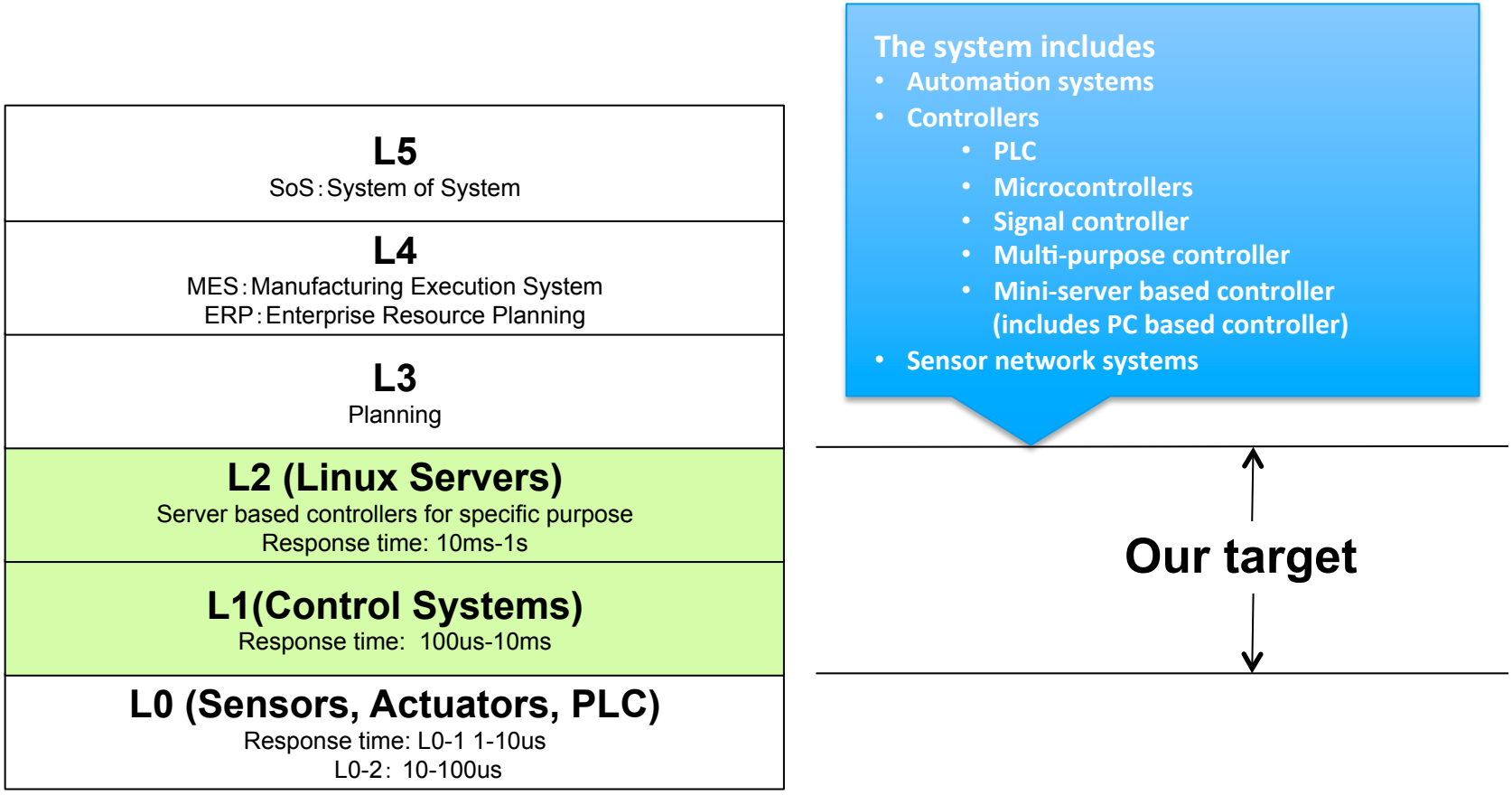
- Linux kernel and filesystem for some target boards
- Build tools/environments for companies to build their own distributions for SI systems.
- Test-cases
- Specification

LINUX FOUNDATION

The result of initial Study

Target Layers

- ICT system categorized in six layers
- L3 layers and above should be implemented by enterprise system
- Network connected controllers which uses on infrastructure systems



Requirement

	L2	L1	Plan
Security / Safety	- White-List execution control - Log output - Access Management (SE Linux/ SMACK) - One-Way gate way (Date Diode)	- Security in non-IP network - Security in IEC 611311-3 language	- Test cases for certification (EDSA, etc.)
Update	- I/O card hot swap (CG Linux) - Failover in less than 100msec	- I/O card hot swap (CG Linux) - Failover in 5msec (with memory tracking enabled)	- Dual node: CG-Linux - Single node: Live patching with deterministic behavior
Real-time	- 250usec - 1msec response time - 100msec network communication frequency - Resource Management (container)	- 100us-1ms (Hard-realtime) - 5 msec in Control frequency - Over 10 I/O cards, and 30K in/out-puts	- Preempt RT patch / Hard realtime support / Test cases
Reliability	- Compatibility test - 24/7 operation - Error detection (CPU/Memory/BUS etc) - Error record (trace/Panic Log/Crash dump)	- Compatibility test - 24/7 operation - Error detection (CPU/Memory/BUS etc) - Error record (trace/Panic Log/Crash dump)	- Framework for failure detection and recovery / Verification test cases
Long-term Support	- 7 years sales and 17 years maintenance - Enable old Linux drivers - 2038 problem	- 12 years sales and 30 years maintenance - Enable old Linux drivers - 2038 problem	- Very Long Term Supported (VLTS) distribution / VLTSI kernel
Functional Safety			- SILnLinux
Virtualization	- HW update - Compatibility - Full-system test		- L2: Might be able to use current VM technology - L1: Very light weight VM / Container with RT capability /

Standards to work with

Requirement for standards	Implementation	Kernel	OSS	Proprietary software	Remarks
IEC61131-3	Development environment, Execution Engine	-	UniSim(For Education)	SIMATEC, Codesys	
IEC61850	Kernel, Library, Hardware	-	LibIEC61850 (C), OpenIEC61850(Java)	SISCO	
IEC61970 (EMS, CIM,CIS)	Middleware, Hardware	-	NONE	NONE	
IEC62278 (RAMS)	Development process	-	-	-	
IEC62280	Library, Application	-	OSS libraries (encryption, verification, authentication) are used for implementation		
ISO15745-4 (ADSNet)	Library, Application			NX-dlink	
IEC61508 SIL2	Development process	SIL2LinuxMP (OSADL)			SIL2MPLinux is working in progress
IEC61508 SIL4	Development Process	NONE			
PROFINET	HW(PROFINET IRT), Library, Application	NONE			Usually, SDK is provided by device vendor.

Test

The tests required in SI Systems are including the followings:

- Vulnerability (eg. Virus check)
- Performance Test
  - Testing APIs as non-functional requirements
- Conformance Test
- Install test
- Boot Test (Inc. APPs)
- Boot time (Inc. APPs)
- Run-Frequency (Inc. APPs)
- Devise driver test
- Heat-Run Test (with HW.)

LINUX FOUNDATION

Free Discussion