A Consilience-Based Approach to Engineering Services in Global Supply Chains

Eswaran Subrahmanian, Albert Jones

A Consilience-based Approach to Engineering Services in Global Supply Chains

Eswaran Subrahmanian[1] and Albert Jones[2]

[1] Carnegie Mellon University, Pittsburgh, PA, USA
asub@cmu.edu
[2] Systems Integration Division, NIST, Gaithersburg, MD, USA
albert.jones@nist.gov

Abstract. Technology life cycles are becoming shorter as is the time for those technologies to become ubiquitous in the society. The Industrial Revolution took about 150 years; but the computer revolution took only 50 years. Cell phones, which hit the market in the early 1980s took only 25 years to become a global phenomenon. Computers and cell phones are two examples of a growing number of products that marry hardware, software, communications, and physical components into what are called cyber physical systems. Even though humans are, for the most part, only users of these systems, they are already having a considerable impact on the evolution of society. In this paper, we focus on the next stage of that evolution, cyber-physical systems. We also focus on changes in how these systems are engineered. Formally designed only by OEMs, these systems are now engineered across the supply chain. A number of companies now provide engineering services. We discussed a number of existing approaches to systems engineering and concluded that they are inadequate. Finally, we propose a new, consilience-based approach that draws on the disciplines and practices that can inform and help resolve those inadequacies.

1   Introduction

Large, man-made systems have undergone a major transformation over the past 100 years. They have grown in both size and complexity making the integration of sensing and control significantly more difficult. They have incorporated substantial amounts of hardware and software and they have achieved unprecedented degrees of automation. All of which has led to emergent behaviors that are difficult to predict and often have disastrous consequences. As a result, the engineering of these systems has also undergone significant changes.

Starting about 50 years ago systems were designed by a small team of engineers at the Original Equipment manufacturer (OEM) – the supply chain only produced the components in that design. The design was created using the three-step reductionist approach developed more than 400 years ago by Rene Descartes. The first step is to decompose the system into a hierarchy of constituent components. You then compute their performance capabilities and material properties using well-known scientific

theories. Finally, you infer the behavior of the entire system from the behavior of its components.

The reductionist approach is typically visualized using the classic V model used in systems engineering. The V model encompasses a series of processes beginning with requirements definition and hierarchical decomposition, through functional mapping, component design (down the left-hand-side of the V) and component performance testing, subsystem integration test, and, finally, system validation test (up the right-hand side). The thinking behind a reduction approach is ubiquitous - permeating nearly every facet of engineering practice. It has succeeded to the point where most engineers exclusively focus on a single component or technical discipline of the system - often ignoring the fact that it is, indeed, part of a system.

Until recently, this "components-first, interactions- later" V approach served engineering well. For a number of reasons, this approach has proven to be too costly, too time consuming, and too error prone. This paper focuses on two of those reasons. First, engineering is no longer provided solely by the OEMs. Engineering is now provided as a service by several members of the supply chain. This means that systems and their components are now engineered and produced across the globe. Second, those systems and components are no longer just physical; they are now inherently cyber and physical.

2   The emergence of Cyber-Physical Systems

There has been a large-scale infusion of cyber technologies into these systems and components. We use the term cyber technologies broadly to include computers, micro-processors, software, sensors, and networks. The fusion of, and in some cases the replacement of, physical components with cyber components has been termed Cyber-Physical Systems (CPS) This is not about adding cyber technologies "on top of" conventional physical components where both sides maintain separate identities. This is about marrying cyber technologies with physical components, at multiple temporal and spatial scales, to create new kinds of systems. These new systems are, to a large extent, autonomous. Clearly, the technological advantages – particularly safety, efficiency, and reliability - brought about such a marriage can have broad benefits on the economy and the society.

We must stress cyber-physical systems are not simply the connection of different kinds of components. They are rather a new system category that is intrinsically a multi-layered network of interacting physical, computational, and human components. The resulting systems exhibit evolutionary behaviors that are (1) increasingly dynamic, unpredictable, and complex, (2) the results of the structural interactions among the various components, and, (3) whose cause and effects are often separated in time and space [19]. It is not possible, however, to determine whether these evolutionary behaviors are the result of components acting alone or combinations of components working together.

Effective methods and tools for designing and predicting the behaviors of physical components and physical system and have been in common use for years. These

methods and tools work because compositionality and composability assumptions are valid for physical systems. There is a growing belief that these assumptions are not valid for cyber-physical systems. Consequently, new methods and tools are needed that allow us to engineer these cyber-physical systems [10].

In the following sections, we provide an historical perspective on OEM engineering practices and discuss the impacts of the change to supply-chain engineering services. We then propose a new consilience-based approach that addresses those changes.

3 Historical Approaches to Engineering

3.1 Systems Engineering

The classic model of systems engineering is embodied in the V shape. The V shape comprises a set of methods starting from requirements, hierarchical decomposition, component design (down the left-hand-side of the V) and component testing, subsystem composition test, and, finally, systems testing (up the right-hand side). This methodology focusses on the design of the system in very top down fashion. This process has worked extremely well for purely physical systems; it has had problems, however, since the emergence of cyber-physical systems. The fundamental reason is the added complexity introduced by the cyber components. The historical evolution and increase of complexity and the rise of new approaches and trans-disciplinary efforts to address that complexity illustrate this best.

Before the use of computing and software, most early systems were electro-mechanical systems with a clear definition of functional boundaries. This clarity was present even when there were numerous possible choices (say n) for the functional decompositions. Further, for each such decomposition there were many possible realizations (say m) of the physical artifact. This led to n*m (order n squared) possibilities to realize a given system design; at of the each levels of system, subsystems and sub-subsystems. However, with the introduction of cyber components, the boundaries between mechanical and electrical components have become more ambiguous. Ambiguity arises because of the potential for computationally efficient choices (say r) for replacing some or all of the functions of, and the interfaces between, existing electrical and mechanical components.

Such choices add to the complexity of both the design process and the result products. They change the original functional-to-physical mapping into a functional-technology-realization mapping. The resulting complexity goes from n*m (n squared) to n*r*m (order n cubed) for each subsystem in the system network [13]. In addition, the specification of interface requirements has become dramatically more difficult. This happens because of the constant change in the boundaries between the physical and cyber components. As the authors in [31] have observed most failures in systems design happen at the interfaces, which presents significant design challenges.

There has been a long tradition of studying and modeling socio-technical systems where the work requires deciphering and understanding the social interactions, social norms, and behavior in the design of these systems [35]. The focus of this effort was increasing participation of the employees in the design of the systems to humanize,

the industrial aspects of a technical system. This view came of out of the ideas of learning organizations and the development of idea that practice is guided by "theory of use" [2]. The methods that arose out of this work are often termed soft systems methodology [9]. More recently, the rise of modeling social systems as computer models have opened up the possibility to model different forms of social in terms of agency and actor motives and goals [12, 36]. In line with these developments, more recently there have been calls for rethinking socio-technical perspective calling for co-design and analysis of both the physical and organizational systems using actor based models [11].

3.2 Software Engineering

One can observe that the field of software engineering has changed from the earlier approaches of waterfall model of software development to more flexible model represented by Spiral model of development [5]. Currently software engineering is moving away from Value-neutral approaches (requirements to product without any analysis of the intrinsic and explicit value of software products) to Value based approaches that advocate concurrent engineering, justification of choices, evaluation of real options in terms of strategy and evolution and issues of ethical production of software [6, 7]. These efforts not only address the issue of the tangible and intangible value of these systems but also the fact that to avoid failure, concurrent engineering must focus on the interfaces between different systems [16].

3.3 Concurrent Engineering

Concurrent engineering is another approach that originated in the 1980's in the design of complex engineered systems like cars, aircraft and other products [21]. The main focus of this approach has been to bring the variety of functional perspectives and disciplines in the context of design and manufacture of systems. These approaches focus on ensuring that identification potential mismatches between the different subsystem and the interfaces early in the process of design. It is well known that the cost of mismatch when caught early in the process is less than when the mismatch is identified at the later stages of product development and manufacturing process. To facilitate concurrent engineering, considerable effort was placed on developing collaborative engineering tools some of which have evolved over time and entered the main stream in engineering [15].

3.4 Cognitive Systems Engineering

Another discipline that has made an impact on the design of physical systems over the last 25 years is cognitive systems engineering. Cognitive systems engineering has focused on the match between the human cognitive ability and the interface to the physical system. Originally, started from the design of operator rooms for nuclear power plants, this effort has moved to the area of cockpit design for aircraft and other interfaces where the criticality of reaction of the human in the loop to respond to the

state of system [17]. In this view of systems design, the combination of operators and machines constitutes the system. Operators here are not users in the sense of human-computer interaction but of humans, machines, and systems that constitute the work-place.

Cognitive systems engineering is distinguished from the study of human computer interaction (HCI). HCI has evolved into the new discipline of Interaction Design. The history of this evolution is recounted by Moggridge in his book "Designing Interactions" [20]. Here, the human is considered a user with a free range of operations – examples include the mouse and the smartphone. The underlying principles of interaction design still have limitations in the sense of treating the process of interaction as purely an information processing task [pg 17-19, 17]. As more of these devices become part of the work environment, the necessity to incorporate the lessons of cognitive systems engineering will become critical, since users will no longer have complete freedom. Instead, they will become operators in the work environment with specified functions to perform.

3.5   Model-based Engineering

In systems engineering a new trend is to increase the use of computer-interpretable models especially in the specification and design stages, . This approach is generally known as model-based engineering. Model-based engineering is an attempt to codify the underlying information models that characterize the different aspects of designed product. The model-based effort has always existed in the form of modeling physical systems through differential equations and other mathematical and graphical formalisms in systems engineering. What is new in the recent effort is create models that represent software in languages such as UML. In the systems engineering domain, the extension and adaptation of UML to systems design has resulted in intuitive modeling tools such as SYSML.

3.6   Social Aspects of Engineering

For the most part, the social aspects of systems engineered using the aforementioned approaches are neglected. That is, the role that humans play in the operation and maintenance of such systems is rarely included in their design. The famous sociologist, Charles Perrow, in his analysis of the accidents at Three Mile Island and other complex engineered systems, points out that it is impossible to identify all the paths and dependencies in such a system. He concluded, therefore, that many of these catastrophic accidents are what he called "normal" [23]. What he meant by this term is that such accidents are a part of the systems design that often remain unknown to the designers. He and others recently refined this theory of "Normal Accidents" to make the case that as the complexity of the engineered system increases, the humans organizations that interact with and manage these systems often contribute to their failure [23]. He also argues that if the system is monolithic and tightly integrated the potential for dire consequences of such failures can be catastrophic as was the case in Fukushima, recent financial crisis and other disasters [24, 26]. In his essay on complexi-

ty, catastrophe and modularity [25], he argues such systems should be linearized and modularized to ensure that any failure remains local and poses minimum vulnerability both to the systems themselves and to the surrounding societal and environmental systems. This thesis is based on the idea that events with very low probability but very high consequences cannot be ignored when designing and building systems whose complexity is not fathomable. Recent experiences of Fukushima and the financial crises, among others, certainly lend credence to this thesis [27].

3.7 Remarks

This section has illustrated historically the development of, and some of the limitations of the existing approaches to address the ever growing complexity of engineered systems. These approaches have been necessary to incorporate new advances from a variety of cyber and physical technologies that help manage that complexity. Our claim is that the design of Cyber Physical systems and Cyber Physical Social systems require a new approach that synthesizes and integrates more than the traditional scientific and engineering disciplines. This new approach must include insights, theories, methods, and models from the social, cognitive, organizational and behavioral sciences. We call this new approach consilience-based systems engineering.

4 A new consilience-based approach to Systems Engineering

Consilience, according to the famous entomologist, E.O. Wilson is the synthesis of inductions from more than one discipline [37]. From this perspective, consilience in design is to draw upon all disciplines that can inform the design of a system in ways that transcend these disciplines themselves. As noted above, the V-structured systems engineering approach of the past is no longer viable. The rising complexity of engineered systems, the growing infusion of cyber components into these systems, and proactive role of humans and other social institutions in these systems makes the need for a new approach imperative. This new approach is what we call a "consilience based approach" [32]. This approach relies on integrating the product characterization in terms of complexity and the societal characterization in terms of its associated disciplinary perspectives. These disciplinary perspectives come with their own inductions on the structure and behavior of complex systems as we have observed in the previous section. The question then is how do we integrate these inductions and perspectives?

Engineers model every physical and cyber component of the cyber physical system. Without these models, they could not achieve either a comprehension of, or a valid design of, that system. Each model, by its nature, is limited in scope. Each model attempts to replicate the behavior of the corresponding component. Therefore, multiple models are needed to capture every aspect of the system and to predict its overall performance under different operating conditions. Moreover, these models are refined continually to deal with anomalies that arise in the system over time. A very nice example is from aircraft design, where computational fluid dynamics models, wind

tunnel experiments with physical models, and inflight testing of prototype models are all used to understand different aspects of the performance of a new aircraft.

Since each of these models is developed and tested using different technical disciplines, there is the need for additional models that serve as interfaces between the disciplines and the models that participate in the design. These additional models capture the information exchanges that represent the interfaces between the disciplines and the models. UML [8] for software engineering and SysML [33] for recording the interactions during the requirements stage among software, hardware and physical systems are used to represent those information exchanges.

Following the traditional V structure, these component cyber, physical, and information models would be developed and tested separately before attempting to integrate them into a system model. However, this approach fails to account for the potential, unintended, emergent behaviors that arise from the integrated system. Moreover, the additional post-hoc integration of separate societal models will only increase the likelihood of those behaviors. Hence, we need an approach that takes into account the financial and social value of engineering in CPSS as they are highly integrated heterogeneous components and systems that need to be failure proofed by design. In doing so, we argue that the resulting systems must maximize safety and reliability, and minimize the potential consequences of their failures.

To address this need we advocate the extension and propose that a model-based approach that characterizes all aspects of the Cyber Physical Social System (CPSS) be undertaken. This approach not only models the Cyber-physical part but also includes models of human-CPS interactions and organization-CPS interactions. This approach necessarily borrows modeling methods from the traditional scientific and engineering disciplines described above. Additionally, it requires the creation of new modeling paradigms to represent (1) the temporal/spatial interfaces among all components, (2) the behaviors of the human and societal components, and (3) their interfaces with the CPS components. For example, there is a need for time encoded programming languages as proposed in [18] for cyber physical systems. On the other hand, understanding the interactions between humans and machines and developing high fidelity models of those interactions is a relatively new cross-disciplinary effort. Similarly, we would require network models of human behaviors - both individual and collective - and organizational behaviors of relevant societal systems. More importantly, we need cross-disciplinary models that can be used to evaluate vulnerabilities arising from the interactions and dependencies between human, organizational, and CPS components.

The advocated model-based approach specifically addresses the dynamic relationships between the system's structure and its behavior. This approach starts with a complete and computer-interpretable representation of the system's behavioral requirements. Traditional reductionist techniques are then used to identify all of the components, their desired material and behavioral properties, their relationships to one another, and their associated interfaces. This results in a multi-layered, highly integrated structure with the components within and across each layer forming complex networks of physical and social systems. The third step involves the development and testing of numerous mathematical and computational models of the individual components, their behaviors, and their properties. New synergistic techniques are

needed to integrate these component models together layer by layer until the system model is generated. At every step, the behaviors, and where relevant the material properties, of these models are checked against the requirements. The real-world system will be constructed, or modified if it exists already, only after meeting all of the requirements.

To ensure that such modeling efforts are carried out consistently to address the problem of integrating the different disciplines new metrics and measurement methods will be needed. Beyond measurements there would be an explicit need to develop standards for the different modeling paradigms that will be encountered in the design of these complex interlinked networks. We will also need standards for modeling and designing these network topologies of the socio-technical organizations that will ensure linearization properties that can minimize the scope consequences of failures. Scale-free networks provide such possibilities but they are also vulnerable to catastrophes under certain design conditions [28, 3]. The need for modeling and designing such networks is still a nascent field. In all of these domains of enquiry, the timely availability of models for testing conformance to specified behavior and standards will be critical.

5   Summary

Technology life cycles are becoming shorter as is the time for those technologies to become ubiquitous in the society. In [14], the authors estimate that the Industrial Revolution took about 150 years; but the computer revolution took only 50 years. Cell phones, which hit the market in the early 1980s took only 25 years to become a global phenomenon. Computers and cell phones are two examples of a growing number of products that marry hardware, software, communications, and physical components into what are called cyber physical systems. Even though humans are, for the most part, only users of these systems, they are already having a considerable impact on the evolution of society.

In this paper, we have focused on the next stage of that evolution, cyber-physical systems, and the change to supply-chain engineering services. We claimed that humans and other social organizations would play a much more active role in these systems – often contributing directly to their success or failure. Because of this, we have argued that the roles of the humans and organizations must be taken into account when engineering these systems. We discussed a number of approaches to systems engineering and concluded that they are inadequate for this purpose. Finally, we propose a new, consilience-based approach that draws on the disciplines and practices that can inform and help resolve those inadequacies in the design of CPS. This new approach would critically depend on the development of new measurements and standards for the design and performance of these systems at varied interfaces between these systems.

References

1. Amanna, A., Overview of IntelliDrive / Vehicle Infrastructure Integration (VII), Virginia Tech Transportation Institute, May, 2009.
2. Argyris, C., and Schon, Theory in Practice, Jossey-Bass, Sanfranciso, 1974
3. Barabasi, A., Scale-Free Networks: A Decade and Beyond, Science, Vol. 325 no. 5939 pp. 412-413, July, 2009
4. Bashshur, R., Reardon, T., and Shannon, G., Telemedicine: A new Kind of Health Care System, Annual Reviews of Public health, Vol. 21, pp. 613-637, 2000.
5. Boehm B., "A Spiral Model of Software Development and Enhancement", ACM SIGSOFT Software Engineering Notes", "ACM", 11(4):14-24, August 1986.
6. Boehm B. and Huang, L.G., "Value based software engineering: A case study," IEEE Computer, March, 2003.
7. Boehm, B., Value based Software engineering: Seven Key elements and ethical considerations, USC-CSE 2005, University of Southern California, 2006. http://csse.usc.edu/csse/TECHRPTS/2006/usccsse2006-640/usccsse2006-640.pdf
8. Booch, G., Rumbagh, J. and Jacobson, I., Unified Modeling language user guide, Addison Wesley, New York, 2005.
9. Checkland, P., Soft systems methodology: A thirty year retrospective, Systems and Behavioral Science, Issue 17, pp. 11-58, Nov., 2000.
10. CPS Summit, Report from the Cyber-Physical Systems Summit, St. Louis, April 24-25, 2008.
11. de Bruijn, H. and Herder, P. M., System and actor perspctives on Socio-technical systems, IEEE Transactions on Systems, Man and Cybernetics – Part A; Systems and Humans, Volume. 39, no.5, pp. 981-993, 2009.
12. Epstein, J.M., Generative Social Science, Princeton University Press, 2006,
13. Erens, F. J., The synthesis of variety : developing product families, PhD thesis, Technical University of Eindhoven, 1996
14. Evans, P. and Annunziata, M., Industrial Internet: Pushing the Boundaries of Minds and Machines, http://files.gereports.com/wp-content/uploads/2012/11/ge-industrial-internet-vision-paper.pdf , 2012
15. Fenves, S. J., et al. "Product information exchange: practices and standards." Transactions of the ASME-S-Computing and Information Science in Engineering, 3, 238-246, 2005.
16. Finger, S., Konda, S. L. and Subrahmanian, E., "Concurrent design happens at the interfaces," M, Volume 9, Issue 2, pp 89-99, April 1995.
17. Hollnagel, E. and Woods, DD, Joint Cognitive System: Foundations of Cognitive Systems Engineering, Taylor and Francis, 2005.
18. Lee, E., "Cyber Physical Systems: Design Challenges," Proceedings of ISORC, Orlando, May, 2008
19. Meadows, D., Thinking in Systems, Chelsea Green Publishing Company, 2008
20. Moggridge, B., Designing Interactions, MIT press, 2007.
21. Nevins, J. L. and Whitney, D., Concurrent design of Products and Processes, McGraw Hill, 1989.
22. NextGen, http://www.faa.gov/nextgen/ as of December 6, 2012

23. Perrow, C., Normal Accidents: Living With High Risk Technologies, (Revised edition, 1999) Princeton, NJ: Princeton University Press.
24. Perrow, C., "Fukushima, risk, and probability: Expect the unexpected," Bulletin of the Atomic Scientists, 2011.
25. Perrow, C., Complexity, Catastrophe, and Modularity, Sociological Inquiry 78:2, 162-73, May 2008.
26. Perrow, C., "The meltdown was not an accident," in Michael Lounsbury, Paul M. Hirsch (ed.) Markets on Trial: The Economic Sociology of the U.S. Financial Crisis: Part A, Research in the Sociology of Organizations, Volume 30, pp.309-330, Emerald Group Publishing Limited, 2010.
27. Perrow, C., The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters. Princeton, NJ: Princeton University Press, 2011.
28. Perrow, C., "Software Failures, Security, and Cyberattacks," Paper available at http://www.yale.edu/sociology/faculty/pages/perrow/ as of December 6, 2012.
29. Rajkumar, R., "Cyber physical Future," Proceedings of the IEEE, pp 1309-1312, March 2012,
http://www.rockwellautomation.com/resources/downloads/rockwellautomation /pdf/about-us/company-overview/TIMEMagazineSPMcoverstory.pdf, as of December 6, 2012
30. Subrahmanian, E et.al, "Boundary objects and prototypes at the interfaces of engineering design," Journal of CSCW, April, 2003.
31. Subrahmanian, E, Reich, Y., Smulders, F. and Meijer, S,M., "Design as synthesis of spaces," Proceedings of the International Association of Design Research Societies, November, 2011.
32. SysML, http://www.sysml.org/ as of December 6, 2012.
33. Tassey, G., The Technology Imperative, Edward Elgar, 2007
34. Tripp, E, "The Evolution of Socio-technical systems," Occasional paper, no 2., Faculty of Environmental Studies, York University, Toronto, 1981. http://www.sociotech.net/wiki/images/9/94/Evolution_of_socio_technical_system s.pd
35. Whitworth, B, "Socio-Technical systems." In Handbook of Human Computer Interaction, pp. 531-541, 2006. http://brianwhitworth.com/hci-sts.pdf
36. Wilson, E.O., Consilience: The Unity of Knowledge, Knopf, 1998.