

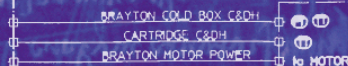
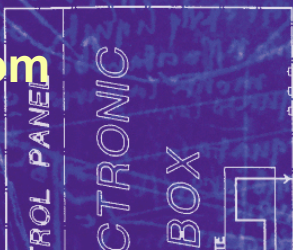
Engineering and Architecting
Multidisciplinary Systems
Volume 3

SYSTEMS ARCHITECTURE AND DESIGN

ALAIN FAISANDIER



Sinergy'Com



COLD BOX

Practical
Guidelines

spare machin

COPYRIGHT

Copyright © 2012 Sinergy'Com

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, scanning, or otherwise, without prior written permission of the publisher.

Permissions may be sought directly from publisher Sinergy'Com.

Sinergy'Com
2 chemin de la Serre
31450 BELBERAUD – France
Vox: +33561279861
sinergycom@mapsysteme.com

ISBN: 979-10-91699-00-6

FOREWORD

Purpose of this volume

This volume, dedicated to Systems Architecture and Design, is part of the series of books entitled “Engineering and Architecting Multidisciplinary Systems”.

This practical guideline is intended primarily for professionals who want to understand and apply daily engineering of systems, and in particular to those who will have to conceptualize and/or design complex or multidisciplinary systems. Here they will find methods, processes, modelling and analysis techniques, reasoning elements, useful recommendations for application, as well as case studies or examples to start using this approach.

Other people having to understand or to exchange with system architects and designers will find simple and concrete explanations. They will then be able to judiciously apply certain precepts and concepts to their own job. For example, they can be responsible for integration, verification and validation, program and project managers, technological study engineers, service developers, etc.

This guideline is most useful to University professors who desire teaching System Architecture Definition or Conceptualization, to university students, and to researchers, as a certain number of topics discussed in this book could possibly lead to more extensive studies, as well as studies which have not yet been tackled by the engineering community.

In this book, the approach used to present processes, activities, methods, and techniques related to systems architecture and design is gradual. It includes definitions, descriptions, discussions; examples and case studies illustrate practices. The case studies explain step by step how to perform the activities and tasks. Readers can directly transpose the step-by-step and use provided templates for their current or future projects.

Content abstract

The present volume contains what is necessary to know for defining the architecture of a system and for designing the system:

- ◆ Fundamentals related to the notion of system architecture and system design
- ◆ Principles and approaches related to Logical and Physical Architecture Definition processes, activities, and tasks
- ◆ The transition from System Requirements to Architecture Definition
- ◆ Basic Constructs for modelling a logical architecture
- ◆ Some system functional and behavioural patterns often encountered with industrial and service systems
- ◆ The description and definition of major system Architectural Characteristics and associated Design Properties
- ◆ The separation between Architecture Definition processes and System Elements Design process, and their relationships
- ◆ Some applicable methods, modelling techniques, architecture and design considerations, and their utilisation on examples and case studies
- ◆ Some pitfalls, proven practices, recommendations and Frequently Asked Questions

CONTENT

FOREWORD	1
1 INTRODUCTION	15
2 TERMINOLOGY	17
2.1 Terms and definitions	17
2.2 Abbreviations	21
3 REMINDERS ABOUT FUNDAMENTALS OF SYSTEM DEFINITION	23
3.1 Introduction	24
3.2 Top-down and bottom-up engineering approaches	29
3.2.1 Top-down approach: from the problem to the solution	29
3.2.2 Bottom up approach and evolution of the solution	29
3.2.3 Mixed approach	29
3.3 Engineering approaches supported by ontology elements	31
4 GENERAL PRINCIPLES AND CONCEPTS RELATED TO SYSTEM ARCHITECTURE AND SYSTEM DESIGN	35
4.1 Definition of System Architecture and of System Design	36
4.1.1 System Architecture	36
4.1.2 System Design	37
4.2 Approach to System Architecture and Design	39
4.2.1 Simplified categorisation of structural domains	39
4.2.2 Purpose of System Architecture and Design	40
4.2.3 Properties, characteristics and goals	40
4.2.4 Transition from System Requirements to Physical Architecture	41
4.2.5 Iterations between Logical and Physical Architectures Definition	42
4.2.6 Re-use of System Elements and Reverse Engineering	43
4.3 General concepts related to System Architecture and Design	45
4.3.1 System Breakdown Structure and Product Breakdown Structure	45
4.3.2 Projection of System Architecture onto implementation technologies	48
4.3.3 System Architecture and technological Architectures	49
4.3.4 Concept of Interface	50
4.4 Intellectual creation principles	51
5 SYSTEM LOGICAL ARCHITECTURE DEFINITION	53
5.1 Introduction, definitions and purpose	54
5.2 Concepts related to System Logical Architecture Definition	55
5.2.1 Functional Architecture concepts	55
5.2.2 Behavioural Architecture concepts	60
5.2.3 Temporal Architecture concepts	71
5.2.4 Integration of functional, behavioural and temporal views	74
5.3 Approach and principles to define Logical Architectures	77
5.3.1 Where to find and how to define Functions and Input-output Flows?	77
5.3.2 How to define a candidate Logical Architecture?	80
5.3.3 Utilisation of Behavioural Constructs and Patterns	84
5.4 Process approach – What to do?	86
5.4.1 Location of the process in the development cycle	86
5.4.2 Purpose of the process, inputs and outputs	86
5.4.3 Activities of the process	87
5.4.4 Ontology elements	92
5.4.5 Verification and validation of Logical Architecture Definition	94
5.4.6 Documentation templates	94
5.5 Practice – How to do?	95
5.5.1 Which language to use with architecture and design?	95

5.5.2	Methods and modelling techniques	96
5.5.3	Practical considerations	106
5.5.4	Frequently Asked Questions	107
6	SYSTEM PHYSICAL ARCHITECTURE DEFINITION	109
6.1	Introduction, definition and purpose	110
6.2	Concepts related to System Physical Architecture Definition	111
6.2.1	System Element, Physical Interface, Port	111
6.2.2	From Architectural Characteristics to Design Properties	117
6.2.3	Emergent properties	123
6.3	Approach and principles for defining Physical Architectures	125
6.3.1	Allocation and partitioning principles	125
6.3.2	Physical Interface focalisation	132
6.3.3	Principles for defining candidate Physical Architectures	135
6.3.4	Selecting the preferred candidate Physical Architecture	139
6.4	Systems and System Elements Acquisition	141
6.5	Systems of Systems Architecting	143
6.6	System Architect and Designers challenges; fields of choice	144
6.7	Process approach – What to do?	146
6.7.1	Location of the process in the development cycle	146
6.7.2	Purpose of the process, inputs and outputs	146
6.7.3	Activities of the process	147
6.7.4	Ontology elements	153
6.7.5	Verification and Validation of Physical Architecture Definition	156
6.7.6	Documentation templates	156
6.8	Practice – How to do?	158
6.8.1	Methods and modelling techniques	158
6.8.2	Architectural Frameworks - abstract	160
6.8.3	Practical considerations	162
6.8.4	Frequently Asked Questions	165
7	SYSTEM DESIGN AND SYSTEM ELEMENT DESIGN	167
7.1	Introduction, definition and purpose	168
7.2	Principles and concepts related to System Design	169
7.2.1	One System and several Implementations	169
7.2.2	System Element Detailed Design Characteristics	170
7.2.3	Concept of Design Descriptor	171
7.3	Process approach	172
7.3.1	Introduction	172
7.3.2	Location of the process in the development cycle of a system	172
7.3.3	Purpose of the process, inputs and outputs	173
7.3.4	Activities of the process	174
7.3.5	Ontology elements	176
8	SOME REFERENCES	179
9	CASE STUDIES	181
9.1	Case study 1 - Tank filling	182
9.1.1	Exercises	182
9.2	Case study 2 - SIBERIA	205
9.2.1	Inputs: SIBERIA System Requirements	205
9.2.2	Exercises Nr 1: Logical Architecture Definition	207
9.2.3	Exercises Nr 2: Physical Architecture Definition	210
9.2.4	Solutions of exercises Nr 1 - SIBERIA: Logical Architecture Definition	212
9.2.5	Solutions of exercises Nr 2 - SIBERIA: Physical Architecture Definition	229
9.3	Case study 3 – FITVEE	243
9.3.1	Inputs: FITVEE System Requirements	243

9.3.2	Exercises Nr 1: Logical Architecture Definition	245
9.3.3	Exercises Nr 2: Physical Architecture Definition	248
9.3.4	Solutions of exercises Nr 1 - FITVEE: Logical Architecture Definition	250
9.3.5	Solutions of exercises Nr 2 - FITVEE: Physical Architecture Definition	261
10	ANNEXE 1 – GENERIC BEHAVIOURAL CONSTRUCTS	287
10.1	Construct: Sequence	288
10.2	Construct: Concurrency	289
10.3	Construct: Selection (alternative)	291
10.4	Construct: Iteration	293
10.5	Construct: Multiple exits	294
10.6	Construct: Loop with exit	296
10.7	Construct: Replication without monitoring	298
10.8	Construct: Replication with monitoring	299
11	ANNEX 2 – BEHAVIOURAL PATTERNS EXAMPLES	301
11.1	Pattern: Sequence of functions	302
11.2	Pattern: Parallelism of functions through allocation	303
11.3	Pattern: Monitor performance of an operation	305
11.4	Pattern: Send and receive a message	307
11.5	Pattern: Man Machine Interface (MMI)	309
11.6	Pattern: Mutual exchanges	311
11.7	Pattern: Monitor transitions of operational modes	313
11.8	Pattern: Real time monitoring of processes	315
11.9	Pattern: Process threats	317
11.10	Pattern: Queue management	318
11.11	Pattern: Production - consumption	320
11.12	Pattern: Control-command (simple)	322
11.13	Pattern: Supervised control-command	328
12	ANNEX 3 – DEFINITION OF SYSTEM LIFE CYCLE ABILITIES	330
13	ANNEX 4 – DEFINITION OF ARCHITECTURAL CHARACTERISTICS	332
14	ANNEX 5 – DEFINITION OF DESIGN PROPERTIES	334
15	ANNEX 6 - EXAMPLES OF ENVIRONMENT ARCHITECTURAL CHARACTERISTICS	337
16	ANNEX 7 - SYSTEM DESIGN DOCUMENT - TEMPLATE & GUIDELINES	339
17	ANNEX 8 - SYSTEM JUSTIFICATION DOCUMENT - TEMPLATE & GUIDELINES	349

3 REMINDERS ABOUT FUNDAMENTALS OF SYSTEM DEFINITION

This chapter provides necessary fundamentals to know about System Definition before reading and studying concepts, principles, approaches and processes dedicated to systems architecture and design. You will find only reminders about those fundamentals here; they are detailed in other volumes: in volume 1 “System Notion and Engineering of Systems” for general approaches, and in volume 2 “Systems Opportunities and Requirements” for requirements definition.

Following subjects are summarized hereafter:

- ◆ The notion of life cycle processes and the notion of system – section 3.1
- ◆ The top-down and bottom-up engineering approaches – section 3.2
- ◆ How these engineering approaches are supported by system development ontology elements – section 3.3

4 GENERAL PRINCIPLES AND CONCEPTS RELATED TO SYSTEM ARCHITECTURE AND SYSTEM DESIGN

You will find in this chapter definitions, principles and concepts related to System Architecture and System Design as well as interesting discussions concerning these subjects.

- ◆ Definition of System Architecture and of System Design – section 4.1
- ◆ Approach to System Architecture and Design – section 4.2, including:
 - Simplified categorisation of structural domains – section 4.2.1
 - Purpose of System Architecture and Design – section 4.2.2
 - Properties, characteristics and goals – section 4.2.3
 - Transition from System Requirements to Physical Architecture – section 4.2.4
 - Iterations between Logical and Physical Definition – section 4.2.5
 - Re-use of System Elements and Reverse Engineering – section 4.2.6
- ◆ General concepts related to System Architecture and Design – section 4.3, including:
 - System Breakdown Structure and Product Breakdown Structure – section 4.3.1
 - Projection of System Architecture onto realisation technologies – section 4.3.2
 - System Architecture and technological Architectures – section 4.3.3
 - Concept of Interface – section 4.3.4
- ◆ Intellectual creation principles – section 4.4

5 SYSTEM LOGICAL ARCHITECTURE DEFINITION

This chapter deals with specific concepts and principles related to System Logical Architecture Definition, and provides *What to do* (the activities and detailed tasks of the process), and *How to do* (concepts, approaches, modelling techniques and practical considerations). Are described and discussed:

- ◆ Definitions and purpose of this topic – section 5.1
- ◆ Concepts related to System Logical Architecture Definition - section 5.2, including:
 - Functional Architecture concepts: Functions and Input-output Flow, Functional Hierarchy, Control flow and Trigger
 - Behavioural Architecture concepts: Scenario of Functions, Operational Mode, Transition of Modes
 - Temporal Architecture concepts: Synchronous and asynchronous Functions, Temporal hierarchy levels, Temporal Analysis
 - Integration of functional, behavioural and temporal views: Systemic grid
- ◆ Approach and principles to define Logical Architectures – section 5.3, including:
 - Where to find and how to define Functions and Input-output Flows?
 - How to define Logical candidate Architectures?
 - Utilisation of Behavioural Constructs and Patterns
- ◆ Process approach – What to do? – section 5.4, including:
 - Location of the process in the development cycle
 - Purpose of the process, inputs and outputs
 - Activities of the process
 - Ontology elements
 - Verification and validation of Logical Architecture Definition
 - Documentation templates
- ◆ Practice – How to do? – section 5.5, including:
 - Which language to use with design and architecture?
 - Methods and modelling techniques: mainly Functional Flow Block Diagram, and SysML Activity Diagram, Utilisation of behavioural constructs to model scenarios
 - Practical considerations: Pitfalls and Proven Practices, Our strongest Recommendations, Frequently Asked Questions

6 SYSTEM PHYSICAL ARCHITECTURE DEFINITION

This chapter deals with specific concepts and principles related to System Physical Architecture Definition, and provides *What to do* (the activities and detailed tasks of the process), and *How to do* (concepts, approaches, modelling techniques and practical considerations). Are described and discussed:

- ◆ Definitions and purpose of this topic – section 6.1
- ◆ Concepts related to System Physical Architecture Definition – section 6.2, including:
 - Notions of System Element, Physical Interface, Port, Physical Architecture
 - System life cycle Abilities, Architectural Characteristics and Design Properties
 - Emergent Properties
- ◆ Approach and principles for defining Physical Architectures – section 6.3, including:
 - Allocation and partitioning principles
 - Physical Interface focalisation
 - Principles for defining candidate Physical Architectures
 - Selecting the preferred candidate Physical Architecture
- ◆ System Elements Definition and Acquisition – section 6.4
- ◆ Systems of Systems Architecting – section 6.5
- ◆ System Architect and Designer challenges; fields of choice – section 6.6
- ◆ Process approach – What to do? – section 6.7, including:
 - Location of the process in the development cycle
 - Purpose of the process, inputs and outputs
 - Activities of the process
 - Ontology elements
 - Verification and validation of Physical Architecture Definition
 - Documentation templates
- ◆ Practice – How to do? – section 6.8, including:
 - Methods and modelling techniques: mainly Physical Block Diagram, and SysML Blocks
 - An abstract about Architectural Frameworks
 - Practical considerations: Pitfalls and Proven Practices, Recommendations, Frequently Asked Questions

7 SYSTEM DESIGN AND SYSTEM ELEMENT DESIGN

This chapter deals with general concepts and principles related to System Design and System Elements design, and provides the generic activities and tasks of the corresponding process.

Are described and discussed:

- ◆ Definitions and purpose of this topic – section 7.1
- ◆ Principles and concepts related to System Element Design – section 7.2
- ◆ Process approach – section 7.3, including:
 - Location of the process in the development cycle
 - Purpose of the process, inputs and outputs
 - Activities of the process
 - Ontology elements discussion

8 SOME REFERENCES

Some references cited or used in this volume are listed below. The reader can read some of the following books and documents related to the subject of the present volume.

Books in English:

- ◆ [ALE 77] Alexander, Christopher; Sara Ishikawa, Murray Silverstein, Max Jacobson, Ingrid Fiksdahl-King, Shlomo Angel. 1977. A Pattern Language: Towns, Buildings, Construction. New York: Oxford University Press.
- ◆ [CHE 99] Checkland, P. B. 1999. Systems Thinking, Systems Practice. Chichester, UK: John Wiley & Sons Ltd.
- ◆ [CHS 65] Chestnut, Harold. 1965. Systems Engineering Methods. New York: Wiley & Sons.
- ◆ [CHS 65] Chestnut, Harold. 1965. Systems Engineering Tools. New York: Wiley & Sons.
- ◆ [FRI 11] Friedenthal, Sandford; Moore, Alan; Steiner, Rick. 2011. A Practical Guide to SysML. Morgan Kaufmann Publishers. Burlington, MA: Elsevier.
- ◆ [GAM 95] Gamma, Erich; Richard Helm, Ralph Johnson, and John Vlissides. 1995. Design Patterns: Elements of Reusable Object-Oriented Software. Addison-Wesley.
- ◆ [LAW 10] Lawson Harold.2010. Systems Thinking and Systems Engineering series. Volume 1, A Journey Through the Systems Landscape. King's College London, UK. College Publications.
- ◆ [LUZ 11] Luzeaux Dominique; Ruault Jean-René; Wippler Jean-Luc. 2011. Large-scale Complex System and Systems of Systems: Case Studies. London, UK: ISTE; Hoboken, NJ, USA: Wiley.
- ◆ [MAI 09] Maier, M., and E. Rechtin. 2009. The art of systems architecting. 3rd ed. Boca Raton, FL, USA: CRC Press.
- ◆ [OLI 95] Oliver, D., T. Kelliher, and J. Keegan. 1997. Engineering complex systems with models and objects. New York, NY: McGraw-Hill.
- ◆ [THO 93] Thome, B. 1993. Systems engineering, principles & practice of computer-based systems engineering. New York, NY: Wiley.
- ◆ [VIT 60] Vitruvius. 1960. De Architectura. The ten books on architecture (transl. Morris Hicky Morgan, 1960). Dover, NY: Courier Dover Publications.
- ◆ [VIT 99] Vitruvius. 1999. Ten Books on Architecture, translated by Ingrid D. Rowland. Cambridge University Press.

Standards:

- ◆ [ISO 08] Systems and software engineering - system life cycle processes. Geneva, Switzerland: International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 15288:2008.
- ◆ [OMG 10] OMG Systems Modeling Language – specification - version 1.2 – July 2010 - http://www.omg.org/technology/documents/spec_catalog.htm
- ◆ MOD Architecture Framework, UK MOD, version 1.2.004 available from UK MOD at <http://www.mod.uk/DefenceInternet/AboutDefence/WhatWeDo/InformationManagement/MO DAF/>
- ◆ DOD Architecture Framework, DOD, version 2.02 available from US DOD at <http://cio-nii.defense.gov/sites/dodaf20/>

Handbooks:

- ◆ [INC 11] INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities". 2011. San Diego, CA, USA: International Council on Systems Engineering (INCOSE), INCOSE-TP-2003-002-03.2.1.
- ◆ [NAS 07] NASA. 2007. Systems engineering handbook. Washington, D.C.: National Aeronautics and Space Administration (NASA), NASA/SP-2007-6105.
- ◆ [SEB 12] Guide to the Systems Engineering Body of Knowledge – version 1 – 2012 – <http://www.sebokwiki.org>

Books in French:

- ◆ [MEI 98] Meinadier Jean-Pierre. 1998. Ingénierie et intégration des systèmes. Paris: Hermes.
- ◆ [MEI 02] Meinadier Jean-Pierre. 2002. Le metier d'intégration des systèmes. Paris: Hermes-Lavoisier.
- ◆ [PEN 97] Penalva Jean-Michel. 1997. La modélisation par les systèmes en situation complexe. Thèse Université. Paris XI Orsay.
- ◆ [ROQ 09] Roques, Pascal. 2009. SysML par l'exemple. Paris: Eyrolles.

9 CASE STUDIES

Case studies are presented in the form of exercises. The reader is invited to do the exercises using material included in the previous chapters. Elements of solutions are provided afterwards. The exercises have the goal to illustrate what should be done and how to obtain progressively the outcomes of the engineering activities. The goal is not to provide here complete solutions.

Three case studies are treated:

- ◆ Case study 1 – Tank filling, section 9.1
 - This case figures out how logical and physical definition activities are supported by appropriate modelling techniques;
 - As a starting example, few activities of the processes are illustrated.
- ◆ Case study 2 – SIBERIA, section 9.2
 - This case provides guidance about the progression of the definition using major activities and tasks of the processes.
 - In particular several behavioural patterns are used with eFFBD and SysML Activity Diagrams.
 - Two physical architectures are defined.
- ◆ Case study 3 – FITVEE, section 9.3
 - This case provides also guidance about the progression, using the same guidance template than the previous one. Tasks, models and considerations about the allocated logical architecture are added.
 - Other behavioural patterns are used with eFFBD and SysML Activity Diagrams.
 - Also two physical architectures are defined and their structures are discussed.

10 ANNEXE 1 – GENERIC BEHAVIOURAL CONSTRUCTS

The following representations illustrate the Generic Behavioural **Constructs** and the result of their execution in the form of a timeline as a system architect or designer could expect it.

Two modelling techniques are used to represent these Constructs: Functional Flow Block Diagrams (FFBD) and Activity Diagrams of SysML (AD).

FFBD constructs are using the graphs theory principles; the set of constructs constitutes a "well structured language" mathematically speaking. Timelines have been obtained through the execution of FFBD models.

Activity Diagrams of SysML include simpler and more basic idioms – refer to SysML OMG specification for complete descriptions. As SysML is more a natural language than a formal one (authors said), models presented here are interpretations from the author; other presentations could be acceptable.

The following figures present main generic constructs useful at system engineering level. To understand the figures below you should read before part of sections 5.5.2.2 and 5.5.2.3.

List of constructs:

- ◆ Sequence – section 10.1
- ◆ Concurrency – section 10.2
- ◆ Alternative (selection) – section 10.3
- ◆ Iteration – section 10.4
- ◆ Multiple exits – section 10.5
- ◆ Loop with exit – section 10.6
- ◆ Replication without monitoring – section 10.7
- ◆ Replication with monitoring – section 10.8

11 ANNEX 2 – BEHAVIOURAL PATTERNS EXAMPLES

This annex presents some examples of general functional / behavioural patterns:

- ◆ Sequence of functions – section 11.1
- ◆ Parallelism of functions through allocation – section 11.2
- ◆ Monitor performance of an operation – section 11.3
- ◆ Send and receive a message – section 11.4
- ◆ Man Machine Interface (MMI) – section 11.5
- ◆ Mutual exchanges – section 11.6
- ◆ Monitor transitions of operational modes – section 11.7
- ◆ Real time monitoring of processes – section 11.8
- ◆ Process threats – section 11.9
- ◆ Queue management – section 11.10
- ◆ Production – consumption – section 11.11
- ◆ Control-command (simple) – section 11.12
- ◆ Supervised control-command – section 11.13

16 ANNEX 7 - SYSTEM DESIGN DOCUMENT - TEMPLATE & GUIDELINES

Preliminary

This template is a form to use and fill in for producing the document related to a specific system in the context of a development project.

The "System Design Document" (SysDD) presents the outcomes generated by the performance of the System Logical Architecture Definition Process and of the System Physical Architecture Definition Process.

It contains the selected solution in terms of Logical views of the Architecture of the system XX (functional, behavioural, and temporal architectures or views) and of Physical views of the Architecture of the system XX.

It does not present the justification and rationale of the selected solution; these elements are described in the System Justification Document – refer to the corresponding template in Annex 8.

17 ANNEX 8 - SYSTEM JUSTIFICATION DOCUMENT - TEMPLATE & GUIDELINES

Preliminary

This document is a form to use and fill in for producing the document related to a specific system in the context of a development project.

The "System Justification Document" (SysJD) presents the justification and rationale for selection of main engineering elements. Main engineering elements include the set of Stakeholder Requirements, the set of System Requirements, the architectural and designed elements: Functions, Input-output Flows, Operational Modes, Transition of Modes, Scenarios, System Elements, Physical Interfaces (links/connectors).

It provides the traceability between engineering elements, and the outcomes of cost analysis, effectiveness analysis, risk analysis, dependability analysis, safety analysis, and trade-offs analysis (refer to System Analysis Process) that argue chosen engineering elements.

The purpose can be extended to system integration.