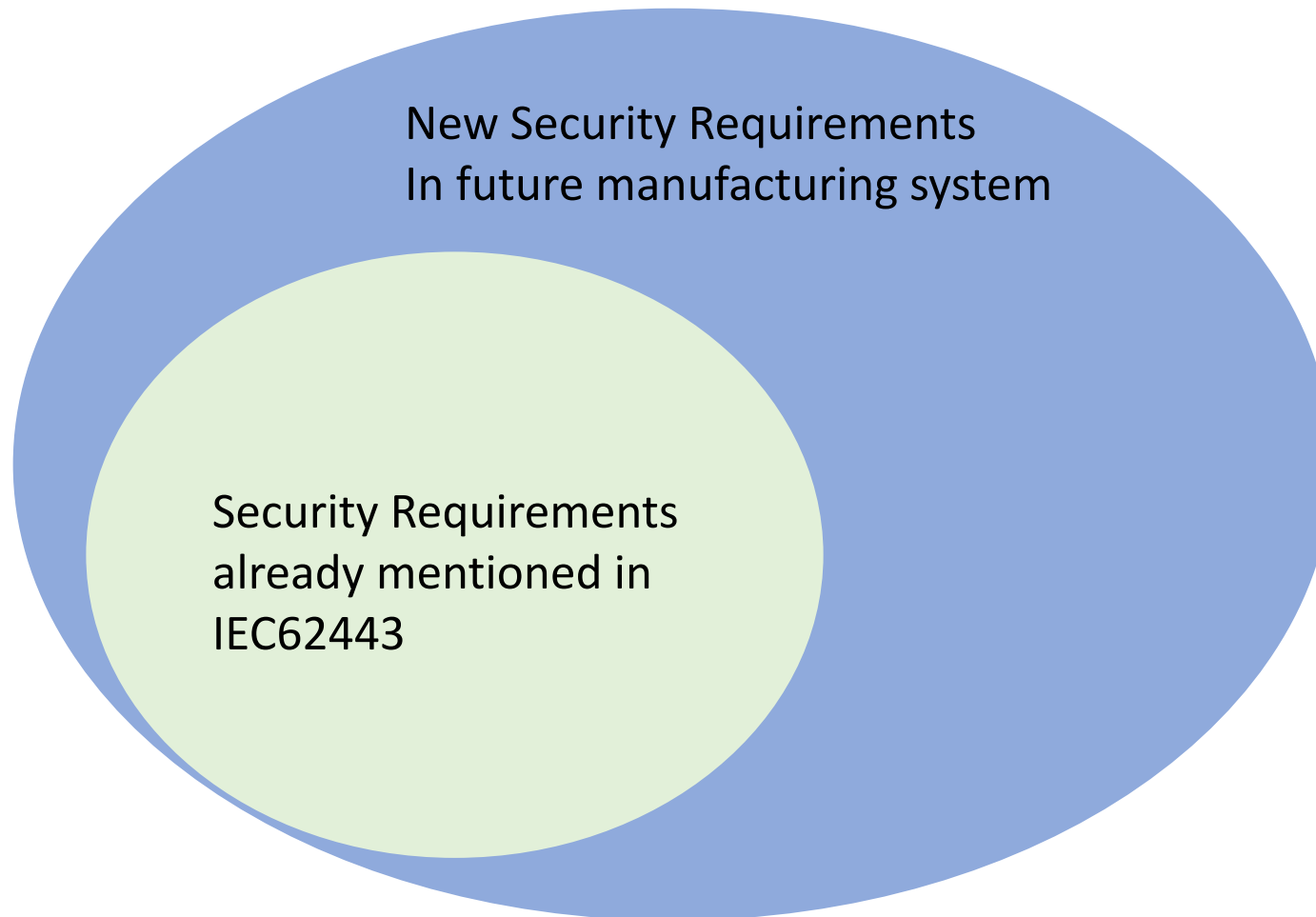


Industrial security Requirements

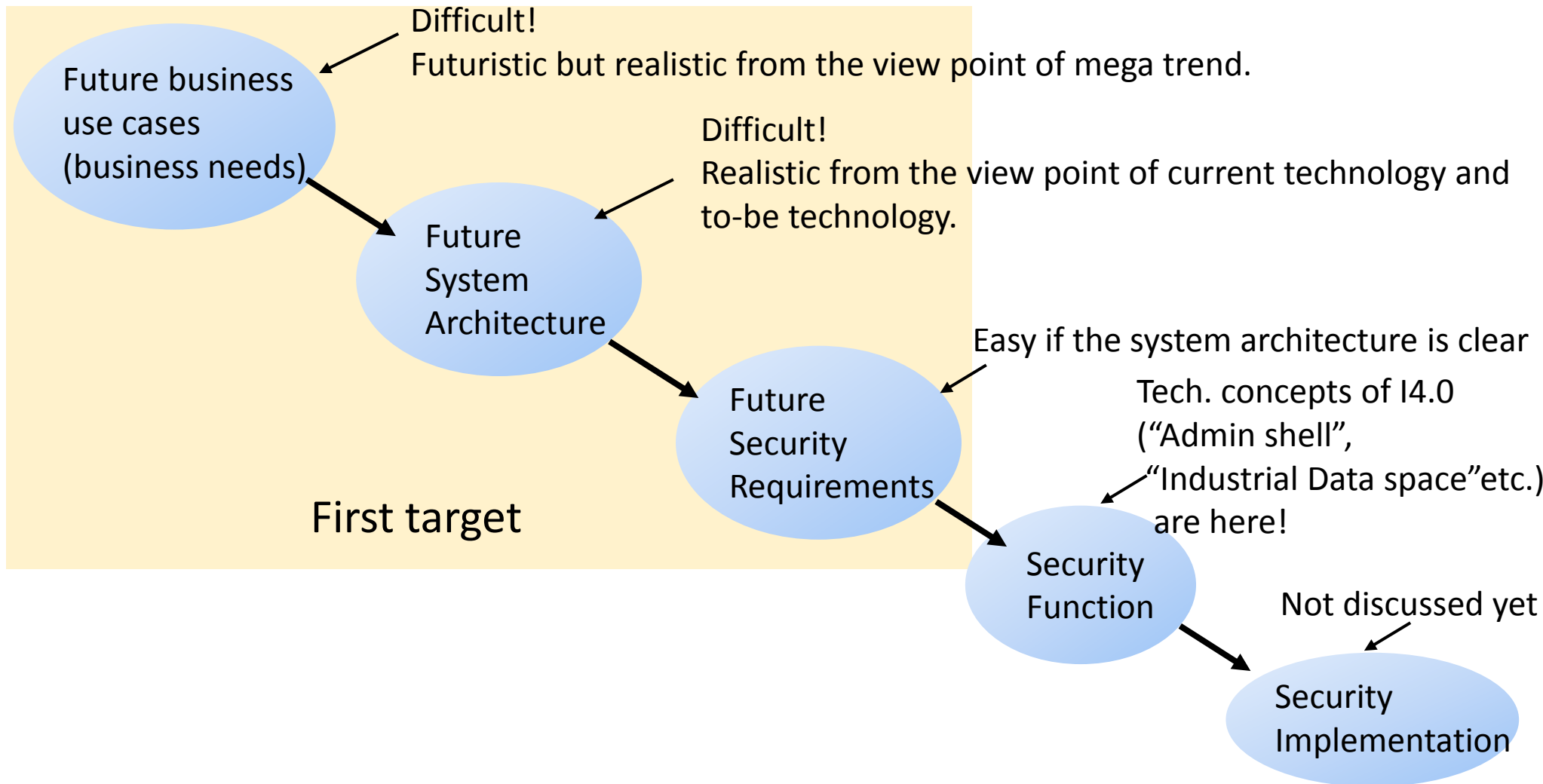
-extracted from discussion on a cross organization use case-

Industrial security AG, RRI

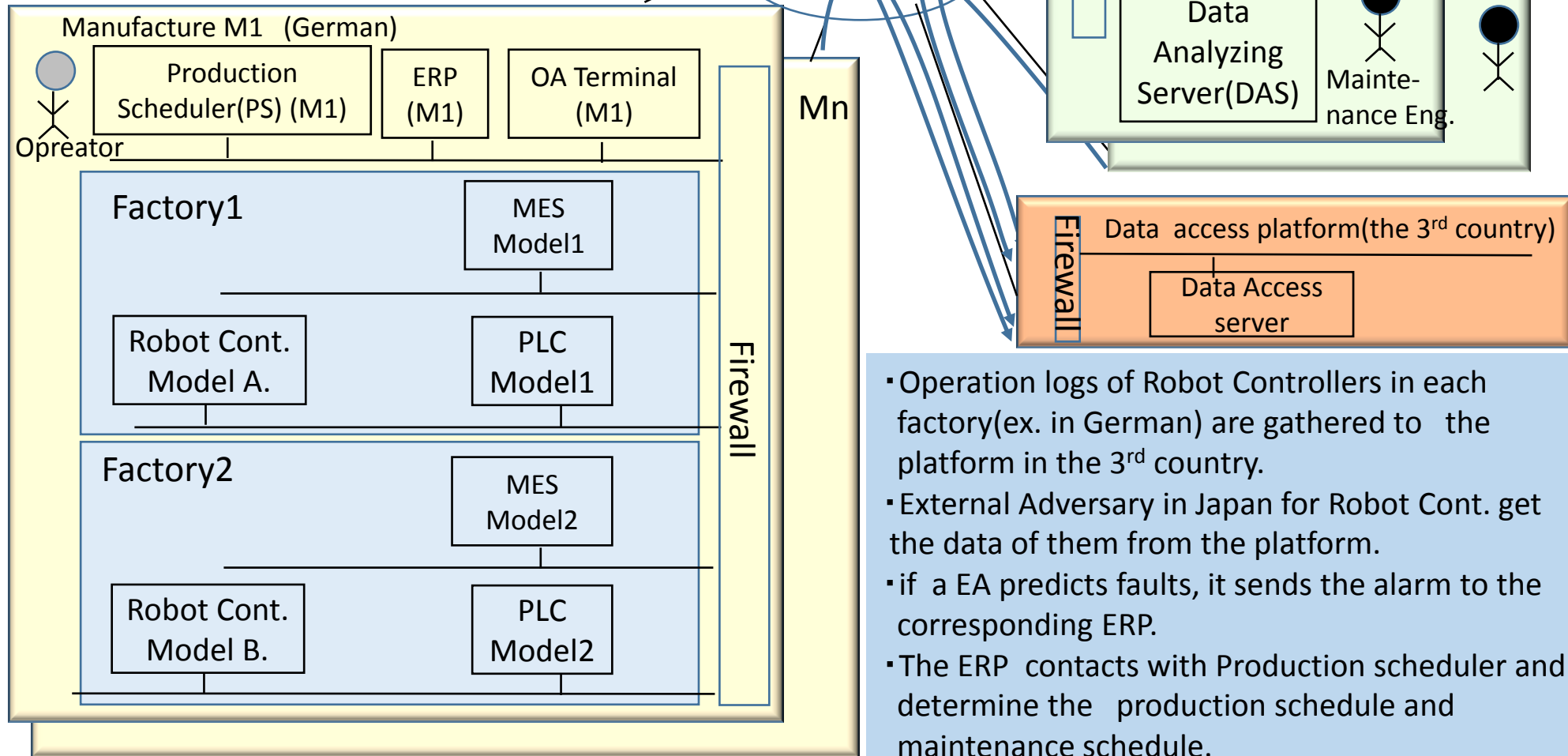
Our Goal: To identify new security requirements in future manufacturing systems of Industrie4.0



To identify new security requirements, we have to first identify and share future business use cases and their system architecture.



Operation states of each controller in factories are monitored through the Data Access Platform by External Advisors for early fault detection and recovery.



- Operation logs of Robot Controllers in each factory(ex. in German) are gathered to the platform in the 3rd country.
- External Adversary in Japan for Robot Cont. get the data of them from the platform.
- if a EA predicts faults, it sends the alarm to the corresponding ERP.
- The ERP contacts with Production scheduler and determine the production schedule and maintenance schedule.

Security requirements for the architecture

“Connected Industries”

New vision for the future of Japanese industries

“Global”, “dynamic” and “horizontal integration” could be the key to identify I4.0 specific security requirements. Red: I4.0 specific seq.req.candidates

System/network

- Unique IDs should be assigned to users to authenticate them
- Need to access policy” should be applied to system and network
- In order to adapt dynamic change of entities which need access to the system and network, automatic access control change mechanism should be introduced.
- Communications for inter-organization and inter-component should be protected.

Components

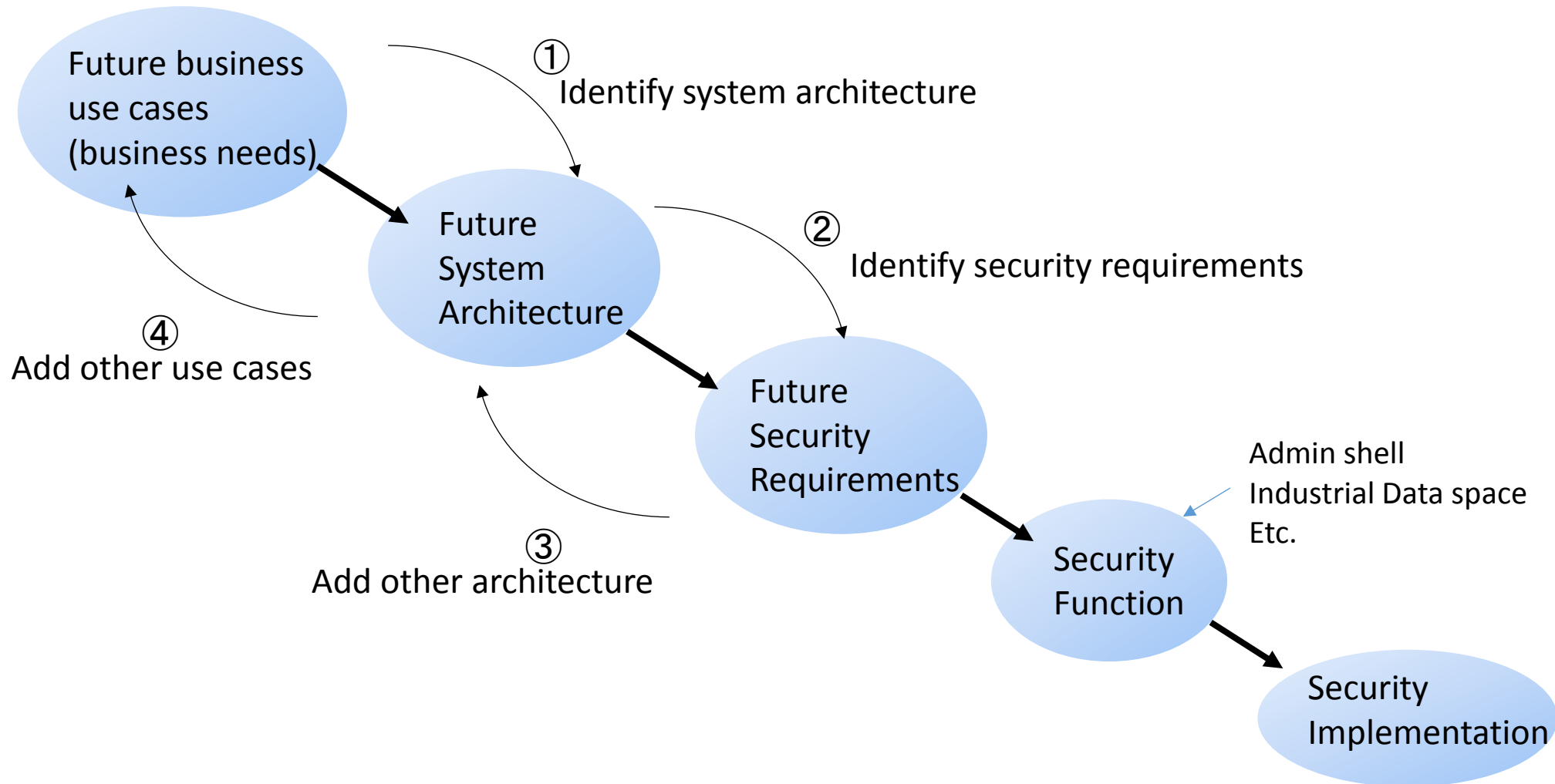
- Unique IDs are assigned for unified global access and identification.
- Access right for components should be “need to access” basis(ex. in a role based manner).
- “Who access to what components when” should be kept for audit and tracability.

Etc.(data)

- Personal information should be protected for complying with privacy regulation.

Future work

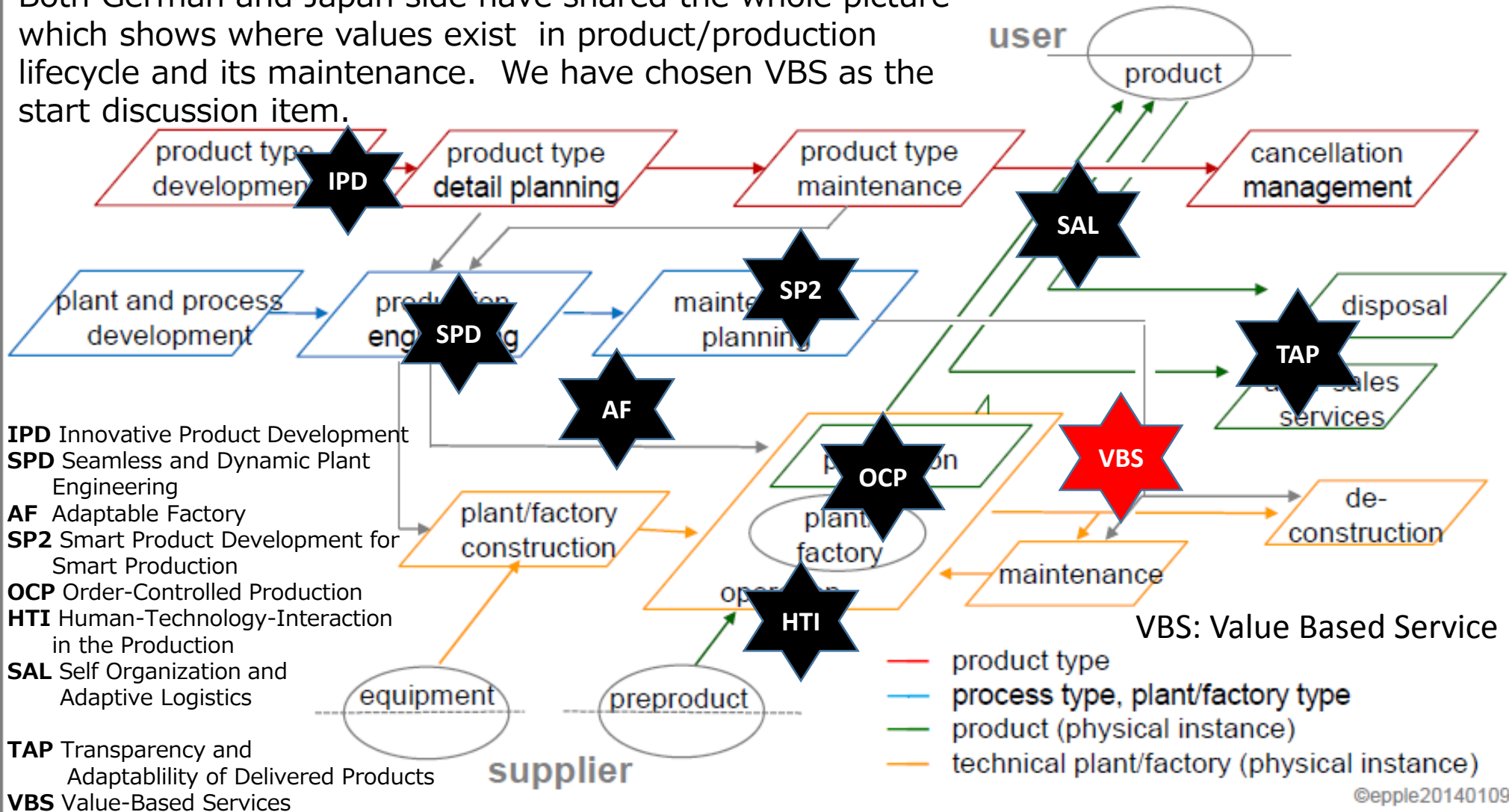
We are going to identify new security requirements though the process of ①②③④, and also to deeply understand Industrie4.0 Sec.Func. with the need of proper implementation.



Appendix

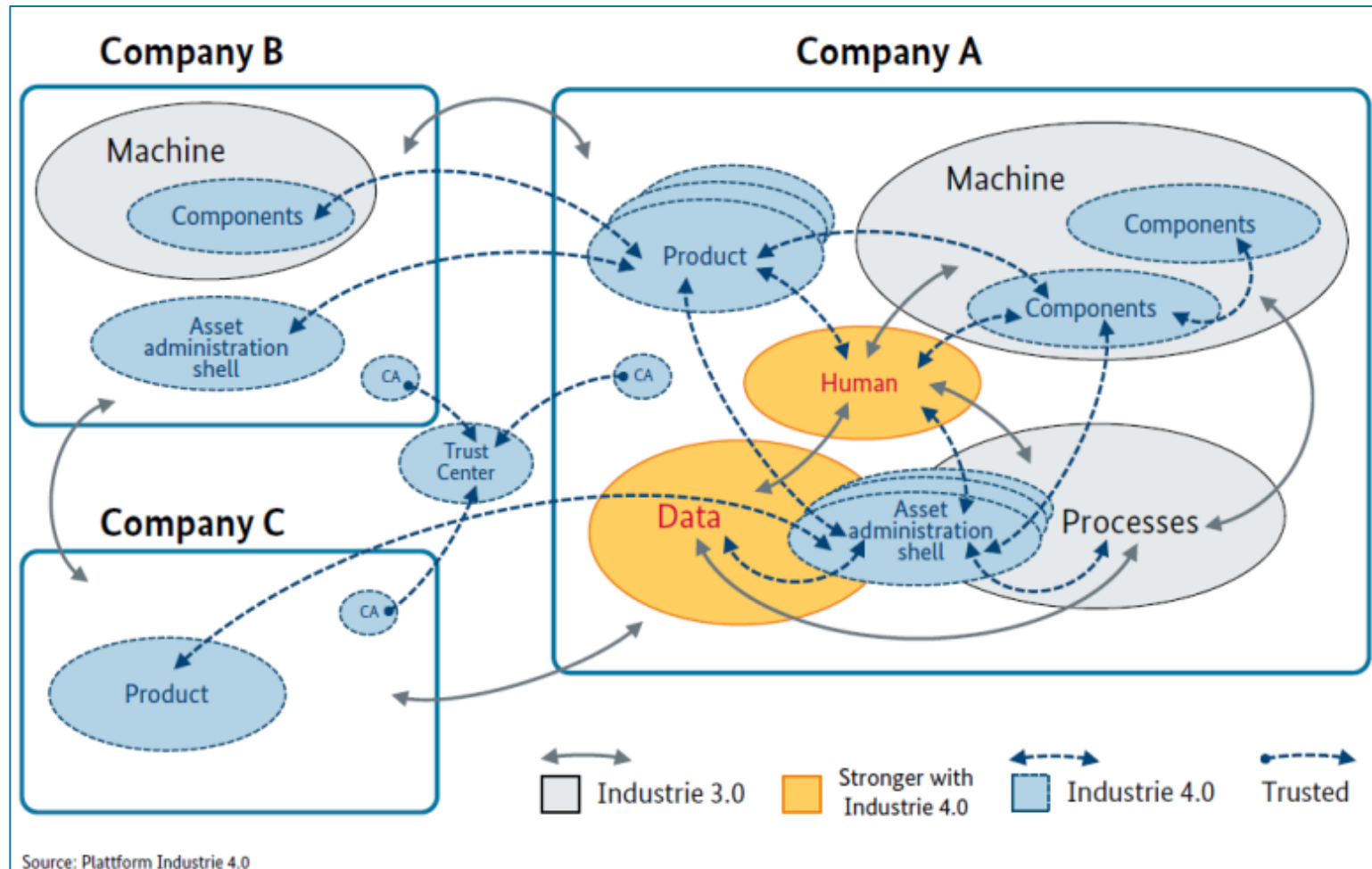
Business use case map (Where is our business use case?)

Both German and Japan side have shared the whole picture which shows where values exist in product/production lifecycle and its maintenance. We have chosen VBS as the start discussion item.



9

This figure shows how new kinds of interactions and trust are needed in industrie4.0
So that management can intuitively understand the security challenges in industrie4.0.



Admin shells applied for the system structure

Each component and server with “admin shell” could be join to I4.0 systems and interact with each other as a standardized I4.0 object.

