OCORA

Open CCS On-board Reference Architecture

Guiding Principles

Main Executive and Design Principles

Document ID: OCORA-BWS03-020

Version: 2.01

Date: 10.06.2022

Revision history

Version	Change Description	Initial	Date of change
1.00	Official version for OCORA Delta Release	JH	30.06.2021
1.90	• Version for Coreteam Review	JH	29.11.2021
2.00	Official version for OCORA Release R1	PV	03.12.2021
2.01	Decoupled document from a specific OCORA release	RM	10.06.2022

Table of contents

Table of figures

References

Reader’s note: please be aware that the numbers in square brackets, e.g. [1], as per the list of referenced documents below, is used throughout this document to indicate the references to external documents. Wherever a reference to a TSI-CCS SUBSET is used, the SUBSET is referenced directly (e.g. SUBSET-026). OCORA always reference to the latest available official version of the SUBSET, unless indicated differently.

[1] OCORA-BWS01-010 – Release Notes

[2] OCORA-BWS01-020 – Glossary

[3] OCORA-BWS01-030 – Question and Answers

[4] OCORA-BWS01-040 – Feedback Form

[5] OCORA-BWS03-010 – Introduction to OCORA

[6] OCORA-BWS04-010 – Problem Statements

[7] OCORA-TWS01-030 – System Architecture

1 Introduction

1.1 Purpose of the document

OCORA has developed a comprehensive and coherent set of organisational, collaboration and design principles to provide guidance for the OCORA team in the planning and execution of the OCORA program portfolio, as well as for its interaction with its environment, primarily the railway community. OCORA publishes this set of principles not only as a guideline for its own activities, but also to inform stakeholders about what can be expected from OCORA and OCORA from members and avoid ambiguities on OCORA intentions. Therefore it is suggested to read this document together with the OCORA Introduction, ref. [5].

In this document two categories of leading principles are addressed:

1. Organisational and collaboration principles
2. Architecture design principles.

This document is addressed to experts in the CCS domain and to any other person, interested in the OCORA concepts for on-board CCS. The reader is invited to provide feedback to the OCORA collaboration and can, therefore, engage in shaping OCORA. Feedback to this document and to any other OCORA documentation can be given by using the feedback form [4].

If you are a railway undertaking, you may find useful information to compile tenders for OCORA compliant CCS building blocks, for tendering complete on-board CCS system, or also for on-board CCS replacements for functional upgrades or for life-cycle reasons.

If you are an organization interested in developing on-board CCS building blocks according to the OCORA standard, information provided in this document can be used as input for your development.

1.2 Applicability of the document

The document is currently informative. Subsequent releases of this document will be developed based on a modular and iterative approach, evolving within the progress of the OCORA collaboration.

1.3 Context of the document

This document is published as part of the OCORA Release, together with the documents listed in the release notes [1]. Before reading this document, it is recommended to read the Release Notes [1]. If you are interested in the context and the motivation that drives OCORA we recommend to read the Introduction to OCORA [5], and the Problem Statements [6]. The reader should also be aware of the Glossary [2] and the Question and Answers [3].

2 OCORA organization and collaboration principles

The OCORA collaboration is established primarily with the objective to transform the CCS market to achieve the economic and business interests of its founding members. OCORA is convinced that this is a necessary not only to support the drive for automation and digitalisation of the involved railways themselves, but that OCORA objectives also serve and benefit key institutional and industrial stakeholders.

OCORA acts according to key principles defined in the MoU and CoC on which the collaboration is based:

1. OCORA is first and foremost a technical collaboration platform for its members. OCORA output will be made available to any stakeholder of the railway community.

2. As expressed in the CoC, OCORA acts in full conformity with existing competition law under any circumstances and within the existing sectoral regulatory framework. Proposals formulated by OCORA, will e.g. be registered for further treatment through existing channels like CER or EUG.

3. Although OCORA aims at standardisation of the on-board CCS function, it does not envisage to set up a formal, “de iure” standard. However, OCORA will develop for its members and third parties, specifications for procurement purposes, following the examples of e.g. EULYNX.

4. Acknowledging that the sector has to be able to manage its legacy, currently available system versions (e.g. ERTMS B3) will as a matter of fact be the starting point for the migration towards the envisaged OCORA platform. The OCORA architecture intends to fulfil current TSI functional requirements to enable compatibility with the existing rolling stock and infrastructure configurations. Nevertheless, when configuring the migration process, OCORA intends to take due account of breakthrough concepts within (e.g. RCA) and out of the direct railway perspective (e.g. the automotive cyclical, concurrent engineering approach, allowing for cumulative, simultaneous product research and development cycles). Modularity on a system level (hardware, HW/SW interface, software applications, etc.) shall allow for a software based functional evolution under compatibility control. This approach will allow for a certain measure of stability for major parts of the system while at the same time allowing for rapid replacement or innovation of key elements thereof.

5. OCORA as an independent collaboration of railways, first of all seeks consensus between stakeholders and partners on the preferential way forward. But it is also aware of the need to remain in a position where it can articulate specific railway views. Therefore, OCORA intends to keep its autonomous position, despite or, rather, in support of ongoing developments, e.g. the establishment of Europe’s Rail JU. OCORA believes that to effectively impact relevant developments, it should remain independent while at the same time being deeply involved and supporting such developments. Autonomy will ensure the balanced, qualified and authentic contribution of railway points of view, opinions and expertise to important European programs and institutions.

6. OCORA believes that it needs to keep an open ear to the interests of other stakeholders in the railways community as a solid foundation for constructive and productive dialogue and discussion, and to keep a keen eye on opportunities to find joint solutions which satisfy the interests of the community as an integral whole and, as much as possible, of its individual members.

OCORA has developed and adheres to a number of leading principles in order to achieve its business objectives. These principles will guide any dialogue and collaboration with partners in the railway community:

1. **Openness**: OCORA is an open collaborative technical platform open to all railway companies. This includes IMs and RU's. It is based on sharing and making publicly available its deliverables for the benefit of the railway sector.
2. **Modularity**: OCORA intends to decompose the on-board CCS subsystem into an optimal c.f. reasonable number of standardized building blocks. System modularity is the basis for a modular safety approach and exchangeability, supporting different life cycles.
3. **Simplification**: OCORA intends to manage the exponentially increasing complexity of CCS systems by migrating from the current paper based to a model-based system engineering approach, allowing for a more systematic and concurrent requirement specification development process. Furthermore, OCORA plans to isolate in its architecture the functional blocks that will become obsolete in the foreseeable future (e.g. GSM-R, class B systems, current balise technology). This is the basis to easily simplify OCORA based implementations once the respective functions are not needed anymore.
4. **Independence**: OCORA intends to minimize the dependencies between different building blocks and components, such as dependencies between hardware, software and peripherals. This provides the basis for a modular product-based CCS system approach.
5. **Evolvability**: Recognizing that continuous updates and upgrades are paramount to the railway digitalization, OCORA intends to introduce secure upgradability and interchangeability to speed-up the integration of future innovations in a flexible manner and to provide a solid basis for introducing game changers such as FRMCS or ATO.

Both the corporate objectives themselves as well as the translation of those principles in architecture design principles, which provide the preconditions to achieve those objectives, are discussed in the next chapters.

3 OCORA architecture design principles

3.1 Context and coherence

Architecture design principles explain how and why system design enables RUs to achieve business objectives and, therefore, always have an economic rationale. They are not necessary to explain how or why a system works or performs, but how a system supports the corporate goals of its users[1].

CCS systems, especially ERTMS, have become important drivers for the life cycle costs of rolling stock, operational performance and transportation capabilities. Defining architecture design principles is of paramount importance to manage financial, operational and performance risks by design. This requires, foremost, providing the preconditions for effective life cycle management of the CCS system as part of the rail vehicle, allowing differentiation between systems or system elements with varying life expectancies. Additionally, building blocks with similar life cycle expectancy should be implemented as isolated objects or functions to allow effective maintenance, replacement, upgrading removal or adding new elements when these emerge. In other words: enable fast and cyclical adoption, migration and removal of key elements in sync with technology life cycles. Of course, there is always the question of the optimum level of granularity to which the monolith should be decomposed, but this, too, should primarily be a matter of economic reasoning rather than a technical discussion issue.

For the current generation of on-board CCS solutions, these requirements imply moving away from the current, monolithic CCS architectures that result in any (minor) change almost automatically affecting the integrated whole. The subsequent need to replace entire systems, repeated authorization processes and persistent complexity and performance issues, in the end damages the economic viability of both users and suppliers while it prevents early adoption of innovations and slows down the automation of railway processes.

OCORA architecture aims at breaking down the CCS on-board in independent building blocks that provide an optimum between economic value and technical feasibility. The following parameters influence the level of decomposition:

- Life cycle expenditure and revenues of the selected level of decomposition (meaning not only costs and benefits, because these not only pertain to financial drivers but also e.g. competitiveness, compliance with stakeholder or shareholder requirements and reputation);
- Building block life expectancy
- Building block performance requirements
- Physical location of building blocks in the vehicle
- Building block hardware requirements
- Procurement requirements, e.g. with respect to the desired level of complexity, planning issues or operational requirements

In economic terms: the upper limit of granularity, is the first level of decomposition where it is more cost effective to exchange single building blocks than to replace the monolithic system, they are part of. For example: if the total cost of ownership of a monolithic system exceeds that of the coherent and integrated whole of the sum of its independent building blocks, then the user should opt for decomposition of the system. And vice versa. This rule also applies to the question whether to further decompose single building blocks, defining the lower limits of decomposition. When it is e.g. more cost effective to replace a subsystem or component than to repair it, the lowest level of granularity is reached. When it is more cost effective to repair it, it is worthwhile to decompose it further since that will allow reaching the level of modularity needed for maintenance.

[1] See e.g.: Maier, Mark W. and Rechtin, Eberhardt. *The Art of Systems Architecting*, CRC Press, Inc. USA.

OCORA has defined a number of core architecture design principles pertaining to the breakdown and clustering of functional building blocks that are to be perceived as mutually related and dependant and can be both cause and effect of the others:

1. **Openness:** the property that design, contents, operation of a system and any information hereon is fully transparent and accessible to users and stakeholders.
2. **Modularity:** The property of being composed of a coherent whole of individual, independent building blocks, each of which can be separately treated as an independent, single and isolated entity necessary to make a system work. These could be concrete products or devices (such as 'functional vehicle adapter module') but also software and services (e.g. testing, insurance).
3. **Exchangeability**: The property that individual building blocks can be replaced without affecting the integrity of the whole system or of other building blocks. This property implies that provisions have been made regarding the connection between discrete building blocks which should enable the system to retain its integrity in case building blocks are replaced.
4. **Migrateability:** The property allowing to add or remove independent building blocks to the system or exchange existing building blocks by alternative ones, without compromising the integrity of the structural environment they are part of, and…
5. **Evolvability:** The property of enabling new technologies to be integrated into existing building blocks (or the mortar between them) while retaining at least the necessary functions of the integral system.
6. **Portability (Platform Independence):** the property to exchange software between systems. A good example is regular office software that can be installed and used on laptops from multiple manufacturers and using different operating systems (e.g. Windows and iOS), e.g. software.
7. **Security:** the property that a system cannot be used, or its correct functioning compromised by an unauthorized source.

These and supporting system architecture principles are further described and defined in the next paragraphs. Please take account of the fact that the system engineering principles, which sometimes at least in terminology overlap with system architecture principles, are dealt with in the architecture document [7].

3.2 Openness

As the most important principle for collaboration within OCORA, the concept of 'openness' certainly also pertains to the architectural level. Here, OCORA has adopted the interpretation of 'open' as proposed by the OSI DARTS open spectrum[2]. DARTS stands for data and information being discoverable, accessible, reusable, transparent and sustainable. These words indicate in short that information can be found, used, shared, easily understood, analysed, validated and verified and applied without the user being hampered by financial, legal, technical or ethical barriers or constraints.

3.3 Modularity

Modularity is expressed by the degree to which a system or computer program is composed of discrete building blocks. OCORA assumes that as a matter of design principles, its architecture must anticipate the need that a change made to one building block, has no impact on other building blocks or the communication layer connecting those building blocks. As per definition, modularity is one of the main drivers for maintainability, performance and capabilities and, therefore, expenditure and risk. OCORA aims at managing RU's financial, operational and performance risks through improved exchangeability.

In the OCORA context, modularity is defined as follows:

> Modularity is a prerequisite for having "plug and play"-like exchangeability of an on-board CCS system or its subsystems without the need to involve either the original supplier of the vehicle, of the CCS system or one of its subsystems.

[2] http://osiglobal.org/2018/11/15/osi-brief-what-do-we-mean-by-open/

While the main target of modularity for OCORA based systems is to achieve “plug & play”-like exchangeability as defined above, modularity brings along other advantages:

1. Life cycle orientation on building block level. Where now monolithic systems often need to be replaced while only specific components or subsystems have become (technologically or economically) obsolete, life cycle management enables decentralisation from a systems’ level to the single building blocks of the system. Life cycle costs of the CCS on-board system can be improved, since subsystems at the end of their life cycle can be replaced individually.
2. Decomposing a system into subsystems reduces the research and development effort needed to sustain the overall system, since it improves the possibility for parallel development and specialization of the different development teams. It prevents waste of scarce (financial and engineering) resources.
3. Decomposing a system reduces complexity during development and maintenance of the overall system. For example, single subsystems and components can be easily isolated, exchanged, or replaced for trouble shouting purposes. Testing and acceptance efforts can be concentrated on the respective subsystem. As a result, life-cycle costs and implementation time can be reduced.
4. If the interfaces of the subsystems are well-designed, introducing new functionality to the CCS on-board system is greatly simplified and the system can evolve rather than be replaced as a whole.
5. If safe functionality is encapsulated and separated from non-safe functionality, the likelihood of having the need to modify, test and accept safe subsystems decreases. At the same time, it increases the capability to easily introduce changes to non-safe subsystems.

Modularity not only comes with the advantages pointed out, but also has its downsides, e.g. a potential increase in integration testing effort when building the system for the first time in a situation where a reference implementation or at least an unambiguous specification is missing. Modularity with the purpose of having “plug and play”-like exchangeability as defined in the OCORA context (see red box), requires very detailed interface descriptions as well as harmonized requirement specifications (functional and non-functional) for all subsystems. Defining these interfaces and requirements to the level needed for the OCORA desired “plug and play”-like exchangeability, requires a substantial deployment of scarce human resources. Therefore, the granularity of the decomposition needs to be a result of a well-balanced analysis of the effort against the business needs (expected benefits). A relevant size for standardised building blocks is also essential to avoid that the workload to update interface specification will at the end become a new bottleneck for evolutions.

This modularity principle leads to an appropriate modular Safety process as well as a suitable Integration & Testing strategy (allowing to integrate, verify and validate the complete Onboard CCS subsystem and its external interfaces, in particular integration & testing shall allow to verify that the building blocks within the “CCS On-Board” support the whole functional scope of OCORA, for all grades of automation).

Therefore, modularity not only comes with the advantages pointed out, but also has its downsides, e.g. a potential increase in integration testing effort when building the system for the first time in a situation where a reference implementation or at least an unambiguous specification is missing. Modularity with the purpose of having “plug and play”-like exchangeability as defined in the OCORA context (see red box), requires very detailed interface descriptions as well as harmonized requirement specifications (functional and non-functional) for all subsystems. Defining these interfaces and requirements to the level needed for the OCORA desired “plug and play”-like exchangeability, requires a substantial deployment of scarce human resources. Therefore, the granularity of the decomposition needs to be a result of a well-balanced analysis of the effort against the business needs (expected benefits). A relevant size for standardised building blocks is also essential to avoid that the workload to update interface specification will at the end become a new bottleneck for evolutions.

3.4 Exchangeability (Interchangeability)

In the OCORA context, exchangeability is often also referred to as interchangeability. The OCORA definition for exchangeability is as follows:

> Exchangeability (Interchangeability) is the ability to replace one or multiple OCORA defined building blocks with (a) respective building block(s) of (an)other supplier(s), without affecting other building blocks of the train or the overall CCS on-board system.

Exchangeability (interchangeability) is an important driver for maintenance as it should allow OCORA defined building blocks to be fitted in various type of rolling stock (e.g. generic spare parts that are configured automatically when plugged in a specific train).

Exchangeability is also a prerequisite for structural changes that allow economies of scale, specifically for the migration of the CCS system in rail vehicles, Life expectancy of CCS systems and trains differ considerably, involving the cyclical exchange of the CCS system, even for new trains that are delivered including e.g. ERTMS.

At this moment, there is a huge variety of rolling stock types, each and every one requiring high risk and high cost specific design, engineering, prototyping, installation, testing and approval sequences. In other words: fleet size or rolling stock type volumes are a major cost and risk driver for all those involved. Which currently is a major argument fleet owners to avoid investments.

Decoupling the CCS system from the vehicle would hugely reduce implementation cost and investment risk. Of course, the first time the development cycle must be absolved to enable isolating the CCS from a harmonised vehicle interface, the Functional Vehicle Adapter. But every next retrofit would basically be a plug and play replacement of the CCS system on the harmonised train interface. This first step of achieving interoperability for CCS would not only reduce cost and investment risk, but also processing times and, therefore, the risk of obsolescence. Fleet size or vehicle type volume would cease to be a major issue for both fleet owners as well as the supply industry and could result in increased market volumes. And scarce resources that are now necessary for the safe integration process, could be allocated to other tasks, specifically fostering innovation.

3.5 Migrateability (Upgradeability)

In the OCORA context, the terms migrateability or upgradeability are often used as alternatives. The OCORA definition for migrateability is as follows:

> Migrateability (Upgradability) is the ability to introduce changes to one or multiple OCORA defined building blocks, without affecting other building blocks or the overall CCS on-board system.

Migrateability is best interpreted as the potentiality of existing technology solutions to integrate other or new solutions. As such, it supports the decoupling of building blocks with different life cycles. For example: in actual versions of the CCS system, bus systems are relatively stable and, in some cases, remain in use for decades. The same should apply to interfaces between building blocks, managing data exchange.

Specific applications or technologies have much shorter technology life cycles (specifically telecom equipment, e.g. chip sets). Basic CCS infrastructure solutions, therefore, should be resilient and scalable to the extent that shorter life cycle building blocks can be effectively isolated from other parts of the system which they are connected to via the basic layers. There should be no need to change anything on the interface connecting the affected building block to the bus system, the bus system itself, or any other building blocks of the system. And this at least during the life cycle of the longest lasting element of the connectivity layer.

3.6 Evolvability (Flexibility)

In the OCORA context, the words evolvability, evolutivity, and flexibility are often used as alternatives. The OCORA definition for Evolvability is as follows:

> Evolvability (Flexibility) is the ability to easily adopt to new technologies or to extend the functionality of an on-board CCS system without the involvement of the original supplier.

Evolvability primarily pertains to the ability to absorb and deploy ever evolving technology cycles or generations to execute a function or a specific configuration of system functions. As an example, a CCS on-board typically consists of elements with different life cycles, the most enduring being the bus system. Migrating from one generation bus system to the next, should be possible without compromising the integrity of the system. Likewise, building blocks should be isolated to the extent that it becomes immaterial who exchanges, in this example, the bus system.

OCORA is fully aware that this requirement of diachronical, persistent exchangeability and migrateability poses a challenge, not only to the supply industry but also to the users and the institutional environment. Regulatory and standards change management processes do not respect accelerating technology life cycles and accompanying life cycle management requirements. The TSI CCS backward compatibility requirement between ETCS baseline, for instance, may at first glance seem to protect user interests, but in the end proves to be an effective barrier for rapid migration and innovation, forcing suppliers to always respect effectively obsolete solutions and causing major investment, performance and reputation risks to users.

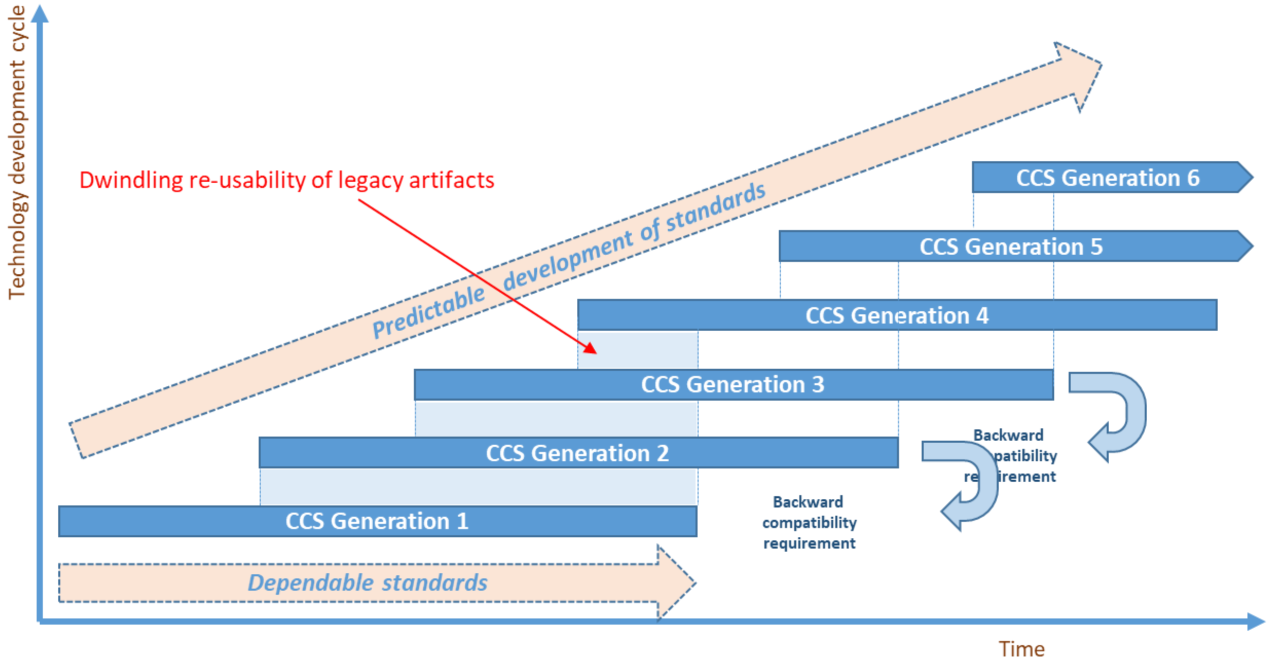

Figure 1 The technology and standards migration dilemma

To establish evolvability, close sector collaboration is necessary to get in charge of change and configuration management of both technology and standards developments. These should be brought in line, content wise and managerial. There will inevitably be an effect on both standards' development and on ownership. Instead of standards leading to product development (with inherent obsolescence as an inevitable consequence), OCORA believes the logical chain of action should become product development resulting in tested and proven standards. Whereby development cycles should be drastically decreased to allow for speedy adoption and absorption of state of art technology developments. This asks for different approaches towards standards management processes and shared ownership of the ensuing standards, driving harmonisation and interoperability. Only in case of shared sector responsibility for technology and standards development, evolvability will be achieved and European ambitions regarding an innovative, automated and digitalized rail network will materialize.

3.7 Portability (Platform Independence)

Portability is the degree of effectiveness and efficiency with which a system, product or component can be transferred from one hardware, software or other operational or usage environment to another. Portability is a main characteristic and includes the sub-characteristics: adaptability, installability, and replaceability (ISO 25010). Portability in the context of OCORA focuses on platform independence of functional applications: the fact of using a "generalized abstraction" (API) between the functional application logic and the underlying (Computing) Platform. The OCORA definition for portability is as follows:

> Portability (Platform Independence) is achieved when a functional application, based on the generalized abstraction, runs un-changed on different (computing) platform implementations. For this, the functional application shall only use external functions through a defined application programming interface (API).

3.8 Security (Cyber Security)

Security is the degree to which a product or system protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization. Security is a main characteristic and includes the sub-characteristics: confidentiality, integrity, non-repudiation, accountability, and authenticity (ISO 25010). In the OCORA context, the focus is on cyber security. Therefore, this term is often used to express this product characteristics. The OCORA definition for security is as follows:

> Security (Cyber Security) is the protection of (especially safety related communication and data used in) CCS on-board systems against threats (in particular cyber-attacks and hacks). To achieve this, all main security functionality like identify, protect, detect, respond and recover are considered.

3.9 Data communication design principles (OSI)

OCORA follows the OSI reference model for data communication design. The model provides the ‘mortar’ that enables modular exchangeability as referred to in paragraph 2.1.1. The OSI, or Open System Interconnection, model defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy[3]

Since OCORA applies the OSI reference model, the design principles applied are given here for reference purposes:

1. A layer should be created where a different level of abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity, and small enough that the architecture does not become unwieldy.

[3] Source: https://www.ukessays.com/essays/information-technology/explain-the-principle-of-network-osi-layers-information-technology-essay.php