PANEL Services, Adaptation and Future Computing

Awareness and Adaptation in Service Computation and Delivery

Moderator: Joel J. P. C. Rodrigues

Institute of Telecommunications, University of Beira Interior, Portugal

joeljr@ieee.org

NetGNA Next Generation Networks and Applications Group

Networks and Multimedia
Instituto de Telecomunicações, Portugal

Department of Informatics
University of Beira Interior, Portugal

PANEL Services, Adaptation and Future Computing

Panelists

- Kendall Nygard, North Dakota State University, USA
- Fatma Mili, Oakland University - Michigan, USA
- Li Li, Avaya Labs Research/Avaya Inc., USA
- Steffen Fries, Siemens, Germany
- Ali Beklen, IBM, Turkey

Designing Adaptive Systems
A necessity rather than choice

Fatma Mili, Oakland University

Embodied cognition

- Situatedness: Systems viewed in situ. Behavior cannot be dissociated from the situation
- Embodiment: bodies through which they receive input, produce actions
- emergence: Granularity—very small scale interactions give rise to high level behavior.

Adaptive design paradigm

- Top down design
  - Requirements (set of pairs context-behavior)→
    - designer selects a process
    - Designer implements a process
- Bottom up adaptive behavior
  - Requirements (desired high level behavior) →
    - Designer selects rewards
    - Autonomous units explore, select

Comparison

Traditional (top down)

- necessity to fully capture all possible interactions
- Problems often computationally hard
- Complexity of the problem and solution
- Potential for many unexpected interactions

Adaptive (autonomous interacting components)

- Desired behavior not instantaneous
- Evolution →
  - Time delay
  - Possibility of dead ends and trial and error
- Interactions between the different components weaved into the behavior
- Randomized algorithms

Towards Intelligent Communication – Convergence with the Web

Li Li

Current Affair: Standard Highlights

AVAYA

- Web Service: proprietary API → SOAP → REST → Web?
  - SOAP: CSTA from ECMA, Parlay X 3.0 from ETSI
  - REST: OneAPI 1.0 from GSMA, Constrained RESTful Environments from IETF, Facebook API, twitter API
- Presence: phone tag → simple presence → rich presence and location → context and prediction?
  - SIP and XMPP from IETF, Parlay X, CSTA (location)
- User Interface: array of windows → web browser → rich interaction and collaboration in one client?
  - HTML 5 from W3C
  - Server-Sent Events from W3C, WebSocket from IETF

Problems and opportunities

AVAYA

Web is fragmenting…

- Started as an interconnected information space
- Becoming a platform of isolated applications – fragmented user contexts
- approach: use semantic web to integrate user contexts

Web is asynchronous…

- Information is not reachable until linked
- Unbounded delay between information publication and consumption – delayed user awareness
- approach: use real-time web and event-driven web to reduce delays

SIEMENS

Corporate Technology

Security in Industrial Automation Environments

Steffen Fries

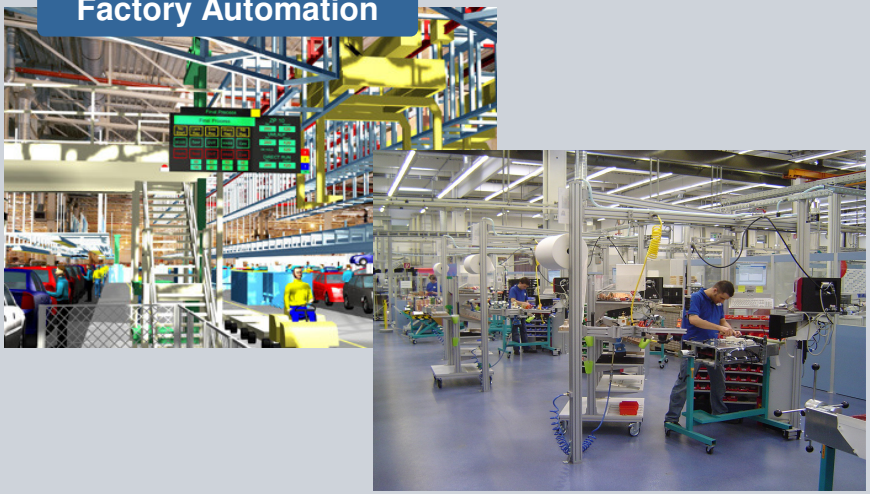
Siemens AG, CT T, GTF IT Security
☎ : +49 89 636 53403
💻 : steffen.fries@siemens.com

Increasing Intelligence and Open Communication in Industry Automation Environments

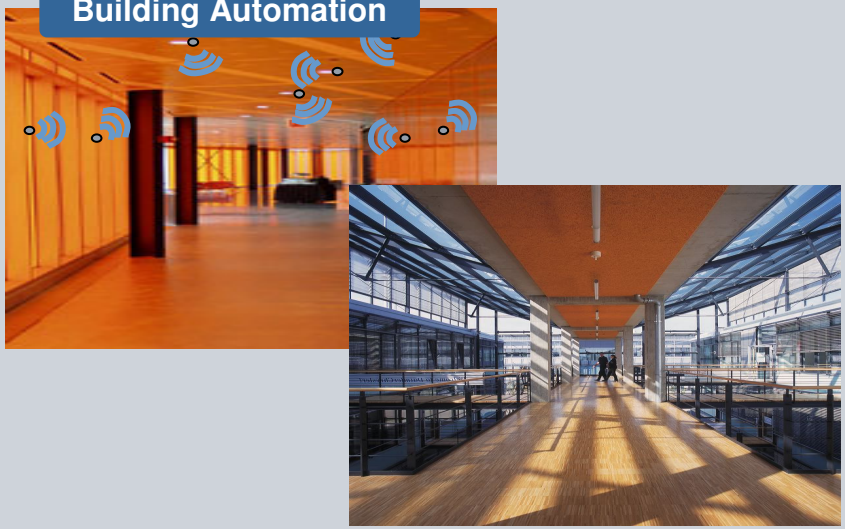
SIEMENS

Process Automation

Factory Automation



Building Automation



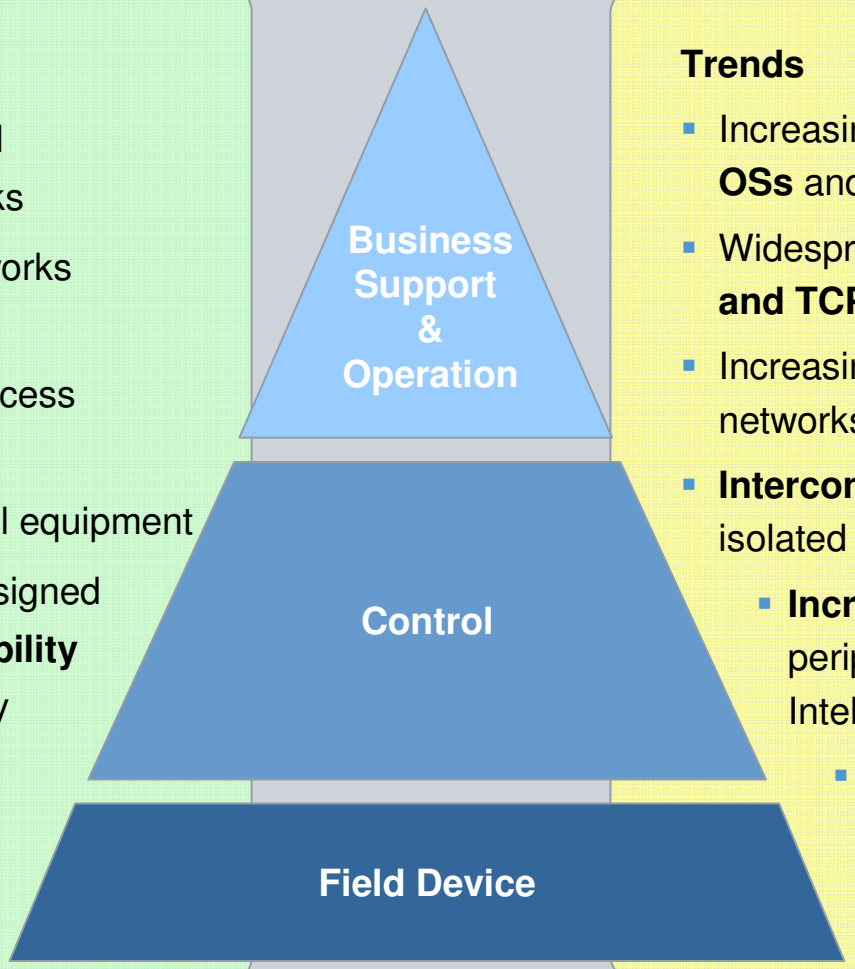
Energy Automation

IT-Security Becomes a Pre-requisite for Future Control Systems Driven by Convergence of Safety & Security

SIEMENS

Status

- Predominantly **isolated** communication networks
- Often **proprietary** networks and applications
- **Physically secured** access to networks
- **Long lifetime** of control equipment
- Systems are mainly designed for **performance, reliability and safety**, not security
- Often availability is the most important security objective



Trends

- Increasing **usage of standard OSs** and applications
- Widespread usage of **Ethernet and TCP/IP** (including Internet)
- Increasing usage of **wireless** networks
- **Interconnection** of formerly isolated networks
  - **Increasing intelligence** in peripheral components (e.g. Intelligent Access Devices)
    - IT-security becomes a pre-requisite for safety applications

Embedded Security Mechanisms Provide Essential Functionality for Ensuring System Integrity

SIEMENS

Security is required to ensure Safety-relevant system properties in environments exposed to attacks

Plant Integrity Check	Verify integrity of overall plant installation (deployed components, cabling, software).
Original spare parts (Anti-Counterfeiting)	Ensure that original spare parts are installed, and not counterfeited replacements with poor quality.
Software Integrity Check	Ensure that firmware and configuration has not been altered. Device operating only with valid configuration.
Secure Software Update	Ensure that only approved software updates are installed in compliance with defined update procedures.
Secured Machine Communication	Prevents manipulation and interception of communicated control and service data (device control, remote service).

Trends and potential Research Topics in Industrial Automation Security

SIEMENS

Security parameter are the base to ensure an appropriate protection of communication between different system entities as well as services like licensing or anti counterfeiting. Setting up and maintaining security parameter securely is crucial!

Security Trends

- Machine-2-Machine connectivity down to field level devices is a major driver for Future Internet.
- Device authentication as prerequisite to protected communication of devices and device-oriented services.
- The non-human security environment requires new device-oriented security and identity infrastructures.

Challenges

- Security is a process → adaptation
  - technical (system design and development)
  - organizational (system management and operation)
- Device-oriented security and identity infrastructure and services
- Plug-and-play security to ease additional administrative effort

Context Awareness and Adaptation: Intelligence, Control, and Decision-making Issues

Kendall E. Nygard
North Dakota State University

Cooperative Distributed Autonomous Systems

- Examples
  - Sensor networks
  - Networked weapons systems
  - Ambient systems
  - Pervasive systems
  - Ubiquitous systems
  - The Smart Grid
- Characteristics
  - Many heterogeneous platforms
  - Widely distributed
  - Distributed Intelligent processing
  - Highly interconnected
  - Must work together in purposeful ways

Reactiveness and Directedness

Reactiveness is achieved by a set of behaviors

Directedness is achieved by an intelligent capability that identifies and exploits structure, maintains a knowledge base, and accesses system knowledge to advantage

Distributed Decision Making

The Case for Centralization

- Rich sources of very complete data and information promotes “best practice” decisions
- Resources can be managed efficiently and effectively
- Embedded devices, processors and systems are viewed as parts of larger and complex infrastructure

The Case for Decentralization

- Individual entities can be context-aware and combine dynamically to drive emergent and adaptive behaviors
- Embedded devices, processors and systems can (sometimes) perform well for certain autonomous functions
- It is essentially impossible to control a large and diverse system with a ‘top-down’ logic – this would require a way to instruct each element as to what to do at each step
- Robustness, redundancy, and timeliness of decision-making is improved through distributing responsibilities.

A Key Unmet Need in Cooperative Control

Develop protocols and algorithms that….

- Work from the bottom-up
- Allow agents to reach consensus on shared information
- Work with limited and unreliable information
- Work with dynamically changing interaction topologies
- Are reliable, secure, and resilient

Cross Cutting Concerns

- Inherently distributed, resulting in systems with duplication of code across many components.
  - Makes functional components less self-contained
  - Often decreases software quality
  - Makes functional components less self-contained
  - Makes reasoning at the architectural level difficult
- Security, context awareness and cultural and language issues are cross-cutting

Some Research Questions

- How to….
  - Balance the need for local autonomy with the need for global consistency and control?
  - Monitor systems that are configured in ad hoc networks?
  - Exploit large-scale concurrency?
  - Maintain appropriate levels of security and privacy?
  - Design distributed software in situations with massive non-functional requirements?

Event Driven Service Oriented Architecture

Ali BEKLEN
Software Group
IBM Turkey

alibek@tr.ibm.com

Computation World 2010

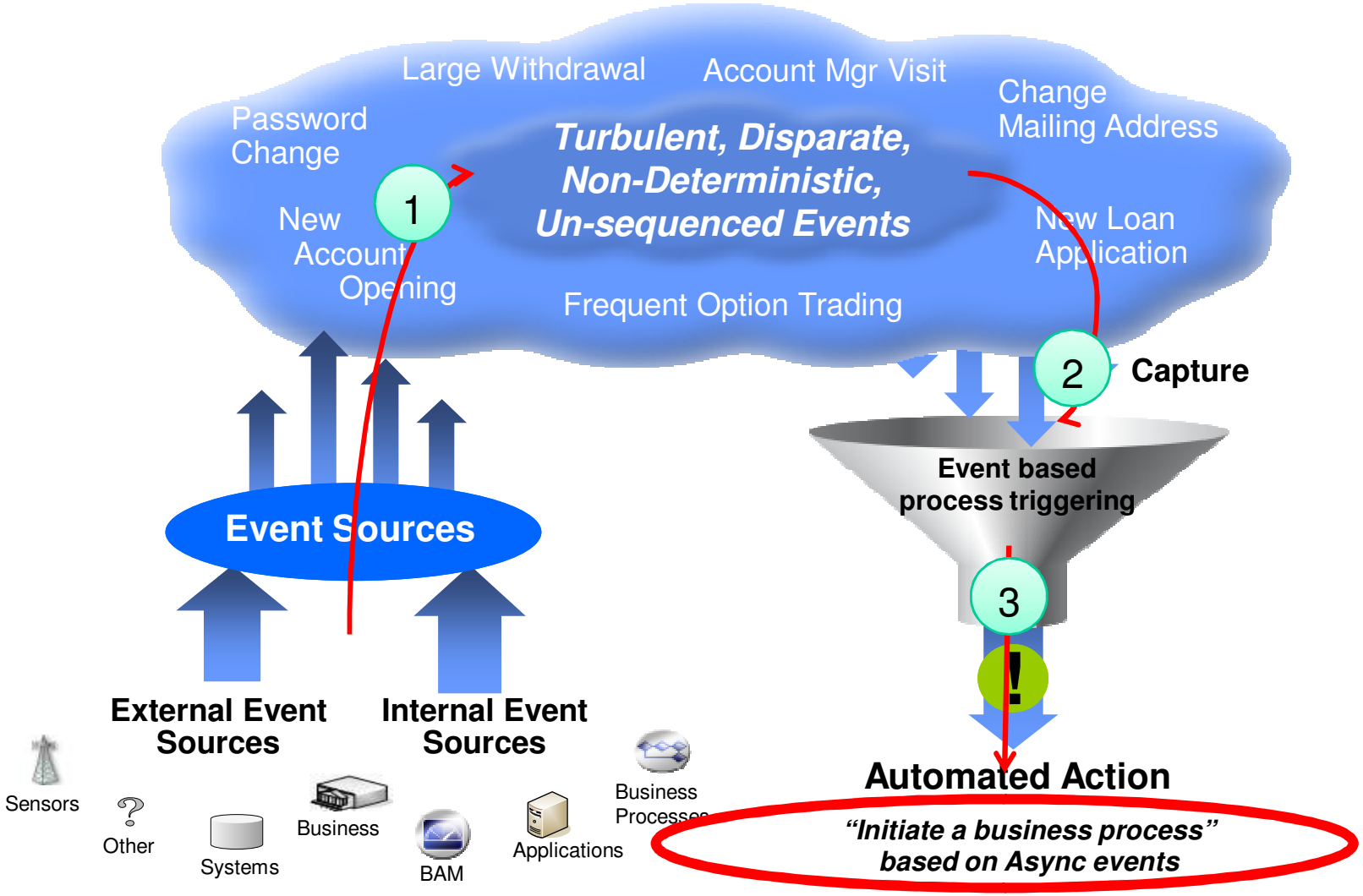
Agenda

- Events
- Event driven SOA

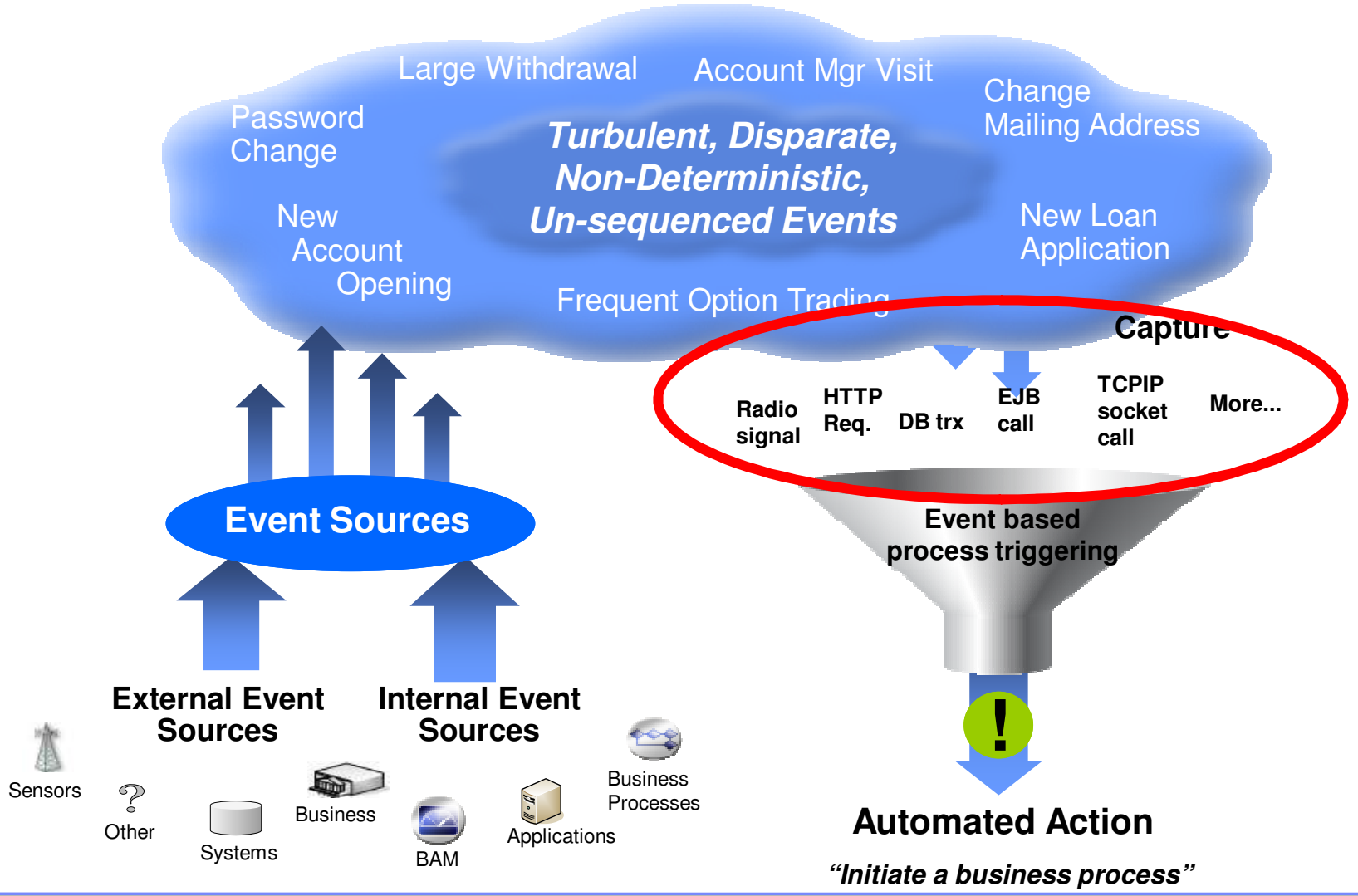
Events


A call to the help desk
A sale is made
A New Location is Detected
Data center temprature is changed
A PIN is changed
Multiple Product Inquiries
Event Sources
External Event Sources
Internal Event Sources
Sensors
Other
Systems
Business
BAM
Applications
Business Processes

Events and SOA



Events and SOA



Will next generation SOA or SOA 2.0 be based on events

What are the potential research areas for implementation

- **Event handling frameworks or adapters**
- **A new web service specification for sensor events**
- **Supporting all types of sensors in a box**
- **more**

धन्यवाद
Hindi

多謝
Traditional Chinese

ขอบคุณ
Thai

Спасибо
Russian

Thank you
English

Gracias
Spanish

ευχαριστώ
Greek

Teşekkürler
Türkçe

alibek@tr.ibm.com

Dziękuję
Polish

Obrigado
Brazilian Portuguese

شكراً
Arabic

Danke
German

Grazie
Italian

多谢
Simplified Chinese

Merci
French

நன்றி
Tamil

ありがとうございました
Japanese

감사합니다
Korean