Models in Healthcare Simulation: Typology and Security Issues

Jerzy Rozenblit
Dept. of Electrical and Computer Engineering,
Dept. of Surgery
University of Arizona, Tucson, AZ, USA
jr@ece.arizona.edu

Johannes Sametinger
Dept. of Information Systems
Johannes Kepler University Linz, Austria
johannes.sametinger@jku.at

ABSTRACT
This paper is a "call for action" to formalize the typology of models used in healthcare simulation models. A brief taxonomy of model types is presented. Issues of model validity, patient safety and data/system security are brought to the fore to illustrate the challenges in this field. Examples are given that further highlight the research and development challenges.

Author Keywords
Healthcare; simulation; security; life-critical systems; models in medicine.

ACM Classification Keywords
I.6 SIMULATION AND MODELING; I.6.3 Applications; J.3 LIFE AND MEDICAL SCIENCES; Medical Information Systems.

INTRODUCTION

Simulation modeling, as traditionally viewed by the engineering and science communities, is an enterprise dedicated to developing a means to "imitate" the operation of a real-world process or system. This is done for a number of reasons. In the context of analysis, we strive to gain introspection into how well an existing system works so that we might modify it to make it better. In design, we develop a virtual system (a model of the system to be designed) — a design blueprint — from which a real system is to be constructed.

In as much real systems can be measured and observed for the purpose of collecting data about them, such abilities may often be limited by the need for "non-invasive" monitoring. It is not difficult to imagine that few people would agree to direct probing of one's brain as opposed to, for instance, a functional MRI scan. Thus, simulation is often indispensable in gaining an understanding of the dynamics of the system being analyzed. Similarly, in model-based design [a1], virtualization of a system to be built allows for relatively fast and inexpensive prototyping prior to the final deployment.

Over the years modeling and simulation (M&S) has developed into a mature scientific and engineering discipline, where rigorous, theory-based foundations [a2] gained considerable footing. However, since the field spans such a broad spectrum of contexts, e.g., mathematics, natural systems in physics (computational physics), astrophysics, chemistry and biology, economics, psychology, social science, engineering, etc., it is often difficult to define its "first principles." In our approach and experience, we use the following [a2] characterization of M&S's three fundamental pillars: the real system is interpreted as the source of data, the model is a set of instructions for generating such data, and the simulator is a device (hardware/software) which executes the model. In model-based design [a3] [a1], we must develop a "digital/virtual" design model so that a system to be built can be assessed through simulation-based experiments.

In this paper, we address the rapidly emerging field of simulation in healthcare. Specifically, we attempt to provide a broad taxonomy of the large variety of models in this field and emphasize the need for rigorous validation, and design of features that will make such models robust and secure. We bring to the fore a case for research that will ensure the security of such models. This is a sorely lacking facet in research and development of models in healthcare. At this point, we have to mention that while we do not explicitly consider safety issues, it is clear that the consequences of the lack of or low security have an effect on safety. The difference between safety and security is not always obvious. Generally speaking, safety is about the protection of a device's environment, i.e., mainly the patient, from the device itself. As patients are typically not involved in simulation scenarios, patients cannot get harmed directly. Security is about the protection of the device from its environment, i.e., just the opposite to safety. As we will show security "gaps" in healthcare simulation can have an indirect effect on patients.

SpringSim 2015, April 12 - 15, 2015, Alexandria, VA, USA
MSM 2015 - Modeling and Simulation in Medicine

The rest of the manuscript is organized as follows. In the next section we discuss simulation in healthcare. Models in medical training and practice are discussed subsequently. Security issues follow next, and a summary is given at the end.

SIMULATION IN HEALTHCARE

In the last decade, we have witnessed burgeoning interest in and demand for simulation-based education and training in healthcare fields. For example, *Simulation in Healthcare* is a multidisciplinary publication encompassing all areas of applications and research in healthcare simulation technology [a4]. The rationale is clear: the goal of simulation is to create a safer patient experience by preventing medical errors and by improving outcomes. The main purpose is to train medical professionals for surgery, emergency care, cardiology, general practice, trauma, etc. Simulation is used to train students in anatomy and physiology during their training as well. The benefits are manifold:

- Providers can practice procedures, techniques and responses to various scenarios without any risk to patients. Such scenarios are indefinitely repeatable.
- Training can occur in true-to-life environments, with facilities and technology identical to those in various medical settings.
- A wide range of learners—expert physicians to high school students—can learn from simulated experiences.
- Training can support the development of a wide variety of skills.

Medical simulators have evolved from simple models of human patients to complex systems with a plethora of training procedures in various medical applications, e.g., blood draw, laparoscopic surgery, trauma care. A few example simulators include:

- Minimally Invasive Surgery
  Simulators provide surgeons, interventionists, nurses and technicians with a platform to learn and master critical skills to ensure procedural efficiency [a5]. Basic and advanced procedures incorporate detailed and complete metrics for skill assessment.
- Endoscopy
  Endoscopic simulators can teach and assess motor skills and cognitive knowledge. The endoscopes look, feel and handle exactly like the real ones. Simulators provide realistic force feedback, thus, allowing users to experience the feel of the real procedure. The level of realism depends on how physiologically accurate digital patients responses are. For example, simulation-based education in gastrointestinal endoscopy is associated with improved performance both in a test setting and in clinical practice [a6].
- Laparoscopy
  Laparoscopic simulators come with flat-screen monitors, cameras and light sources along with full sets of laparoscopic instruments. They allow users to practice various drills to perfect eye-hand coordination, non-dominant hand dexterity and intra-corporeal suturing proficiency. A study has shown the potential for computerized aptitude tests for surgical trainees to predict navigational performance [a7].
- Pelvic Trainer
  Pelvic trainers are simple boxes with apertures that simulate a patient's abdomen. Trainees can use real instruments to practice basic skills and observe the operating scene through a video display. The trainer provides a degree of realism and some haptic feedback, but no objective performance assessment other than a regular stopwatch [a8].

It is clear from the above brief summary that the spectrum of simulation methods and techniques is very broad. In the next section, we attempt to provide an initial taxonomy and argue why it is crucial to ensure that models use in healthcare simulation must be valid and secure.

MODELS IN MEDICAL TRAINING AND PRACTICE

In our view, the most general way to classify simulation models in medicine is to group them into classes that pertain to simulation scenarios and simulation systems. By a scenario, we denote a set of steps, actions that replicate a specific medical procedure which may be as simple as phlebotomy (making an incision in a vain with a needle) or as complex as multiple-organ failure emergency treatment. In all such cases, various actions taken by the trainees are carried out in a simulated setting, either by using actors as patients or with computer-based systems (mannequins) that emulate human anatomy and physiology. Such scenarios are typically scripts written by healthcare experts, which embody the above steps, define roles for each member of the team, and specify a set of performance judgment criteria. From an M&S perspective, they are not models that can be simulated on a computer-based device. However, if well-defined, they do characterize a set of components, a set of descriptive variables (attributes of a scenario), and interactions among the various "actors". It is appropriate to classify them as informal models. In the category of systems, we further classify the models as those which are used in training scenarios and the ones that are embedded in various medical devices and equipment used in actual clinical practice. Either group presents different challenges for validation, assurance of robustness, and security. For reasons of brevity and focus, we omit from the discussion here the specification of training vignettes and process flow models that are used in complex healthcare logistics scenarios, for example, Ebola response training, or mass casualty preparedness exercises. Rather, we point in the direction where formally specified, computer-simulated models can be used.

Simulated training uses not only the requisite physical equipment utilized in medical procedures, but also models that reflect the foundation for emulating the symptoms and

responses to "virtual treatment". For instance, in a scenario of an anaphylactic shock — a life-threatening allergic response — the model should present typical symptoms such as swelling, a weak and rapid pulse, lowered blood pressure, skin reactions. The treatment by injection of epinephrine should be reflected by the reversal of such symptoms. Similarly, a simulated cardiac arrest should present vitals signals from a model that faithfully represents the underlying pathology. This is a key to proper understanding and learning. Embedding models, or more specifically their realizations in the form of computational processes encoded as software and hardware, in medical devices presents an extraordinary set of fidelity, safety, security, and reliability challenges. Such models effectively "run" complex implantable devices and are a key component in medical imaging or robotic surgeries. Consider the two examples below.

It is clear to imagine the complexity of new generation implantable cardioverter defibrillators (ICDs) with pacemaker capabilities [a9]. Such a device not only paces the heart when the heartbeat is too slow, but it also delivers an electric shock in case an abnormal, life-threatening heart rhythm (ventricular fibrillation) is detected. Another case is computer assisted surgery (CAS). In CAS, models are used for pre-surgical planning and guidance. Typically robotic systems such as the surgical robot DaVinci [a10] are utilized to aid in various procedures. CAS enhances the capabilities of surgeons performing surgery but it also requires models of ultimate reliability and robustness. Indeed, it is easy to imagine the dire consequences of improper translation of the surgeon's hands' movements into an erroneous maneuver of a robotic arm's end-effector. These simple instances highlight the need for more research into assuring absolute robustness of such life-critical computing systems.

We call on the community to develop systematic methods for assessing the risk levels that various models used in healthcare systems present. Risk should be assessed in the contexts of validity (how faithfully the models reflect the real system), correctness of execution, and security. For the informal, script models used in training scenarios, the risk level is low with respect to the direct potential to endanger patients' well-being and safety. However, such models must still be validated with respect to standards and norms used in medical procedures. The training systems' models have a higher level of critically. Invalid models will lead to improper, inefficient, confusing, and erroneous training.

Models that are used "in-vivo" in systems such as the examples mentioned above are life-critical. Their failures lead to catastrophic consequences. The key issue here is: How do we know they are safe? Despite the rapid growth of innovative and powerful technologies for hardware and software design, networked computation, sensing and control, critical life-critical systems design and verification issues remain open [a11]. They are:

- Complexity, which significantly increased design, verification and certification time.
- Lack of unifying formalisms for efficient specification and exploration of design options.
- Difficulty of modification due to potential unpredictability.
- Lack of techniques for investigating preciseness of execution timing.
- Potential security vulnerabilities that can be exploited by malicious attackers.

The above issues present major research and development challenges that must be addressed by research. While many of the above aspects are being actively worked on, especially in the cyber-physical systems community, few researchers have addressed the security of medical devices and models [a12].

SECURITY ISSUES

Security measures need to guarantee confidentiality, integrity and availability. In healthcare, confidential information includes medical records but also, for example, data from wearable sensors like heart rate and heart pressure. In the context of medical simulators, confidential information includes the performance of residents during training. The integrity of information becomes critical when medical reasoning is based on this information. In simulation, modified parameters may lead to discrepancies between the simulated and the real world, thus, yielding to medical errors and declined outcomes in real patient scenarios later on. In this case, security issues may result in safety issues. The availability of simulators is less critical. Security is primarily an issue of simulation systems, as they typically involve software and communication features. Simulation scenarios are involved only as long as they include systems with software. Medical devices provide additional security challenges due to their distinctive properties, e.g., limited resources and battery power of implanted devices, less frequent or even missing security patches [a13] [a12].

Safety is the state of being protected against any non-desirable event. For example, in a surgical scenario this includes the fact that surgical equipment will not fail during the surgery. Security is also the state of being protected against any non-desirable event. In contrast to safety, security is about protection of IT itself. It should continue to work as expected even under malicious attack. If an attacker manages to alter software or a person's health parameters, safety consequences may also follow suit. Privacy is about unauthorized access to an IT system and is at stake when security is weak. Thus, any privacy issue is also a security issue. Figure 1 depicts privacy, safety and security in a healthcare simulation environment.

In pure simulation scenarios as described previously, we have only the simulator, which can have an indirect impact on the safety of patients, if the simulator is based on an

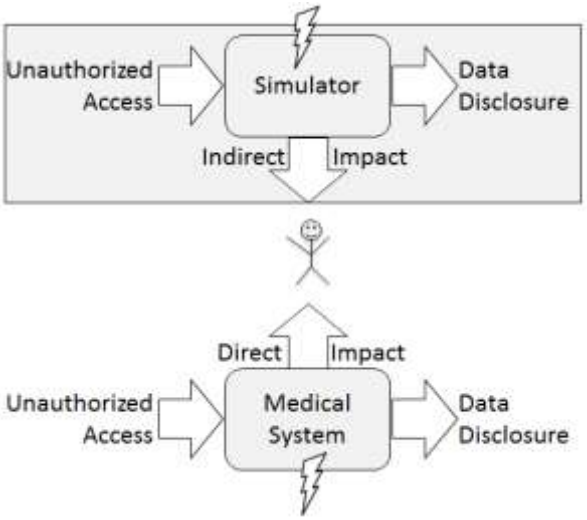

Figure 1. Healthcare simulation scenario

invalid model or if the simulator has been maliciously modified. In both cases, medical doctors may get training that is not compatible with the real world, thus leading to complications later when working with real patients. This is independent from the fact whether any medical system like a surgery robot is later used on the patient. If the simulator models a medical system, it is crucial that both systems correlate in a way that training on the simulator has positive effects on work with the medical system. Also, both the simulator and the medical system have to be protected against security and privacy breaches to prevent unauthorized access leading to data disclosure, data modification, availability problems, etc. Risk assessment is about identifying, estimating, and prioritizing risks, resulting in a function of the degree of harm and the likelihood of harm occurring. Privacy risks are given when information about a patient is accessible to unauthorized persons. Security risks involve unauthorized access not only in a reading but also in a writing mode. Safety risks can be independent of IT, they can be caused through faulty IT, and they can also be the result of security issues.

Simulation can take a variety of forms that require to be looked at separately. In training scenarios with simulators there is no direct impact to real patients. This might mislead us to the conclusion that security issues are non-relevant. However, maliciously modified simulators can have various negative consequences. For example, surgery residents may automate surgical skills based on parameters that will not later exist in the real world, resulting in a negative training effect and increasing the potential for error and negative outcomes. Besides training, simulation can be used in surgery for pre-surgical planning, and for guiding or performing surgical interventions. If robotic systems aid in surgical procedures, limitations of minimally-invasive surgery may be eliminated and capabilities of surgeons performing open surgery may be enhanced. Tele-robotic surgery permits a surgeon to perform an operation on a patient from a remote site.

In a surgery scenario, risks are manifold and depend on the type of surgery being performed. In computer assisted surgery, an attacker may manipulate results of pre-surgical planning, or the guidance for performing surgical interventions. In robotic surgery, an attacker may modify robot's behavior. In tele-robotic surgery, an attacker may make modifications in both directions of the information flow, i.e., send wrong information to surgeon, or send wrong commands to surgery robot, or again modify the robot's behavior. In this scenario, network configurations and encryption need to address security issues and HIPAA (Health Insurance Portability and Accountability Act) compliance without inordinate delay of telecommunication.

Telemedicine in general can take a variety of forms. Benefits and drawbacks have been described in [a14], e.g., breakdowns in the relationship between health professionals and patients. In a simple telemedicine scenario, MRT images are sent to remote radiologists for diagnosis. Attackers may manipulate MRT images sent to radiologists or manipulate the diagnosis being sent back. In such scenarios, regular IT security countermeasures will suffice for protection. There are also many medical simulation games available, where, for example, non-professionals simulate a heart or hip replacement surgery, or fun tools that, for example, show the results of a simulated plastic surgery on a photo. Even though these games and tools might be used to spread false information, we see only a limited risk potential and no need for stringent security measures.

SUMMARY

We have presented our initial efforts to define a typology of models used in medical simulation. Given the enormous spectrum of applications that use informal training scenarios, discrete, continuous, and hybrid models in a variety of medical trainers and simulators, and actual medical devices themselves, we are faced with tremendous challenges to ensure that such systems are safe, reliable, and secure.

Safety has long been a top priority when there is direct impact on patients. We have to make sure that harm on patients is as low as possible also when there is an indirect impact through imperfect simulation models and even through malicious activities that may introduce discrepancies between the simulated and the real world. There are other simulation applications that are interesting from a security point of view as well, e.g., simulators to optimize the use of beds in a hospital. In this scenario, patients will not be harmed, but the hospital's revenue may decrease due to wrong 'optimization'. Security considerations are also important for other simulation domains than healthcare. Just think about potential consequences of maliciously manipulated flight simulators.

REFERENCES

1. J.W. Rozenblit: A Conceptual-Basis for Integrated, Model-Based System Design, PhD Dissertation, University Mircofilms International, Ann Arbor, 1985.
2. B.P. Zeigler, *Theory of Modeling and Simulation*, John Wiley and Sons, 1976.
3. J.W. Rozenblit and B.P. Zeigler, "Design and Modeling Concepts," in *International Encyclopedia of Robotics*. (Ed. R. Dorf), pp. 308-322, John Wiley and Sons, New York, 1988.
4. Society for Simulation in Healthcare. *Simulation in Healthcare Journal*. http://www.ssih.org/News/Journal
5. S.L. De Montbrun, H.M. Macrae. Simulation and Minimally Invasive Colorectal Surgery. *Seminars in Colon and Rectal Surgery*, Elsevier Inc., Volume 24, Issue 1, March 2013, Pages 53-60. http://www.sciencedirect.com/science/article/pii/S1043148912001145
6. S. Singh, R.E. Sedlack, D.A. Cook: Effects of Simulation-Based Training in Gastrointestinal Endoscopy: A Systematic Review and Meta-analysis. Clinical Gastroenterology and Hepatology. Published Online: February 06, 2014. DOI: http://dx.doi.org/10.1016/j.cgh.2014.01.037
7. M. Ghandi, L. Funk. Computer Skills simulations as a predictor of aptitude for Arthroscopic surgery skills. 2004. http://www.shoulderdoc.co.uk/education/flash_tests/arthroscopy_aptitude1.pdf
8. J. W. Rozenblit: Models and Techniques for Computer Aided Surgical Training, *Lecture Notes in Computer Science* Part 2, LNCS 6928, pp 233-241, Springer-Verlag, 2012.
9. National Institutes of Health - National Heart, Lung, and Blood Institute. What Is an Implantable Cardioverter Defibrillator? http://www.nhlbi.nih.gov/health/health-topics/topics/icd
10. Intuitive Surgical. The da Vinci® Surgical System. http://www.intuitivesurgical.com/products/davinci_surgical_system/
11. National Science Foundation. Cyber-Physical Systems (CPS) - Program Solicitation NSF 10-515. March 11, 2010. http://www.nsf.gov/pubs/2010/nsf10515/nsf10515.htm
12. J. Sametinger, J. Rozenblit, R. Lysecky, P. Ott: Security Challenges for Medical Devices, *Communications of the ACM*, to appear April 2015.
13. K. Fu, J. Blum. Controlling for Cybersecurity Risks of Medical Device Software. *Communications of the ACM*, Vol. 56 No. 10, Pages 35-37, Oct. 2013. http://dl.acm.org/citation.cfm?id=2507771.2508701
14. N M Hjelm. Benefits and drawbacks of telemedicine. *J Telemed Telecare* 2005 11: 60. DOI: 10.1258/1357633053499886.