

Security Operation Requirements at Device Maker

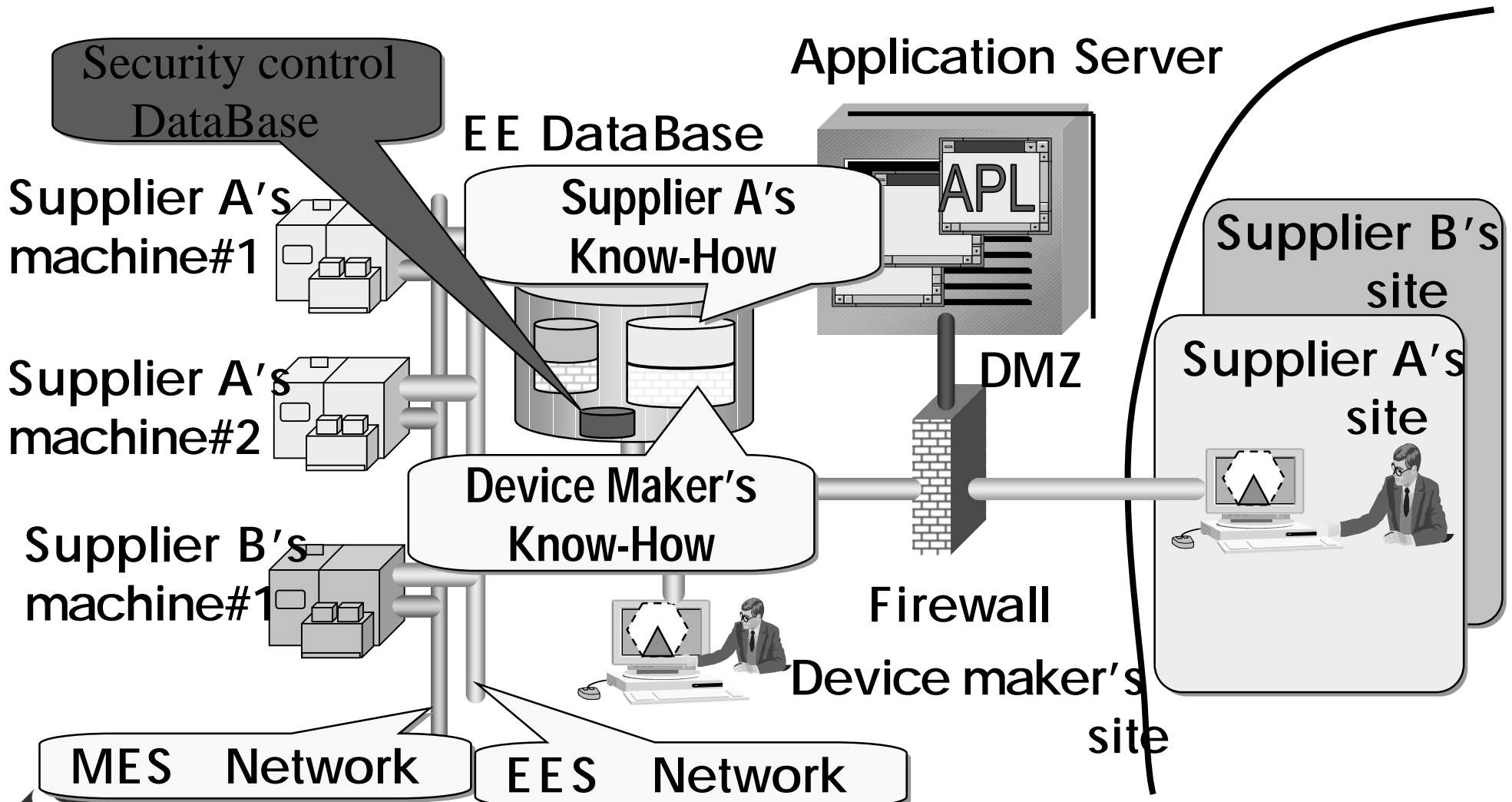
Kanji Morikawa

Hitachi, Ltd

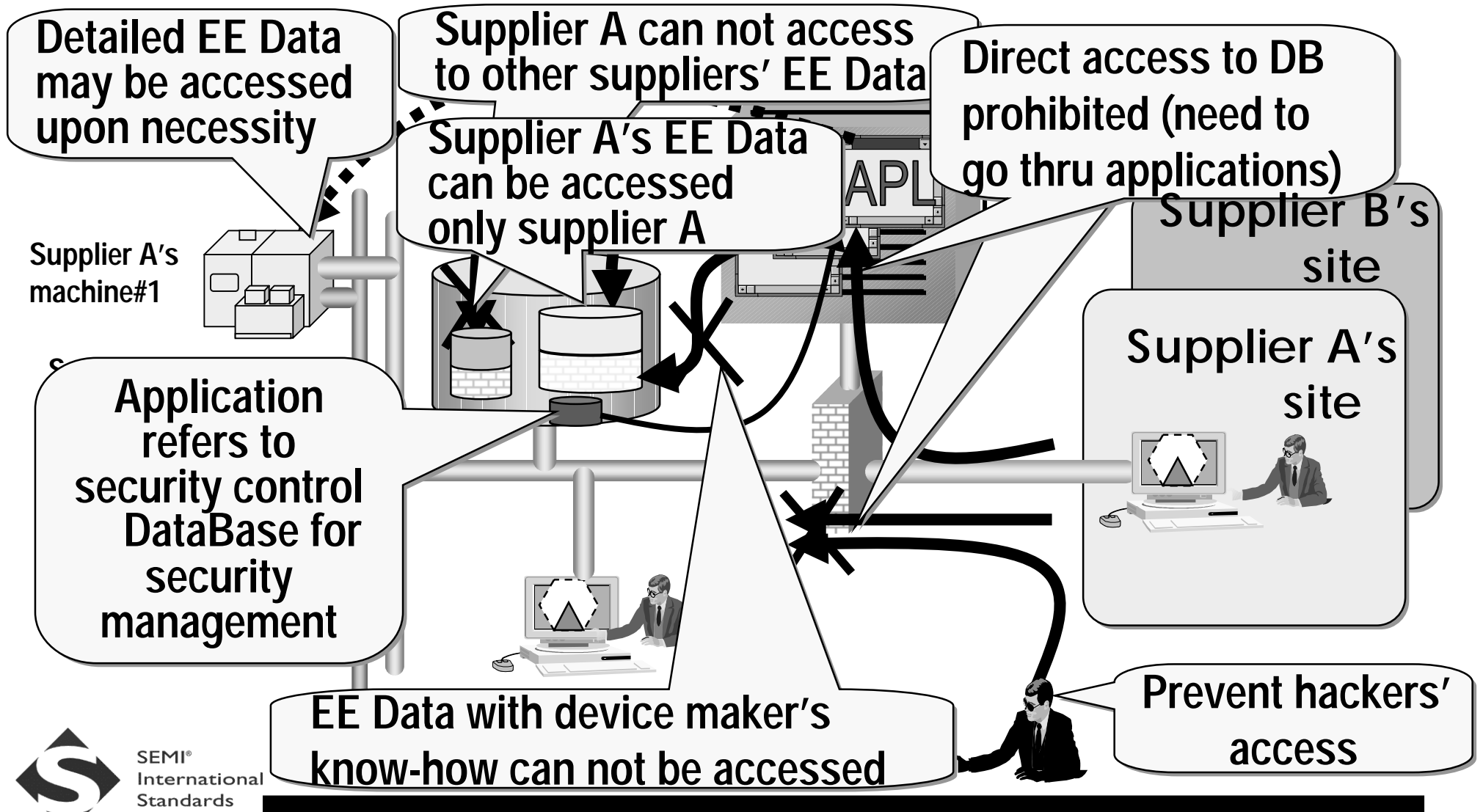
Security Necessity for EES

- **Purpose of EE Data sharing**
 - Device maker and equipment supplier cooperate in order to improve equipment productivity
- **Needs of EE Data sharing**
 - Quick analysis of equipment status and performance will be made possible both at equipment supplier and device maker
- **Security is needed to prevent**
 - unwanted outflow of such information as business secrets and/or through network.
 - jeopardizing factory operation by unjust alteration of EE Data and relevant information such as process recipes

Security Operation Model

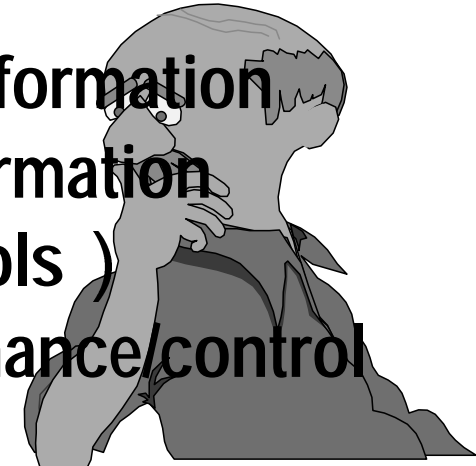


Security Management Model



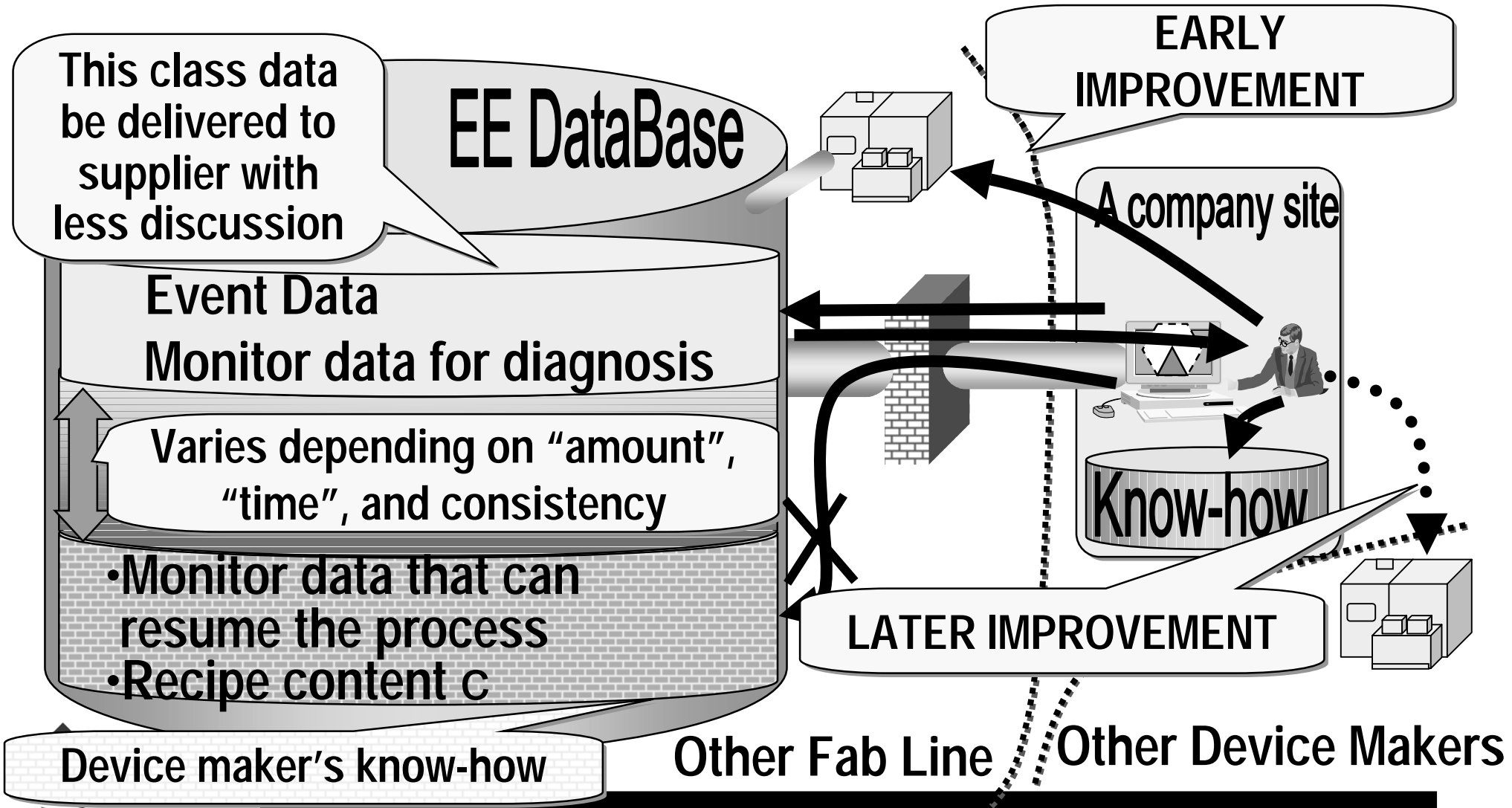
Security Policy (1)

- What is to be protected?
 - General information
 - Company classified and in-house information
 - Customer and related business information
 - Production data (line capability, # of tools)
 - process data(recipe body, tool performance/control information)
- From whom is it to be protect?
 - A general hacker, viruses.
 - Other device makers
 - Equipment makers



Contradiction!
Device maker wants to disclose all the data it has to the supplier as attain the purpose, there are some data device makers do not want to disclose by all means!!

EE Data Security Management Model Example



Device Makers' Concern in EES

Introduction (1)

- **Concern in EE Data sharing**
 - The equipment performance in my factory can be improved
 - Same thing happens in other device makers
 - A forerunner desperate effort can be readily transferred to late comer's tools!
 - This is not good for some particular competitive technologies such as APC algorithm
 - Device makers do not want to disclose APC algorithm employed
 - and related information that can be used for reverse engineering of APC algorithm



Device Makers' Concern in EES

Introduction (2)

- **Concern in remote maintenance operation**
 - **Modification to the tool control S/W and/its parameters**
 - **Risk of possible resultant deterioration in process performance**
 - **Possible damage to tool operation**
 - **Deeper access to EES network**
 - **Potential risk of data unjust modification of factory data and resultant damage to factory operation**
 - **Possible overloading of tool controller**
- **Conflicting commands to tools with MES**



Measure to Security Operation Concerns



- Close examination of security characteristics per data collection items
 - Directly related to EES Data Base & EE applications designing

This analysis and management plan are most important

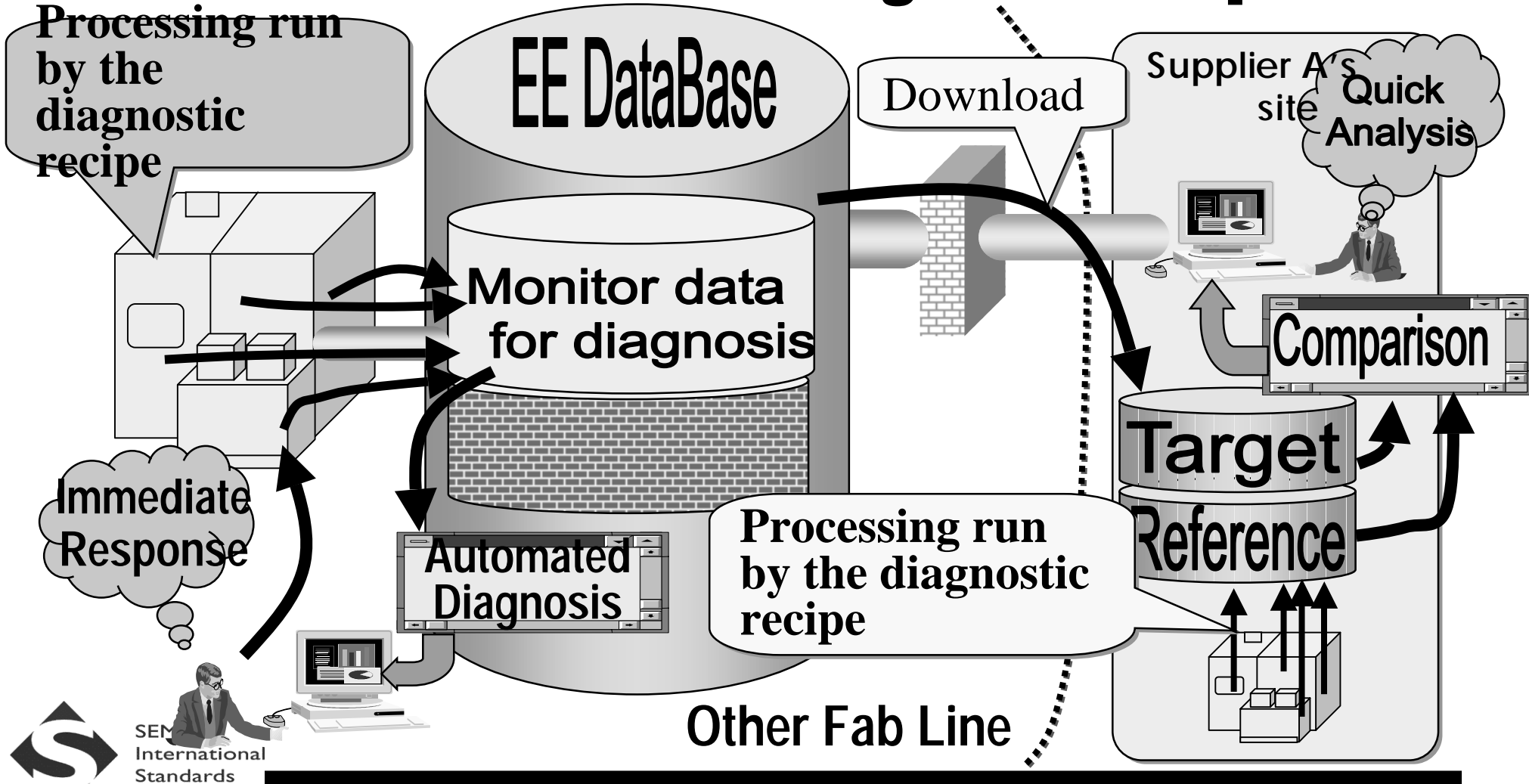
- Allow no direct remote modification to tool control programs and their parameters
 - Supplier sends the data EES server
 - Downloading to the tool may be done by engineers of device makers
 - testing/confirmation of modified functions and regression testing need more study



EE Data Sharing with Device Maker's Ease

- EE Data obtained according to "*Equipment Diagnosis Recipe*" can be easily shared
 - Recipes designed for equipment characteristic/performance extraction
 - Both sides to agree the content
 - Device maker to agree to run these recipes occasionally to collect necessary EE Data to share and diagnosis
 - This will allow EE Data sharing down to the detailed level and device maker feel easy to deliver all EE Data to the supplier

EE Data Sharing and Diagnosis Model Based on Common Diagnosis Recipe



Merit of Common Diagnosis Recipe

- Device makers are happy because;
 - need not to disclose the very recipe used for production
 - Since production quantity is not presumed.
- Equipment suppliers are happy because;
 - Highly efficient EE Data collection especially of that tool specific characteristics
 - Recipe can be written so as to efficiently dig some critical characteristics of the process chamber
 - This brings about eventually very high diagnostic sensitivity in process characteristics/performance of the particular chambers
 - Allow analysis and comparison of many same type tools to further enhance the diagnosis ability



EE Data Security Level

- **Security levels are function of;**
 - **EE Data item**
 - **EE Data item combination**
 - **EE Data time coverage**
 - **Relevant processed recipes**
 - **Tool usage stages such as ramp-up and production runs**

EE Data Security Level Details (1)

- Security level variation with EE Data items
 - Individual detailed equipment event data **LOW**
 - valve open and close
 - Direct process representation data **HIGH**
 - optical emission data in etching
- Security level variation with EE Data combination
 - If detailed EE Data obtained from multiple different tools from the same equipment supplier, it is potentially possible to do reverse engineering to know how that device maker runs their “process modules”

EE Data Security Level Details (2)

- **Security level variation with data generation time**
 - confidentiality of old data decreases with time
 - old EE Data of the processes not run currently has lower confidentiality
 - **EE Data obtained in equipment ramp-up period including period before shipment**
 - EE Data should be shared extensively to seed up the ramp-up business
 - **EE Data during process development or new product development**
- bears the highest confidentiality**

EE Data Security Level Details (3)

- Security level variation with EE Data time coverage
 - EE Data of short duration: LOW LEVEL.
 - EE Data of prolonged time period: HIGH LEVEL
 - production quantity may be presumed
- Security level variation with occasions or incidence such as upon failure and maintenance
 - For quicker business EE Data is to be shared
 - EE Data to confirm tool's restored function is to be shared
- Security level variation with tool usage stages such as ramp-up and stable production runs

Portal Site as Security Management

- Security measures cost becomes serious burden
 - if each pair of device makers and equipment suppliers sets up individual contracts and connections
- Portal site as “security provider” among device makers and equipment suppliers
 - This makes security management feasible for each of device makers and equipment suppliers
 - even if # of equipment makers increases dramatically
 - Small to medium size makers can adapt EES with relative ease

–Standardization of I/F and APL is accelerated



System Examples by Security Policy Levels (4)

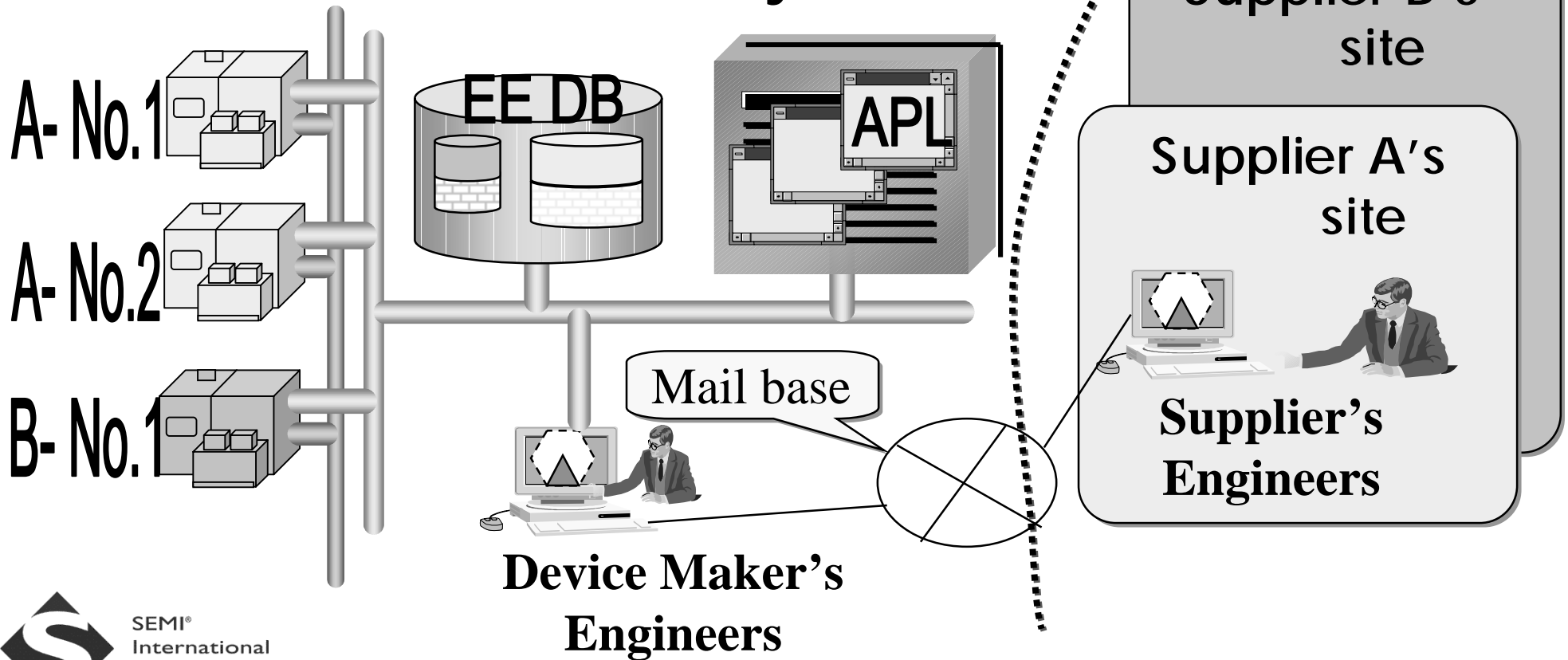
- One-Line external connection with multiple suppliers through portal site
- Suppliers utilize EE Data
- Full disclosure of all EE Data
 - mutual contract on security
 - Equipment suppliers take full responsibility of equipment operation and productivity
- Security management is taken care of at the portal site
 - EE Data storage at portal site
 - (minimum EES IT infrastructure maintenance and operation cost at device makers)

Security Management Operation

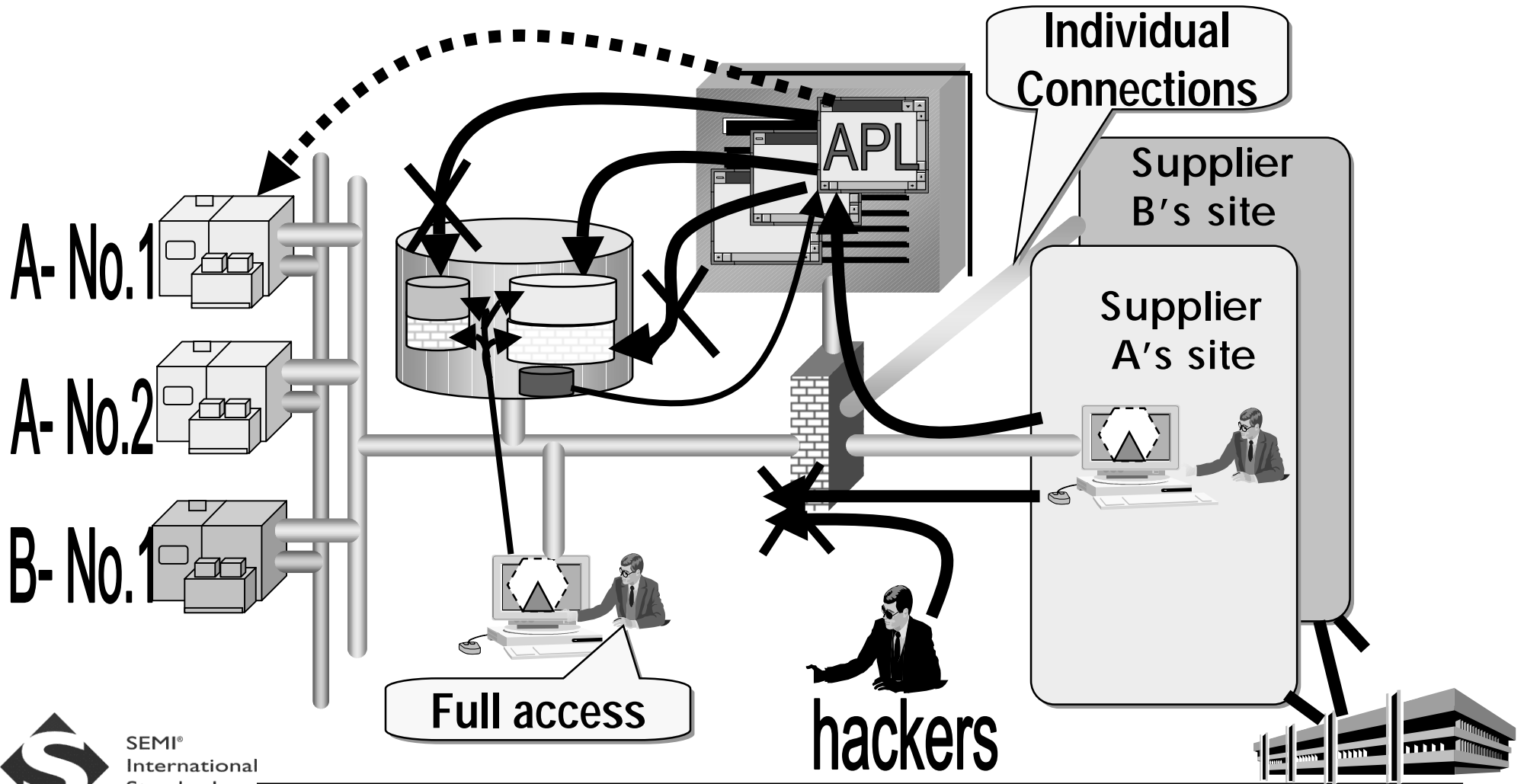
- Upon Introduction EES followings are needed;
 - ① Contract with each of individual equipment suppliers on security measures for their internet connections
 - ② Set Restriction on EE Data access by equipment suppliers
 - ③ Some classification tagging on EE Data items
- Maintenance Operation
 - ① For newly introduced equipment
 - i. registration of new data items (utterly new equipment)
 - ii. authentication and authorization of personnel for EE Data access per tools
 - ② Deletion of tools and relevant security information
 - ③ EES access monitoring
 - ④ Inspection of security proper measures per contract

System Configuration Example (1)

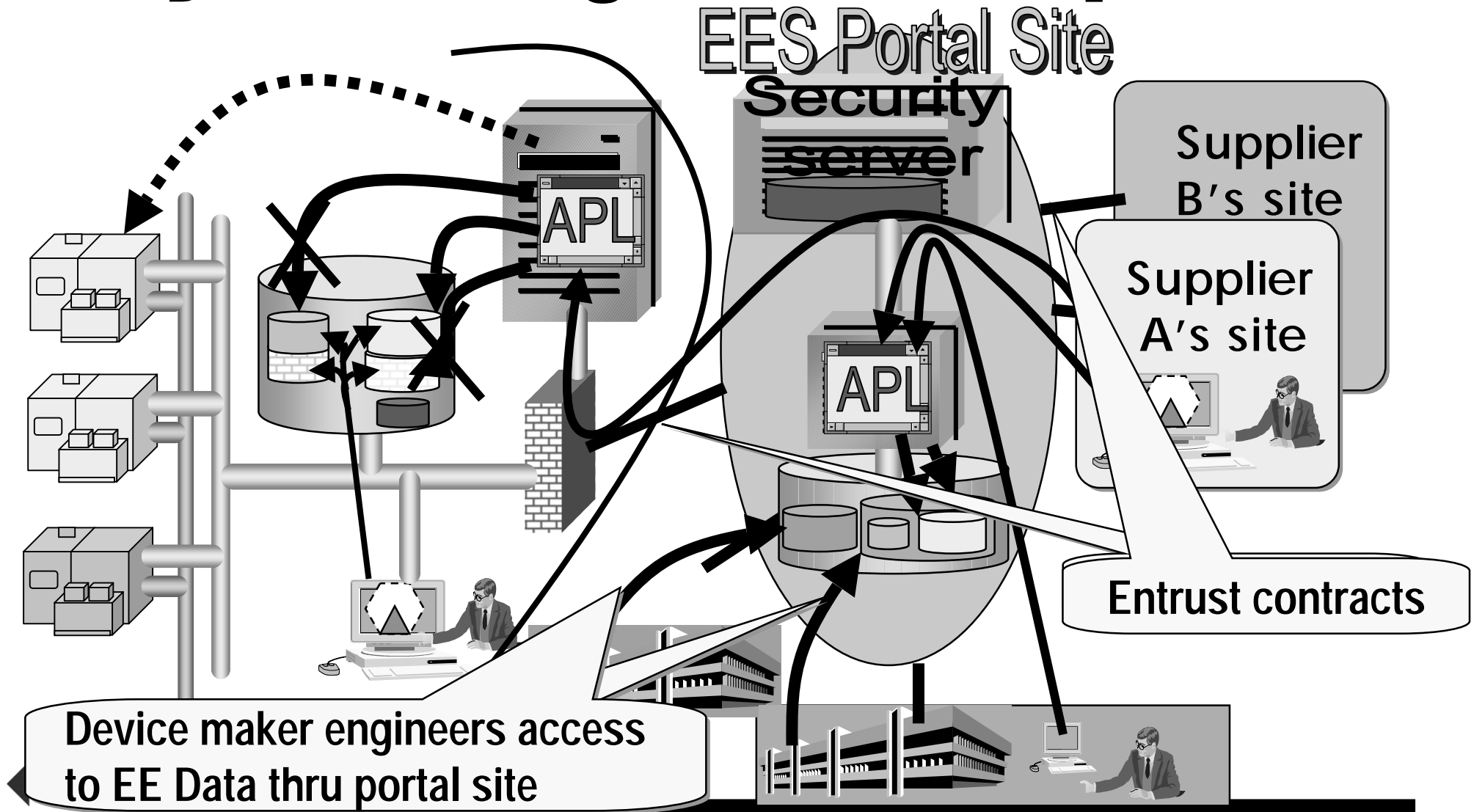
Security management is done "manually"



System Configuration Example (2)



System Configuration Example (3)



Summary

- Security management is a big subject in order to introduce EES.
- Mutual merit must be well studied and understanding must be shared among device makers and suppliers in EE Data sharing.
- EES is in the first stage and has many to be examined in the industry.
- Cooperation between device makers and suppliers is indispensable to resolve the foreseen problems