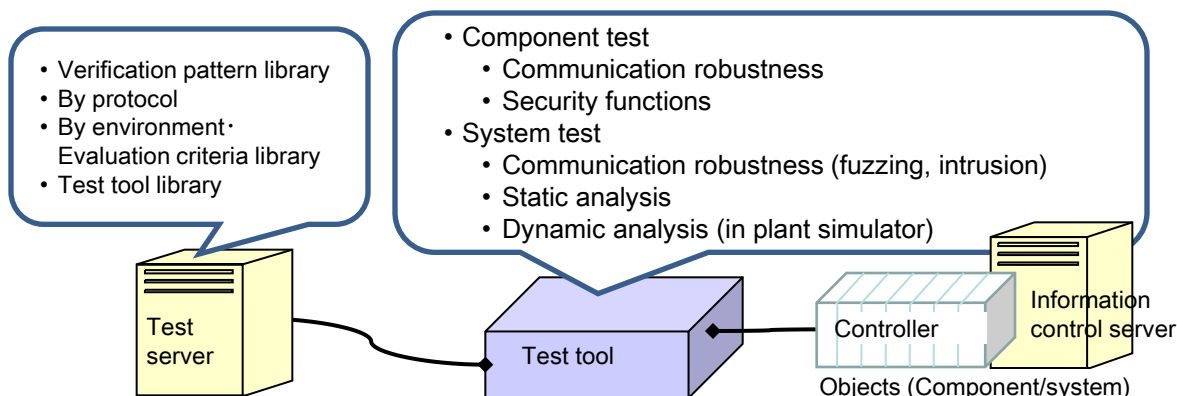# 11. Major implementation plans

(1) System security verification

■Objectives

To provide the latest security verification tools for system components
- To Develop and share security verification tools for components and systems.
- To save and share security verification patterns
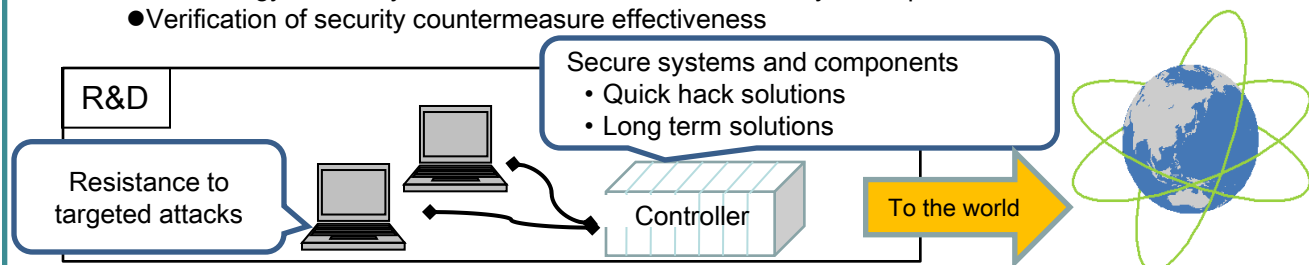- To verify connectivity

- Verification pattern library
- By protocol
- By environment・
  Evaluation criteria library
- Test tool library

- Component test
  - Communication robustness
  - Security functions
- System test
  - Communication robustness (fuzzing, intrusion)
  - Static analysis
  - Dynamic analysis (in plant simulator)

Test server

Test tool

Controller

Information control server

Objects (Component/system)

(2) Establishment of structures and technology to enhance security

■Objectives

To develop secure structures and technology originated in Japan which will meet control system requirements (performance, stability, long-term lifecycle, compatibility with legacy systems and standards etc.)
- Secure structures and technology (encryption, authentication, key management, safety operation, specification description, verification, multiplexing etc.) for wide-area cooperative control in control systems and Smart City (Open Network)
- Technology to identify incident areas linked with control system operations
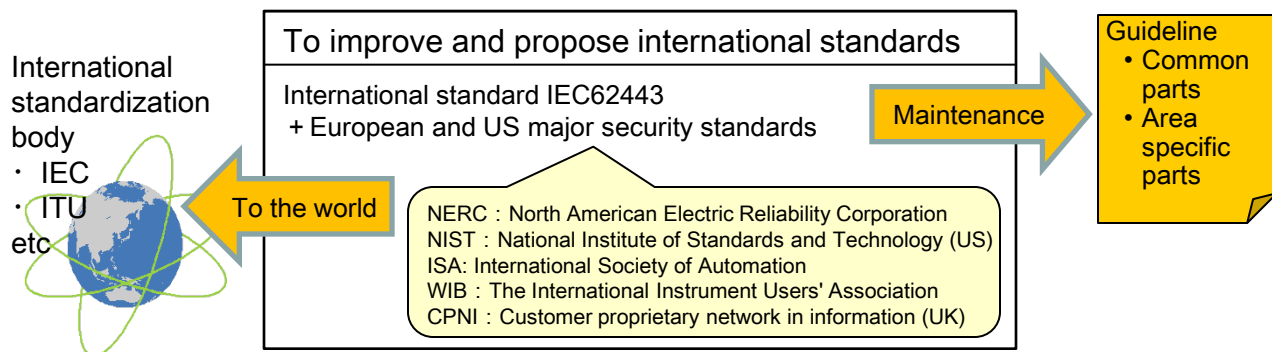- Verification of security countermeasure effectiveness

R&D

Resistance to targeted attacks

Secure systems and components
- Quick hack solutions
- Long term solutions

Controller

To the world

(3) Security international standard

■Objectives

To take an initiative in security international standardization
- To ensure early acquisition of international standard proposals
- To make the first move to propose international standard plans (based on development technology)
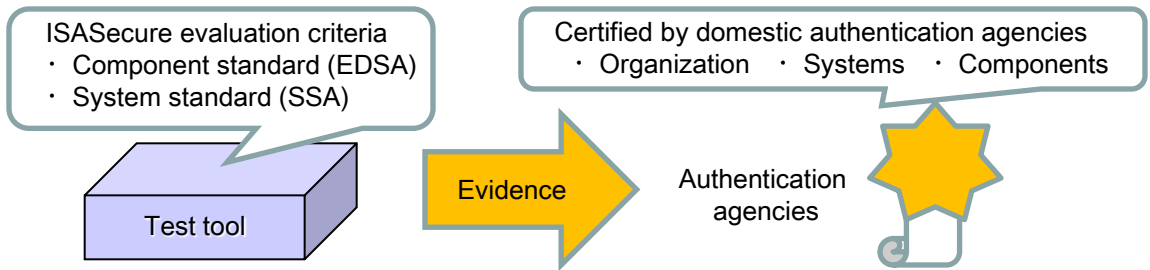- To formulate standard guidelines from security-related standards

International standardization body
・ IEC
・ ITU
etc

To improve and propose international standards

International standard IEC62443
+ European and US major security standards

Maintenance

Guideline
- Common parts
- Area specific parts

To the world

NERC : North American Electric Reliability Corporation
NIST : National Institute of Standards and Technology (US)
ISA: International Society of Automation
WIB : The International Instrument Users' Association
CPNI : Customer proprietary network in information (UK)

(4) International standard compliance certification

■Objectives

To shorten the time to acquire international certificates based on the evaluation criteria by third parties
- Certification linked to test tools
- Short period (low cost) of certification linked to domestic authentication agencies
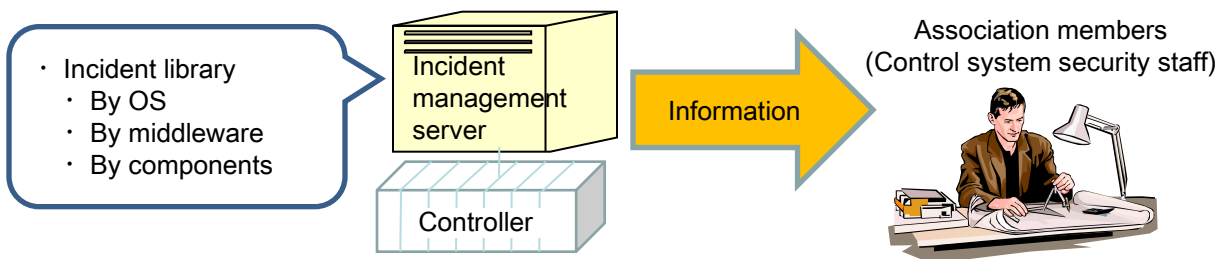
ISASecure evaluation criteria
- Component standard (EDSA)
- System standard (SSA)

Test tool

Evidence →

Authentication agencies

Certified by domestic authentication agencies
- Organization ・ Systems ・ Components

(5) Incident support

■Objectives

To support incident handling related to control systems
- To provide manuals of incident handling
- To develop and offer application environments of incident libraries
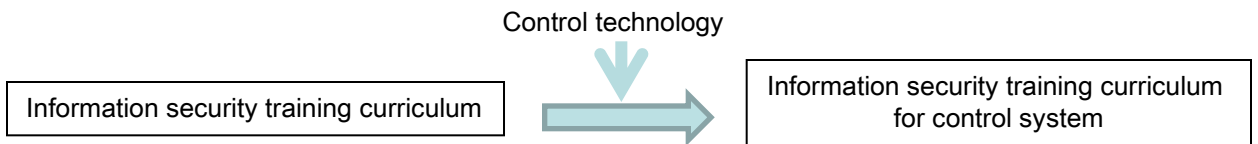- To support association members with incident handling (including on-sites)

- Incident library
  - By OS
  - By middleware
  - By components

Incident management server

Controller

Information →

Association members
(Control system security staff)

(6) Human resource development

■Objectives

To conduct security training including simulations for control system engineers
- Training of security construction with assumption of control systems
- Training of troubleshooting with assumption of control systems

Control technology

Information security training curriculum →

Information security training curriculum for control system

(7) Promotion

■Objectives

Demonstration of security alert and the effect of security countermeasures
- PA system
- FA system
- Wide-area cooperative systems

Simulation

Monitoring of facilities

Alert elements →

Controller

Information control server