PLATTFORM INDUSTRIE 4.0

GUIDELINE


# Security in RAMI4.0

The many new opportunities that are opened up by *Industrie 4.0* also bring a host of different challenges. 'Security by design', for example, becomes an indispensable element in design within *Industrie 4.0*. In many cases, security will be the enabler of new business models.

Security acts as a skeleton that carries and holds together all of the structural elements within RAMI4.0 and, as a result, the design of the *Industrie 4.0* component. This paper seeks to provide the reader with a clear overview of the various security aspects within RAMI4.0. Various security measures are explored using a range of examples that are built upon on all three of the RAMI4.0 axes.

## RAMI4.0 – Reference architecture model for *Industrie 4.0*

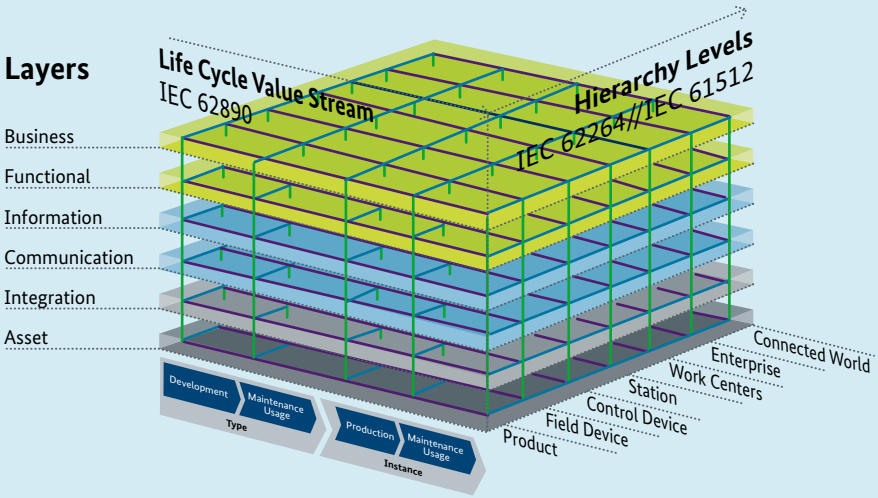
RAMI4.0 describes the key elements of an object/asset based upon the use of a structured layer model consisting of three axes[1]. This structure allows the relevant aspect of a particular asset to be shown at every point in time along its life cycle, thus allowing complex interrelationships to be broken down into smaller, clearer sections. The three axes are as follows:

- Architecture axis (layers) – made up of six different layers indicating the information depending the view to the asset;
- Process axis (value stream) – depicts the various stages within the life of an asset and the value creation process based on IEC 62890;
- Hierarchy axis (hierarchy levels) – assigns the functional models to individual levels based on DIN EN 62264-1 and DIN EN 61512-1.

### Reference architecture model for *Industrie 4.0*

**Layers:**
Security applies to all of the different levels. Risks must be considered for the object/asset as a whole.

**Value Stream:**
The owner of the object must consider security across its entire life-cycle.




**Hierarchy Levels:**
All objects/assets are subjected to security considerations (risk analysis) and need to possess or provide the relevant security characteristics for fulfilling their tasks/ providing protection.

Source: Plattform Industrie 4.0 and ZVEI

As can be seen from the figure, security is embedded within RAMI4.0 and has an integral nature within the model. It is not depicted as an individual layer or hierarchy level, but impacts upon the whole life-cycle within all layers and at all hierarchy levels. Like the use of steel for reinforcing a building, security ensures the stability of RAMI4.0 and protects against potential attacks.

## Hierarchy Levels

The hierarchy axis essentially maps the automation pyramid, depicting the various different components, the product, and the outside world (connected world). The type and extent of protection needed must be determined for both the individual elements, and for the system as a whole. In the first instance, this requires a risk analysis which includes a diagnosis of threats and potential. The results of this analysis will be the basis for the election of the security measures that are need to be undertaken in order to protect the individual *Industrie 4.0* component.

Let us take a machine (station) in a production or process environment (work unit) as an example. The machine must be able to process relevant materials correctly and without disruption. It must also be able to protect process logic against unauthorised changes, access or readouts.

Machine operators need to be able to identify themselves, giving rise to the need for an authorisation concept that enables various different types of intervention to be specified.

At the level of the production environment, the key task is to manage staff and the authorisation rights that have been granted and to manage a number of different machines, to transmit the relevant contracts securely, and to monitor which jobs have been completed.

## Value Stream

Security applies to the whole of the life-cycle which, in RAMI4.0, is represented by the process axis. This axis comprises the design stage, moving on to production, implementation, and usage and maintenance of the object/asset.

'Security by design' concerns all of the different actors involved – the manufacturer, the integrator, as well as the asset owner, in accordance with the type of responsibility held. While defining standards and developing components, security needs to be planned right from the very start and to be provided in line with needs. This applies to both technical and organisational measures (processes).

Right from the planning process, it is vital to factor in the security functions that are shown to be necessary based on risk analysis or requirements by other components. During the development and production process, a consistent method for avoiding errors must be used, e. g. following the Security Development Lifecycle (SDL) developed by Microsoft[2].

When using components and systems, not only existing security requirements need to be met, but any potential weaknesses in operation also need to be eliminated. Any updates that are required must be developed, passed on, and integrated on time.

1 Reference architecture model Industrie 4.0 (RAMI4.0). DIN SPEC 91345.

2 https://www.microsoft.com/en-us/sdl/

## Layers

While identifying security requirements, the six layers of the architecture axis enable various different aspects of an object/asset to be considered in a systematic manner. For example, this applies to the layers of communication and business as follows. By an analysis of the business models the relevant security threats and security requirements will be identified. Thus, at the communication layer, measures may be needed to encrypt data based on secure identities. For the decision which communication links have to be protected, e.g. by encryption, it must be clear, what information shall be transmitted via these links.

## Working together with others

Security plays a role at all points of intersection between the various levels. This means that requirements are derived for every point of intersection by a specific analysis. A solution must then be found for each of these requirements based on the relevant capabilities of the *Industrie 4.0* components involved in the specific application in question. Manufacturers, integrators, and asset owners are all called upon to implement a holistic security concept that brings technical and organisational measures together. Using RAMI4.0 as a basis for designing security enables every kind of security requirement to be implemented for any conceivable application.

As part of this process, RAMI4.0 enables existing security standards to be integrated, especially VDI/VDE 2182 and IEC 62443. The VDI/VDE 2182 standard addresses such issues as feedback on the requirements from the various actors that are part of the process. This standard describes communication between the manufacturer, integrator, and asset owner as a key element within security, thus enabling the relevant requirements to be passed on and implemented. IEC 62443 outlines a reference model for industrial communication networks and sets out how this can be used to raise security requirements and identify security technologies. Both VDI/VDE 2182 and IEC 62443 provide support for a holistic security concept which can be assessed by using 'protection levels'.

**AUTHORS:**

Michael Jochem, Robert Bosch GmbH | Wolfgang Klasen, Siemens AG | Lukas Linke, ZVEI | Lutz Jaenicke, Phoenix Contact Cybersecurity AG | Thomas Gamer, ABB AG | Mario Stolz, NXP Semiconductors Germany GmbH | Jens Mehrfeld, Bundesamt für Sicherheit in der Informationstechnik | Andreas Teuscher, Sick AG | Wolfgang Fritsche, IABG GmbH

## Imprint

**Published by**
Federal Ministry for Economic Affairs and Energy (BMWi)
Public Relations
11019 Berlin, Germany
www.bmwi.de

**Text and editing**
Plattform Industrie 4.0
Bertolt-Brecht-Platz 3
10117 Berlin

**Design and production**
PRpetuum GmbH, Munich

**Illustrations**
GKSD – Fotolia

**Status**
April 2016