Modelling bio-compatible and bio-integrative medical devices

Didier Fass, Dominique Méry

Modelling bio-compatible and bio-integrative medical devices

Didier Fass *didier.fass@loria.fr*
Dominique Méry, *dominique.mery@loria.fr*

AUTHORS VERSION

Abstract

Developing and producing medical devices and healthcare systems is a crucial issue, both for the economy and for providing safe advances in healthcare delivery. We propose a taxonomy of medical human machine systems and we define classes of healthcare applications for identifying a number of approaches and to overcome difficulties of bio-compatibility and bio-integration. Our aim is to demonstrate how medical devices design, and more generally human-machine system concepts and epistemology, depend on our skills to think and conceptualize generally human system integration. We claim that it is necessary to reclaim these concepts for ensuring correct by construction medical devices bio-compatibility and bio-integrative properties from the early stage of the design process.

Keywords

Medical devices, modelling, system engineering, human system integration, bio-CPS, bio-compatibility, bio-integration, correctness by construction

1 Introduction

Developing and producing medical devices and healthcare systems is a crucial issue, both for the economy and for providing safe advances in healthcare delivery. Medical devices become smaller in physical terms (see for instance the new pacemaker implanted inside the ventricular) but larger in software-based elements, the design, testing, validation, and eventual authority device approval is becoming expensive for medical device manufacturers both in terms of time and cost. The increase of alarming rate leads to recalling failing devices. Recalling failing devices is increasing cost and gives a very negative feeling to patients as well as physicians; it leads to consider both forensic and medical issues. Questions on costs should not hide safety and security problems that are now stated in this new generation of software systems. Moreover, safety problems are related to requirements that are either related to technical elements or related to human body - both anatomical and physiological, features. As claims by Dines Bjoerner [9,11,19] "Before software can be developed its requirements must be stated. Before requirements can be expressed the application domain must be understood". Since main healthcare system domain is life and health (biology and its two sub-domains: anatomy and physiology), medical devices require integration within or on the body – living system, it leads *to modeling bio-compatible and bio-integrative medical devices.* That needs to take into account information that is not necessarily explicit in the list of requirements and in the definition of domains such as nature of interactions and time representation. Systems under investigation are often called *cyber-physical systems*, for short CPS, and necessitate medical human-machine systems design integration, validation and certification. We propose a taxonomy of medical human-machine systems and define classes of healthcare applications for identifying a number of approaches and to overcome difficulties of bio-compatibility and bio-integration. Using the pacemaker case study, we sketch our Event-B-based methodology, which did not consider bio-compatibility and bio-integration and we show how we intend to take into account these new ideas in a correct-by-construction approach.

2 . Categorisation of medical devices

Our aim is to focus primarily on the application of software and systems engineering to software-based medical devices used for patients. However, we classify medical devices or healthcare systems into categories corresponding to the use and to the bio-integration of these systems in the life of a patient.

A first class of medical devices is defined as devices which are permanently implanted in the body of a patient, as pacemakers, artificial heart. It requires a clear and as complete as possible statement for the environment. The challenge is to develop models for environment as well as tools. Moreover, when considering the artificial heart, we are facing questions of bio-compatibility and bio-integration.

A second class of medical devices is defined as devices which are permanently used by patients but not implanted in the body of a patient, as the hemodialysis. The model for environment is yet a challenge because the global system is integrating several organs and regulations rules for glucose. It is then clear that models for environment necessitates to express flows of fluid in the body of the patient and rate of sugars in the blood. The system is used on a regular and periodic period.

A third class of medical devices is defined as devices which are temporary used for helping somebody to reach a given target state in intensive care, as for instance the extracorporeal membrane oxygenation (ECMO) [12]. It may happen after a heart attack, when the patient's

heart requires a minimal activity, or / and during a pulmonary insufficiency (i.e. severe state with H1N1 flu) [13]. The system supports one or more functionalities and assists the patient. Still in this case we have to integrate bio-compatibility and bio-integration.

Currently, implantable or wearable medical devices are designed by abstraction with a reductionist and functionalist approach. Thus living systems are reduced to their physical properties and logical models. Therefore developed and implemented algorithms result from functional analysis methods - abstraction and digitalization, and skills (knowledge and understanding) of the designers.

Mockups and prototypes are validated firstly by technical tests for ensuring technological regulatory standards and secondly by experimental and clinical test before their wide distribution and marketing. However, certification of medical devices , as in aerospace and nuclear industry, remains a challenge.

Medical devices require original, sound and reliable validation methods [3,4,5] based on scientifically validated modeling methods and tools (model-based engineering) and grounded on theoretical biology, medical knowledge and clinical evidences, and physicians expertise (evidence-based medicine).

We show how medical devices design, and more generally human-machine system concepts and epistemology, depend on our skills to think and conceptualize generally human system integration. We claim that it is necessary reclaiming these concepts for ensuring correctness by construction medical devices bio-compatibility and bio-integrative properties from the early stage of the design pro*cess grounding on both theoretical integrative physiology principles and trustable formal method. Next, we describe the correct-by-construction approach that was used by Méry and Singh* [5], *when considering the pacemaker challenge using the Event-B modeling language.*

3 Model-based Design of Medical Devices

Formal methods have emerged as a complementary approach to ensuring quality and correctness of high-confidence medical systems, overcoming limitations of traditional validation techniques such as *simulation* and *testing*. In [5], authors propose a new methodology to obtain certification assurance for complex medical systems design, based on the use of formal methods. The methodology consists of five main phases: first, informal requirements, resulting in a structured version of the requirements, where each fragment is classified according to a fixed taxonomy. In the second phase, informal requirements are represented in formal modelling language, with a precise semantics, and enriched with invariants and temporal constraints. The third phase consists of refinement-based formal verification to test the internal consistency and correctness of the specifications. The fourth phase is the process of determining the degree to which a formal model is an accurate representation of the real world from the perspective of the intended uses of the model using model-checker. Last phase provides an animation framework for the formal model with real-time data set instead of toy-data, and offers a simple way for specifiers to build a domain specific visualization that can be used by domain experts to check whether a formal specification corresponds to their expectations. Fig. 1 sketches the methodology based on the refinement process providing possible feedbacks in the design of a system following a correct by construction process and producing a trustable formal model from the informal requirements. As we have mentioned in the previous lines, the animation phase is a way to integrate the domain experts in the design process. We have to warn the reader that the model of the pacemaker is a formal expression in a formal modelling language based on set theory and on the notion of generalized substitution. The link between knowledge of experts and the formal expressions are very critical to elaborate. Our point of view is that we are facing the question of validation

of the formal model with respect to the informal requirements and the integration of physiological information or expert knowledge. A possible solution is to exploit domain ontologies combined with formal modelling language as proposed by Aït-Ameur and Mery [6]. However, it remains to consider how to model physiological features and to validate the resulting model.

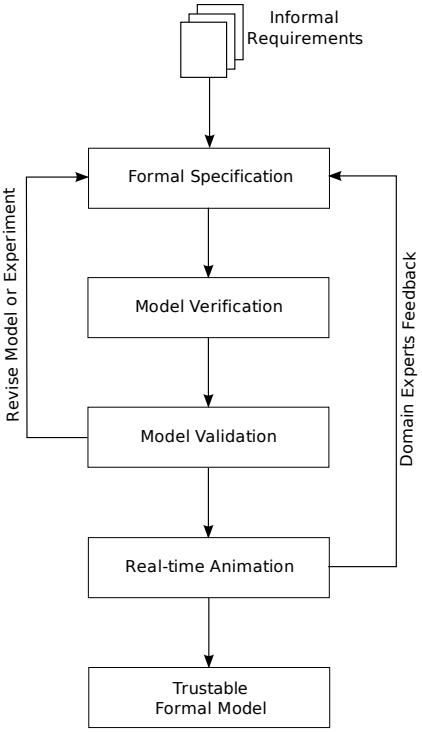

Figure 1: Design of Correct by Construction Medical Devices

We give a short introduction on Event-B [1,8] to identify what we can model with Event-B. Event-B is a formal method for system-level modelling and analysis using set theory. In Fig.1, this phase also gives the feedback to the formalization phase in case of unexpected behaviours of the system. The feedback approach is allowed to modify the formal model and verify it using any theorem prover tool and finally validate it using a model checker tool. The verification, validation and real-time animation processes are applied continue until not to find the correct formal model according to the expected system behaviour. In this phase of the formal development, most of errors are discovered by the domain experts. The real time animation is a key tool for helping the communication with domain experts.

An Event-B model expresses a state property called invariant which is defining the set of possible states of the model. A state is a mapping relating each variable to a given value. The value of a variable is in a given domain which can be either codable in a programming language or member of a domain which is representing possible values. It means that an Event-B model can have variables and state variables modifiable by a finite list of events which are modelling the possible modifications of variables. An event of an Event-B model is not executed but observed, when its guard is true. Only one event may be observed at any time. An Event-B model is discrete and does not express any liveness or fairness property, even if there some extensions of the original Event-B models. Moreover, an Event-B model is based on a logical theory based on set-theoretical or predicate calculus notations. It means that the design of an Event-B model requires specific checking of well typing or verification conditions validating the invariant property. Questions are related to what properties over medical devices can we express and how tractable are these properties? In Event-B,

we can express, first, invariant properties defining a stability condition of the system under consideration, or safety properties stating that nothing bad will happen. For instance, the pacemaker should not pace in the red zone and can pace in the green zone. Fig. 2 is containing the annotated ECG as well as the text of the invariant.

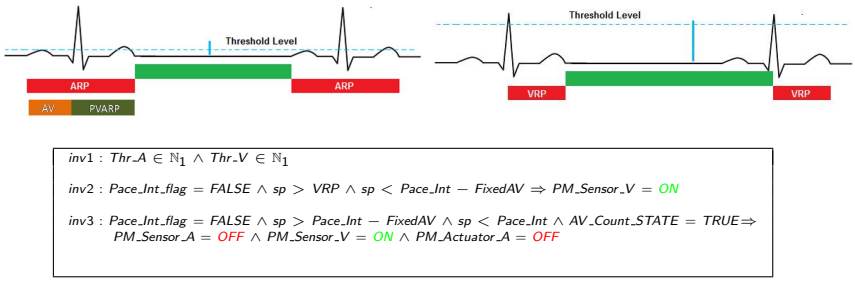

Figure 2: Example of a relation between an invariant and an ECG-based state

When validating an Event-B model, one should prove that each event maintain invariant and safety properties and this operation is done by the underlying proof assistant. The underlying proof process is adding trust to the resulting model and guide the designer when following the incremental refinement-based process for constructing formal models from informal requirements. The formality of Event-B models is helping to get a trustable model but we need to have modalities for communicating to the domain experts.

The choice of the Event-B modelling language is mainly guided by the simplicity of the basic concepts and the existence of a toolset namely Rodin [7]. Others modelling techniques can be used for developing models and the most important feature is the methodology of correct by construction development using the refinement. The refinement allows us to play with levels of abstraction. In next section, we sketch the methodology used for developing a closed-loop model for the pacemaker and we will give more details on the example of the pacemaker. We illustrate what authors were able to handle using Event-B and what we have validated and then we state questions on bio-compatibility and bio-integration in medical design devices.

4 Example of the Pacemaker

The pacemaker is a medical device which is implanted in the body of the patient. It is related to the heart by leads and it interacts with the heart according to modes defined by the physician. It is an example of a device which is supposed to remain for a long time in the body. Moreover, it augments the functionalities of the heart by helping it and the heart is evolving with the presence of the pacemaker. Consequently, the function of pumping is supported not only by the heart itself but also by the pacemaker. The heart is, after a while, working only with the pacemaker. In previous works, Mery and Singh [10] developed a discrete model of the pacemaker and the heart was modelled implicitly by records of ECG. We obtain a validation by off-line records.

In a second step, we should test the model with respect to a heart model called the electrical heart model developed by physicians. We summarize the electrical model. The heart consists of four chambers: right atrial, right ventricle, left atrial and left ventricle, which contract and relax periodically. The natural heart's system requires an electrical stimulus, which is generated by the small mass of specialized tissue located in the right atrium called the sinus node. This electrical stimulus travels down through the conduction pathways and causes the heart's chambers to contract and pump out blood. Each contraction of the ventricles

represents one heartbeat. The atrial contract for a fraction of a second before the ventricles, so their blood empties into the ventricles before the ventricles contract. The electrical current flows progressively in the heart muscle using special conduction cells. In previous works, we developed a discrete model based on the electrical conduction flow according to the points A, B, C, D, E, F, G ,H.

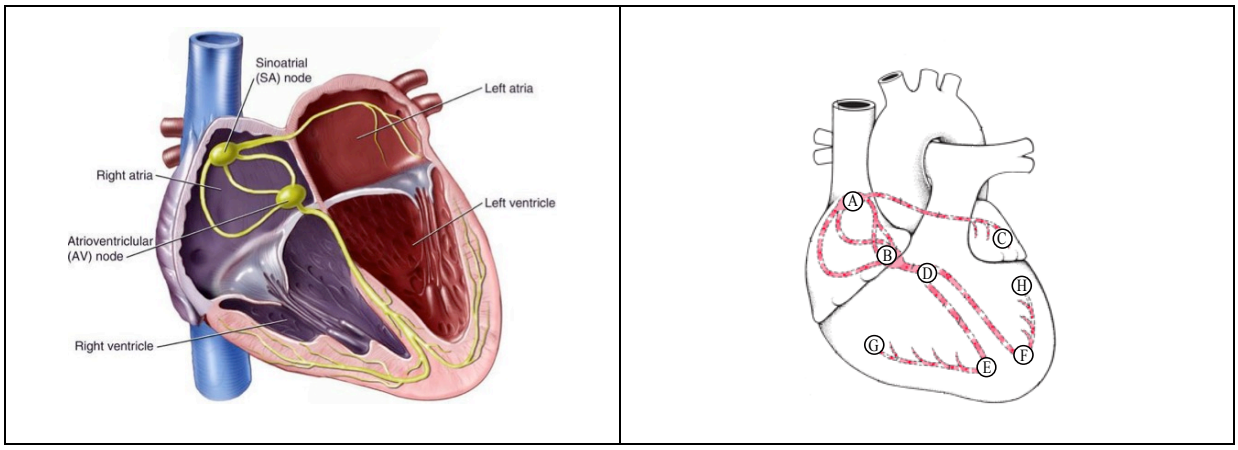

Figure 3: Different elements of the heart and the points defining the electrical conduction model of the heart.

We obtain a closed-loop model of the pumping function, since the heart was no more considered as the environment of the pacemaker but as a part of the model itself. The closed-loop model is used for studying the behaviour of the pacemaker in situ and it takes into account possible dysfunction of heart. Real time animation of formal models is a possible mean for communicating with physicians for instance in clinical experiences. Figure 4 describes the platform for animating Event-B models using a database of ECGs and plugins as Brama for feeding models. The platform is based on the Rodin tool which is offering functionalities for designing, verifying and animating models. An extra work has been done by N. Singh for making visual communications possible.

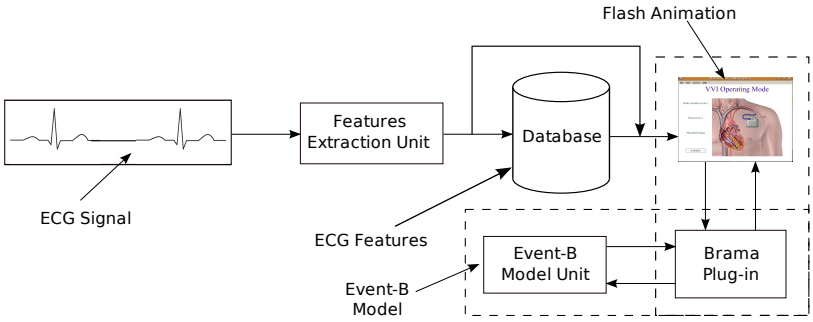

Figure 4 : Implementation of proposed functional architecture on the single electrode cardiac pacemaker case study

In the last step, we have got a more trustable model for the pacemaker. However, we have not completely dealt with questions of bio-compatibility and bio-integration. These two extra-points can be considered with the proposed methodology. However, they require to extend the methodology by considering expertise domains and by improving communication between physicians, designers and patients. Expertise domains require to integrate biology models. Finally, we summarize our position on the two concepts bio-compatibility and bio-integration in the final section.

5 Concluding Remarks and Future Directions

Medical devices belong to the class of cyber-physical systems, since they must be integrated within or on the human body generating integrated wholes, human machine systems. They are made up of two main categories of systems. These two kinds of systems differ in their nature: their fundamental organization, complexity and behaviour. The first category, the traditional one, includes *technical* or *artifactual* systems that could be engineered. The second category includes *biological* systems: the human that could not be engineered. Thus, integrating human and cyber-physical systems in design is to couple and integrate in a structural (anatomical) and dynamical or functional (physiological) coherent way, a biological system (the human) with a technical and artifactual system in the same isomorphic framework. So medical devices engineering needs to model the organ or the part of the human body and its behaviour on the one hand, the cyber-physical system physical and computational components and its behaviour on the other hand, as well as their dynamical relation (interaction or coupling) to test and validate human machine reliability and human systems integration [14].

5.1 Bio - Cyber-Physical Systems (Bio-CPS)

Traditional medical device design methods rely on analytic and reductionist concepts based on a mechanical or computational metaphor. The aim of making human and medical CPS "working" together is to assist a dysfunctional organ, transiently or permanently, to maintain the whole living system (a person) in stable condition or in a recovered "normal" condition. We call bio-CPS the whole and functional "living human artefact system" resulting from human medical CPS coupling and integration. The challenge is the design of medical CPS that ensure the correct integrative coupling by construction in spite of their different nature of interactions and the time representation.cf. table 1.

	Biological	Cyber	Physical
Symmetricity of interactions	Never	Both symmetric and non-symmetric	Always
Locality of interactions	Mainly non-local	Mainly local	Both local and non-local
Time representation	Continuous (Functional level) Discrete (Structual level)	Discrete or Event basd	Continuous

Table 1 : ***Classification of systems considering the nature of the interactions and the time representation [15]***

5.2 Medical CPS domain engineering

Using Bjoerner's framework we can ask the issue of medical devices domain to highlight its fundamental properties, which could satisfy human systems integration requirements. Bjoener's framework [19] based on the triptych: D, S -> R, where D is the domain of the problem and where requirements R are satisfied by the relation ->, which intends to mean *entailment*; so, S is a model of our system built or expressed from D. The domain provides a way to express properties and facts of the environment of the system under construction.

Bio CPS must help organ and the body (a person) to recover a stable state (invariant) compatible with survivability in intensive care or a physiological normal quality of life for implantable system like heart pacemaker despite pathology or illness.

Consequently, Bio CPS specifications or model (S) must satisfy human system integration and integrative physiology requirements (R) [14] and theoretical principles [16] [17] [18]. This especially concerns the artificial biological interface system and the behavioral monitoring and assisting computerized system and its algorithms. Their domain engineering (D) is bio-integrative engineering. By consequence we can say that an "artificial" medical CPS that satisfied human system integration properties must present two fundamental properties: bio-compatibility and "bio-integrability".

For modelling biological system and biocompatible and biointegrable artificial systems - medical devices, we propose an isomorphic framework. This conceptual framework describes three categories of required main system dimension: structural elements, shapes or forms and dynamics. Taking into account two by two this main classes of system variables, one can describe three specification plan: architecture (structural elements to shape or form specify geometrical structure or system architecture), behaviour (shape or form to dynamics specify analytical functions or functionally analysed) and evolution (structural elements to dynamics specify three main types of functional interactions: physical Φ, logical Λ , biological Ψ). If we assume that a function does not exist by itself but is the emerging result of integrative organization, this framework grounds our bio-integrative model based Bio-CPS engineering. The schema extends clearly our methodology.

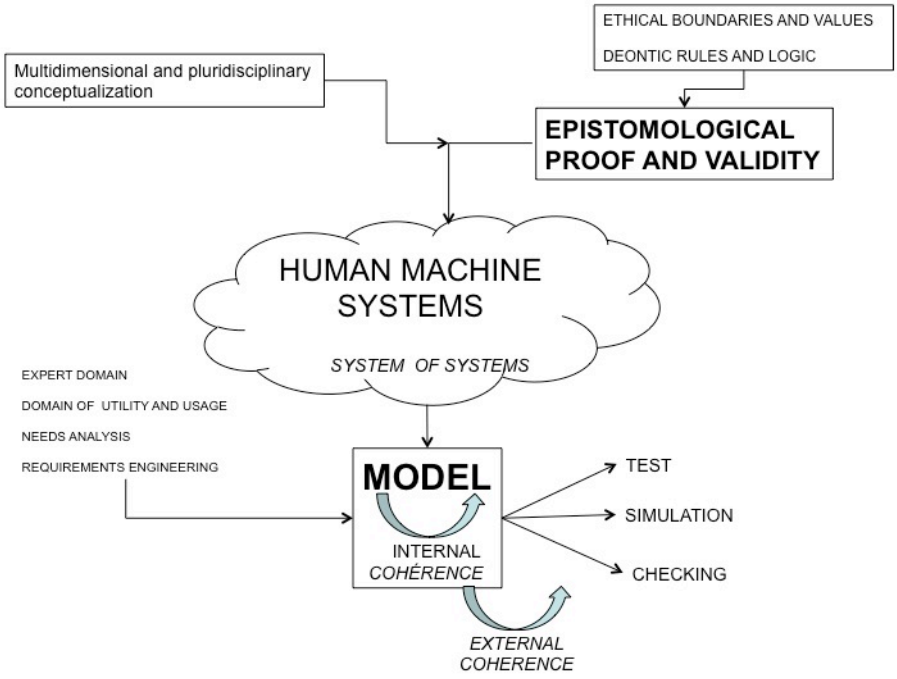

Figure 5: Challenging human-machine system - bio-compatible and bio-integrative medical devices, design and organization is modeling an heterogeneous system of systems (different by nature). That requires a proven and validate epistemic framework fitted to hybrid system, challenging the question of human machine system nature, correctness-by-construction and ensuring human systems integration reliability.

5.3 Bio CPS Methodology

We have first described a methodology based on a formal notation namely Event-B, which has been used for developing a closed-loop model for the pacemaker. The methodology is

described by Fig 1 and is not restricted to Event-B. We have to address questions on the extension of the expressivity of the assertion language that should be able to state properties of the medical domain. Moreover, modelling CPS using Event-B or another formal method is a real challenge because we have to be able to manage hybrid medical models. Hybrid medical models are mathematical objects integrating discrete and continuous features of medical system under consideration.

6 Literature

[1] Dominique Cansell and Dominique Méry. The Event-B Modelling Method: Concepts and Case Studies, pages 33–140. Springer, 2007. See [20].

[2] Cliff B. Jones, Peter W. O'Hearn, and Jim Woodcock. Verified software: A grand challenge. IEEE Computer, 39(4):93–95, 2006. URL http://dx. doi.org/10.1109/MC.2006.145.

[3] R. Jetley, S. Purushothaman Iyer, and P. Jones. A formal method approach to medical device review. Computer, 39(4):61–67, April 2006. ISSN 0018-9162.

[4] I. Lee, G. J. Pappas, R. Cleaveland, J. Hatcliff, B. H. Krogh, P. Lee, H. Ru- bin, and L. Sha. High confidence medical device software and systems. Computer, 39(4):33–38, April 2006. ISSN 0018-9162.

[5] Dominique Méry and Neeraj Kumar Singh. Trustable formal specification for software certification. In Leveraging Applications of Formal Methods, Verification, and Validation - 4th International Symposium on Leveraging Applications, ISoLA 2010, Heraklion, Crete, Greece, October 18-21, 2010, Proceedings, Part II, pages 312–326, 2010. URL http://dx.doi.org/10.1007/978-3-642-16561-0_31.

[6] Yamine Aït-Ameur and Dominique Méry. Making explicit domain knowl- edge in formal system development. Sci. Comput. Program., 121:100–127, 2016. URL http://dx.doi.org/10.1016/j.scico.2015.12.004.

[7] Jean-Raymond Abrial, Michael J. Butler, Stefan Hallerstede, Thai Son Hoang, Farhad Mehta, and Laurent Voisin. Rodin: an open toolset for modelling and reasoning in event-b. STTT, 12(6):447–466, 2010. URL http://dx.doi.org/10.1007/s10009-010-0145-y.

[8] Jean-Raymond Abrial. Modeling in Event-B - System and Software En- gineering. Cambridge University Press, 2010. ISBN 978-0-521-89556-9. I-XXVI, 1-586 pp.

[9] Dines Bjørner. Domain engineering: A software engineering discipline in need of research. In SOFSEM 2000: Theory and Practice of Informatics, 27th Conference on Current Trends in Theory and Practice of Informatics, Milovy, Czech Republic, November 25 - December 2, 2000, Proceedings, pages 1–17, 2000. URL http://dx.doi.org/10.1007/3-540-44411-4_1.

[10] Dominique Méry and Neeraj Kumar Singh. Formalization of heart models based on the conduction of electrical impulses and cellular automata. In Zhiming Liu and Alan Wassyng, editors, FHIES, volume 7151 of Lecture Notes in Computer Science, pages 140–159. Springer, 2011. ISBN 978-3- 642-32354-6.

[11] Dines Bjørner. SOFSEM 2000: Theory and Practice of Informatics: 27th Conference on Current Trends in Theory and Practice of Informat- ics Milovy, Czech Republic, November 25 – December 2, 2000 Proceedings, chapter Domain Engineering: A Software Engineering Discipline in Need of Research, pages 1–17. Springer Berlin Heidelberg, Berlin, Heidelberg, 2000. ISBN 978-3-540-44411-4. URL http://dx.doi.org/10.1007/3- 540-44411-4_1.

[12] Darryl Abrams, Alain Combes, and Daniel Brodie. What's new in extra- corporeal mem-

brane oxygenation for cardiac failure and cardiac arrest in adults? Intensive Care Medicine, 40(4):609–612, 2014. ISSN 1432-1238. URL http://dx.doi.org/10.1007/s00134-014-3212-0.

[13] Antoine Kimmoun, Fabrice Vanhuyse, and Bruno Levy. Improving blood oxygenation during venovenous ecmo for heartsr. Intensive Care Med, 39: 1161–1162, 2013.

[14] Didier Fass. Augmented Human Engineering: A Theoretical and Experimental Approach to Human Systems Integration. INTECH Open Access Publisher, 2012. ISBN 9789535103226. URL https://books.google.fr/books?id= 5ujboAEACAAJ.

[15] Didier Fass and Franck Gechter. Towards a theory for bio-cyber physical systems modelling. In Digital Human Modeling. Applications in Health, Safety, Ergonomics and Risk Management: Human Modeling, pages 245– 255. Springer, 2015.

[16] Gilbert A. Chauvet. Hierarchical functional organization of formal biological systems: a dynamical approach. i. the increase of complexity by self- association increases the domain of stability of a biological system. Philo- sophical Transactions of the Royal Society of London B: Biological Sciences, 339(1290):425–444, 1993.

[17] Gilbert A. Chauvet. Hierarchical functional organization of formal biological sys- tems: a dynamical approach. ii. the concept of non-symmetry leads to a criterion of evolution deduced from an optimum principle of the (o-fbs) sub-system. Philosophical Transactions of the Royal Society of London B: Biological Sciences, 339(1290):445–461, 1993.

[18] Gilbert A. Chauvet. Hierarchical functional organization of formal biological sys- tems: a dynamical approach. iii. the concept of non-locality leads to a field theory describing the dynamics at each level of organization of the (d-fbs) sub-system. Philosophical Transactions of the Royal Society of London B: Biological Sciences, 339(1290):463–481, 1993.

[19] Dines Bjørner. Domain Engineering - Technology Management, Research and Engineering, volume 4 of COE Research Monograph Series. JAIST, 2009. ISBN 978-4-903092-17-1.

7 Author CVs

Didier FASS

FASS Didier, Associate, Associate Professor at ICN Business School and researcher at LORIA in MOSEL team**,** responsible for Artem "Augmented human" project. Professional Skills: Expert for ANR, IEEE, Human and Systems, Health ethics National and International Projects: 6FP EU Craft DRIVESAFE (2004-2007); PPF Fibrous Material "Pôle de Compétitivité" Natural Fibers Grand Est (2005-2008); PAUSA Aerospace Valley and DGAC (2006-2008) Collaborations: NASA Ames Research Center Human System Integration Division, ONERA Salon de Provence, Georgia Institute of Technology, Intensive care unit CHU Nancy Brabois, Academic Title: PhD in Neurosciences on the 23. December 2002 under supervision of Professor Jean-Paul Haton (Artificial Intelligence) and Professor Francis Lestienne (Neurophysiology); Doctor of Dental Surgery on the 6. June 1991 on Knowledge based Diagnosis modeling and Medical imaging (TDM and RMI) under supervision of Professor Daniel Rozencweig (Occlusodontics) and Professor Augusta Tréheux (Medical Imaging); Master in Management Nancy 2 University (1992); Master in Cognitive Sciences, LIMSI, Orsay Paris XI (1994); Degree in Psychophysiology (1995) and Post-graduate in Forensic Expertise

(2010) Medical School Nancy University. Price and Professional achievements: Fellowship French Occlusodontics College (1991), Member of the Board – Forum advisory committee TELECOM International Telecommunication Union (ITU) (2007-2012).

Dominique MERY

MERY Dominique, Full Professor of Computing Science at Université de Lorraine since the first of September 1993, Head of the Research Group (Formal Methods and Applications) at the LORIA Laboratory. Head of the PhD School IAEM Lorraine. Professional Skills: Expert for NSF, Enterprise Ireland, ANR, AERES National and International Projects: ANR SETIN RIMEL (2007-2010); RNRT EQUAST (2003-2005): ACI Sécurité DESIRS (2003-2006); CTI CNET 1995-1998 Academic Titles PhD in Computer Science on the 31. May 1983 under the supervision of Professor Patrick Cousot and Thèse d'état on the 26. February 1993 in Mathematics. Prices and Professional Achievements: Member of l'Institut Universitaire de France [1995-2000]. Grant for Scientific Excellence Grad A (2009- 2013)). Member of IFIP WG 1.3 Foundations of System Specification.

1