Proceedings of the 22nd Annual EMBS International Conference, July 23-28, 2000, Chicago IL.

The Hazard Identification & Safety Insurance Control (HISIC) for Medical Robot

Baowei Fei, Wan Sing Ng, Chee Keong Kwoh

ABSTRACT - **A novel systematic methodology for the enhancement of safety of medical robot, in terms of hazard identification & safety insurance control (HISIC), is put forward in this paper. HISIC is to identify, evaluate, and control medical safety hazards based on seven principles: definitions and requirements, hazard identification, safety insurance control, safety critical limits, monitoring and control, verification & validation, system log and documentation. HISIC tries to provide a standard for the safety of medical robot. Its initial implementation in a robot for urological application named URObot was successful. URObot in our lab is a universal platform for 3D ultrasound image-guided interstitial laser coagulation (ILC), radiation seed implantation (RSI) and laser resection (LR) to treat the benign prostate hyperplasia (BPH) and prostate cancer. URObot is currently undergoing safety test. HISIC improves URObot safety.**

KEYWORDS: **safety of medical robot, interstitial laser coagulation, radiation seed implantation, image-guided surgery, benign prostate hyperplasia (BPH)**

I. INTRODUCTION

Medical robot is a safety-critical computer-based medical system and it may directly contact patient for penetrating, cutting and removing human tissue. Its safety is one of the key issues which concerns patient's life and the risk of hospital and manufacture. Safety assurance can improve the fear of a patient and help him/her to accept the use of high technology, or computer or robotics assisted tools by the surgeon to improve clinical outcomes. Hospital and manufacture are most concern about robot failure or hazard that causes injury or even death to patient. To enhance the safety of medical robot, emergency button, redundancy sensor, and mechanical brake were adopted [1,2]. Formal method from software engineering was introduced into medical robot for the software safety. How safe is safe for a medical robot? Are there any common standard and/or principle? The concept of fault and even tree introduced in [3,4] provides a principle to handle fault event. The dependability principle was also applied to medical robot software [5]. Two general approaches for software safety are fault prevention and fault tolerance [6]. This paper puts forwards a systematic strategy called hazard identification & safety insurance control (HISIC) for the safety enhancement of medical robot. The seven principles of HISIC, include definition and requirement, hazard identification, safety insurance control, safety critical limits, monitoring and control, verification & validation, system log and documentation. HISIC is to be implemented through all phases of development, including research, design, test, application and maintenance, and all parts including software, mechanical and electrical.

II. A CASE STUDY

In CIMIL group of Nanyang Technological University, a robot for urological application called URObot has a history traced back to 1994 when a lab prototype was built for robotic TURP (transurethral resection of the prostate). URObot sought to overcome some of the drawbacks of SARP or PROBOT[1,2] identified by Ng who was among the pioneer development team in Imperial College (1989-1992). A commercial prototype was produced by Dornier Asia Medical System PTE LTD cooperated with CIMIL in September 1995. Verification and validation (V&V) was conducted before it commenced clinical trials in Changi General Hospital (Singapore) in 1998. The universal* robot for urological applications, URObot was developed in CIMIL in 1999. 3D ultrasonic image-guided interstitial laser coagulation (ILC), laser resection (LR) and radiation seed implantation (RSI) are implemented in URObot to treat benign prostate hyperplasia (BPH) and prostate cancer. URObot was designed under the principles of HISIC and is currently undergoing safety tests. Some of our preliminary work was reported in [7,8].

III. METHODS

1. Definitions

Hazard: A potentially detrimental effect on the patient, other persons, animals or surroundings arising directly from equipment. (IEC601-1 B5724 Part 1)

Hazard identification (HI): The process of collecting and evaluating information on hazards associated with the robot under consideration to decide which are significant and must be addressed in the HISIC plan.

Computer Integrated Medical Intervention Lab (CIMIL), MPE, Nanyang Technological University, 639798, Singapore. Email: mbwfei@ntu.edu.sg

* Universal is a special sense; the robot is equipped with different end manipulator module for different applications.

0-7803-6465-1/00/$10.00 ©2000 IEEE

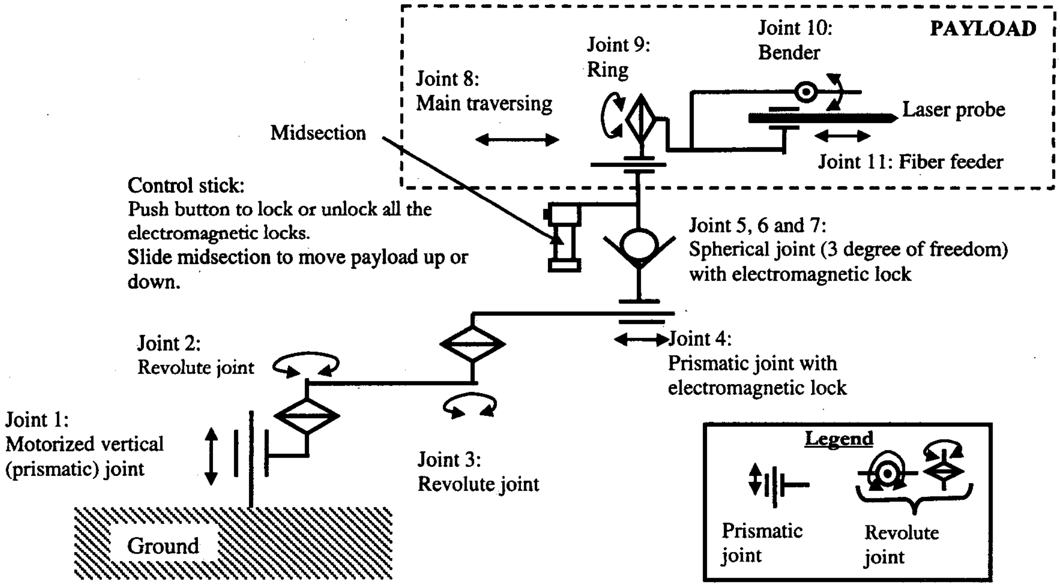
PAYLOAD
Joint 10:
Bender
Joint 9:
Ring
Joint 8:
Main traversing
Laser probe
Midsection
Joint 11: Fiber feeder
Control stick:
Push button to lock or unlock all the electromagnetic locks.
Slide midsection to move payload up or down.
Joint 5, 6 and 7:
Spherical joint (3 degree of freedom) with electromagnetic lock
Joint 2:
Revolute joint
Joint 4:
Prismatic joint with electromagnetic lock
Joint 1:
Motorized vertical (prismatic) joint
Joint 3:
Revolute joint
Ground
Legend
Prismatic joint
Revolute joint

Figure 1. Schematic of the manipulators

Safety insurance control (SIC): A step at which control can be applied and is essential to prevent or eliminate a safety hazard or reduce it to an acceptable level.

Safety critical limit: A maximum and/or minimum value to which a physical, chemical or medical parameter must be controlled at SIC to prevent, eliminate or reduce to an acceptable level the occurrence of a robot safety hazard.

Monitor: To conduct a planned sequence of observations or measurements to assess whether SIC is adequately implemented and to produce an accurate record for future verification.

Control: (a) Manage the conditions of an operation to maintain compliance with established criteria. (b) Action that corrects deviation or performance to meet criteria.

Validation: Evaluating scientific and technical information to determine if the HISIC plan, when properly implemented, will effectively control the hazards.

Verification: Those activities, other than monitoring, that determine the validity of the HISIC plan and that the system is operating according to the plan.

2. Recommended Principles

HISIC is a system methodology in which the robot safety is addressed through the identification and control of physical (mechanical, electrical, acoustic and software), medical and chemical hazards from the research, design, production, test to the end use of the finished product. Every medical robot project should have a HISIC Team which is responsible for developing, implementing and maintaining the HISIC system. The team includes designers, surgeons, physicians, patients and administration officers.

Definitions & requirements (principle 1): At the start, the HISIC team should define the medical robot: the functionality, specifications and the working environment. Then specify the detail requirements of the system, the mechanical sub-system, the electrical sub-system, the software sub-system and safety sub-system. Medical robot encompasses three main application areas: surgery, rehabilitation and supporting the disabled and hospital service. Surgical robot is the most safety-critical one since it directly contacts patient's organ and does operation, such as robot for neurosurgery. Different robot has different safety requirements. As for URObot, it is a surgical robot for urological applications which can be used to treat the BPH and prostate cancer by using 3D ultrasound image-guided ILC, RSI and LR. It is only used in the urological Operation Theater (OT) in hospital.

Hazard identification (principle 2): The purpose of the hazard identification is to develop a list of hazards which are of such significance that they are reasonably likely to cause harm, injury or death if not effectively controlled. It is important to consider medical, chemical and physical factors, such as mechanics, electricity, software, transportation, sterilization and operation. Mechanical injury: shock which causes internal bleeding and/or bone fracture, scar which leads to bleeding and contagion. Electrical injury: electrical shock which may cause burn or death, fire, electromagnetic wave that may lead to cancer, leukemia and interference. Software: out of control, malfunction, data loss and corruption. A thorough hazard identification is the key to preparing an effective HISIC plan. If the hazard identification is not done correctly and the hazards warranting control within the HISIC system are not identified, the plan will not be effective regardless of how well it is followed. The hazard identification accomplishes three objectives: Those hazards and associated control measures are identified. The process may identify needed modifications to product so that the safety is further assured or improved. The analysis provides a basis for determining safety insurance control (SIC) in Principle 3. The schematic of the manipulators of the URObot is shown in Figure 1. There are 11 joints. The mechanical hazards from these parts are listed as: (a) Joints mechanics fail, joints crack; (b) Arms mechanics fail, arms crack; (c) Locks fail, the joints slide or freeze; (d) The cartridge of the system moves during operation.

Safety insurance control (SIC) (principle 3): SIC can be either controlling methods/standards during the implementation or test/check at the end stage. It may be located at any step where hazards can be either prevented, eliminated, or reduced to acceptable levels. Complete SIC is fundamental to controlling safety hazards. SIC method must be carefully developed and documented. The information developed during the hazard identification is essential for SIC. In the above example, to prevent the mechanical failure, the quantitative mechanics data of the joints and arms should be specified during design, and the loading test of the joints and arms should be conducted after the design. In URObot, the software development adopted the methodology (shown in Figure 2) that helps ensure the safety, reliability and quality of the software. The essentials are top-down design, the 8 developing phases, safety check and V&V in a close loop in the whole system and its subsystem. The requirements were clearly defined by HISIC team. The formal methods and code standards should be adopted to prove the correctness of the software and reduce the risk of logical error, writing error and algorithm error.

Safety critical limits (principle 4): A critical limit is used to distinguish between safe and unsafe operating conditions at HISIC. Each SIC will have one or more control measures to assure that the identified hazards are prevented, eliminated or reduced to acceptable levels. Each control measure has one or more associated critical limits. The measure method for limits is to be set up and the critical limits should be scientifically based. The positive and negative limit switchers of motors can prevent the robot run out of the trajectory. Redundancy sensors and encoder feedback are used to measure the position of motors. The quantitative data of mechanical and electrical parts, such as the force, dynamic constraints, velocity, current, voltage, power, is to be addressed and have a safety range. The flow chart, fault tree, event tree and statistic method are used for software test. Ensure every module and integration of the software to be correct.

Monitoring and control (principle 5): Monitoring serves three main purposes. First, it is essential to ensure that the robot is under control. Second, it provides the feed back data to control deviation. Third, it is used in verification. Control includes: (a) specify what is done when a deviation occurs; (b)determine and correct the cause of non-compliance; (c) record the correct actions. The monitoring parameters range from the motor position, working field, touch force of end effector to computer voltage, software run path, and etc. The monitoring system should be independent to the working system and the control should be a close loop control. Redundancy computer, parallel processor, or microprocessor system can be used in the monitoring system.

Verification & validation (principle 6): V&V is the procedure that helps ensure the correctness, reliability, quality and therefore safety. Validation determines the correctness of the end product conform with what was required. Verification is performed at each phase and sub-phase of the development life cycle. It determines that each phase and sub-phase product is correct, complete and consistent with itself and with its predecessor product. V&V processes should take place during the development and implementation of HISIC, including: (a) the HISIC plan itself; (b) the system requirements; (c) software system; (d) mechanical system; (e) electrical system; (f) application (transportation, maintenance, operation). After V&V, the safety is further enhanced which was approved in our robot system.

System log and documentation (principle 7): System log is the record of actions generated by the system, such as the initial states, robot homing, gantry setting up, motor moving, lock free or lock, laser on or off, emergency button pressed or free, key pressed, image requiring, software run path, and any other actions by the robot. It is one of the key ways to monitor/track the robot internally. It also provides useful data to analysis/debug fault action. Documentation in research, design, test, application and maintenance helps to prevent human hazards.

IV. DISCUSSIONS

HISIC is a systematic methodology to deal with safety issues of medical robot. It is a teamwork that involves scientists, engineers, surgeons/physicians, patients and administration officers. The HISIC steps and principles can be applied to different applications. For a specific robot, the detail HISIC plan may be different.

Emergency button, mechanical constrains, position feedback, hardware device, passive arm, brake and redundancy sensors are the general methods for SIC. Different functional medical robots have different solutions. In neurosurgery, low moving speed and then power off before introducing a needle [9]. In total hip replacement surgery, monitoring the cutter force to sure robot does not exert excessive force on patient, external optical sensors for redundancy control system [10]. In URObot, every joint has a lock and every motor has positive and negative limit switchers. Emergency button cuts off power supply to amplifiers and stops motors immediately. Separate power supplies and UPS supports. Encoder feedback provides position information. There are lots of related works on hardware safety in literatures [1,2,9,10], such as electrical safety standard and mechanical design guideline. We put more discussions on the software safety here.

Software plays another key role in safety critical robot. Since software describe a logical process and is not a physical entity, a software failure must be a design or implementation error that may not be detected during the test phases. Its failure can be catastrophic since it controls hardware to perform actions. Inadequate specifications, poor logic design, improper implementation, support software design error or failure are the potential hazard causes. One type of software hazard is execution failure that can be caused by erroneous pointer, memory allocation, call, jump, stack, or unexpected timing and combination of conditions. Fault tree analysis, events tree analysis and failure checklists are used during HI.

The formal method and coding standard were adopted in URObot software design for SIC. The ideas of object-oriented, software reuse, modules and software level are implemented into programming. The software layers includes graphical user interface (GUI), surgeon-robot interfaces (SRI), robot controller interface (RCI) and robot controller (PMAC). Different level of the software is responsible for different task. The encapsulation of the data and the access privilege help provide the security and reliability of the software. The motion plan/cutter path is based on the input data, ultrasound images. The motion plan is carefully verified before it is used by RCI. RCI is the only way to access PMAC to drive the movement of the robot. RCI also regularly checks the status of the peripherals: PMAC, motors, amplifiers and mechanical switch. These ways assure the safety of robot motion. GUI provides simple, effective and correct interface for user to response to hazard. The software provides error process to either customer errors or system errors which are often fatal errors, such as homing fail, no image signal, PAMC off line, motor following error, amplifier fault, etc. As for fatal errors, the programs display error information and gracefully exit.

The first step of software V&V of is based on debug level. One observation is that before testing is completed, every instruction should have been executed at least once. Test data should try every error condition possible. Each branch should be tested. Thus on a two-way or three-way branch they should be tried at least once. Some special routines with unusual input data also need to be tested at least once. The test includes normal cases testing, extremes testing and exceptions testing. The second step is called "black box" testing or functional specification testing method.

HISIC runs through all phases from the research, design, construction, test to end use of a medical robot. Monitoring, control and documentation are also essential parts of HISIC.

V. CONCLUSIONS

The systematic methodology for the safety of medical robot, hazard identification & safety insurance control (HISIC) put forwards in this paper, provides a standard approach to handle hazards issues and enhance safety. The seven principles, definitions and requirements, hazard identification, safety insurance control, safety critical limits, monitoring and control, verification & validation, system log and documentation, are the essential steps towards safety medical robot. The initial implementation of HISIC in URObot for the safety enhancement is successful, it shows that HISIC can help to improve safety and effectively prevent hazards. More safety tests on HISIC are being conducted in our next experiments.

REFERENCES

[1] B.L.Davies. A discussion of safety issues for medical robots. In Computer-Integrated Surgery technology and clinical applications by Russell H.Taylor, Stephance Lavallee, Grigore C. Burdea and Ralpha Mosges. The MIT Press, 1995. PP287-196.

[2] W.S.Ng, C.K.Tan. On safety enhancements for medical robot. Reliability Engineering and System Safety. 54, 1996, PP35-45.

[3] L.D.Gowen. Specifying and verifying safety-critical software system. Seventh Annual IEEE Symposium on Computer-based Medical system. PP235-240.

[4] B.Connolly. Software safety goal verification using fault tree techniques: a critically III patient monitoring example. Proceedings of the Fourth Annual Conference on Computer Assurance, 1989. COMPASS '89, 'Systems Integrity, Software Safety and Process Security', 1989, PP18 -21.

[5] N.J.Dowler. Applying software dependability principles to medical robotics. Computing & Control Engineering Journal. October 1995. PP222-225.

0-7803-6465-1/00/$10.00 ©2000 IEEE

[6] D.L.Hamilton, M.L.Visinsky. Fault tolerance algorithms and architectures for robotics. Proceedings on Electrotechnical Conference, 1994. 7th Mediterranean. Vol. 3, PP1034 - 1036.

[7] B.W.Fei, C.K.Kwoh, W.S.Ng. The software design for a medical robot for urological applications. Proceedings of the First Joint IEEE BMES/EMBS Conference. Oct. 13-16, '99, Atlanta, GA, USA. PP896.

[8] W.S.NG. Robotic radiation seed implantation. Proceeding of the 18th IEEE EMBS international conference, Amsterdam, The Netherland, Oct/Nov 1996.

[9] J.Troccaz, S.Lavallee, E.Hellion. A passive arm with dynamic constraints: a solution to safety problems in medical robotics? International Conference on Systems, Man and Cybernetics, Systems Engineering in the Service of Humans. 1993.Vol.3. PP166 - 171.

[10] R.H.Taylor, H.A.Paul, P.Kazanzides, etc. Taming the bull: safety in a precise surgical robot. Fifth International Conference on Advanced Robotics, Robots in Unstructured Environments. 1991. Vol.1. PP865 - 870.

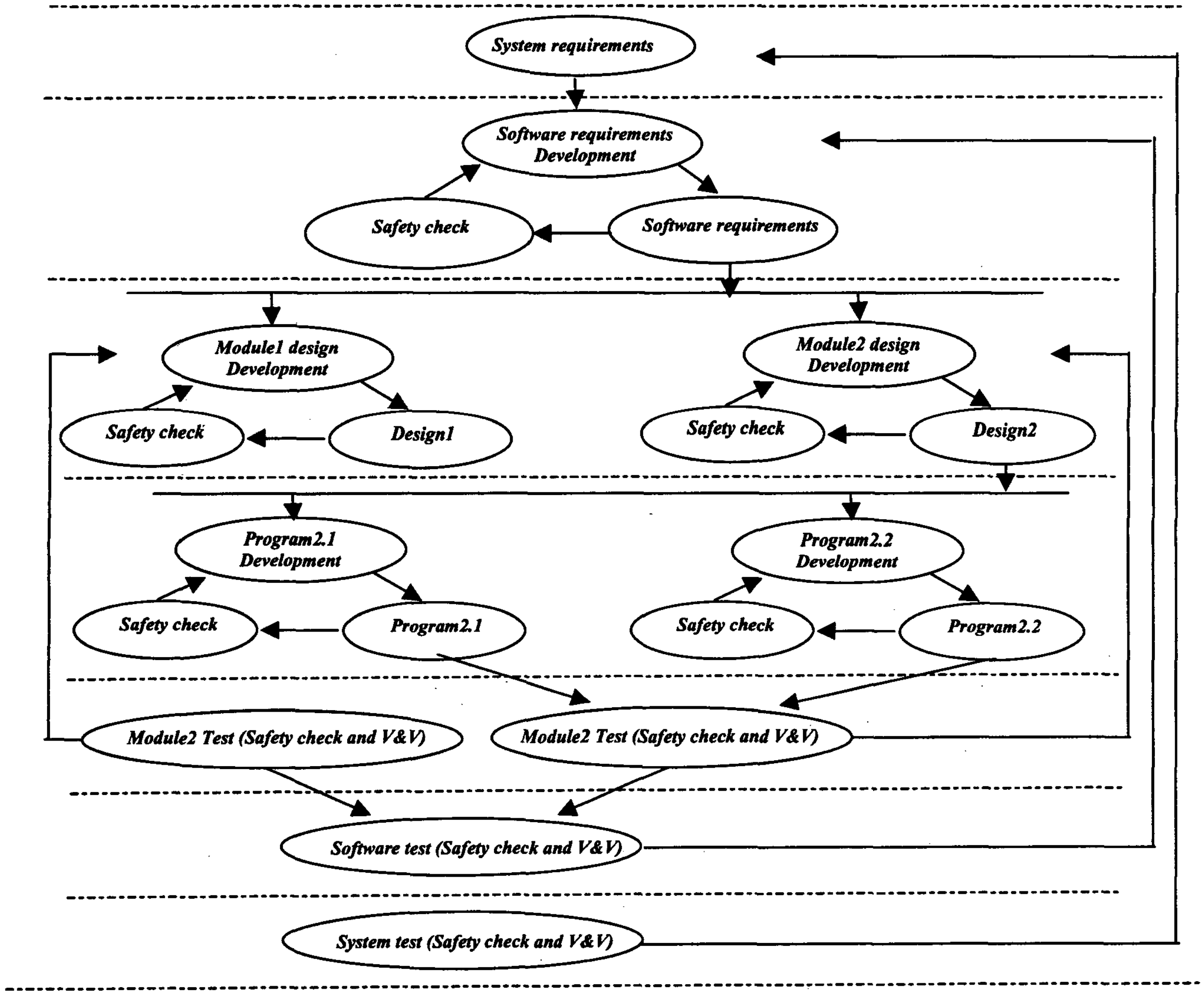
System requirements
Software requirements Development
Safety check
Software requirements
Module1 design Development
Safety check
Design1
Module2 design Development
Safety check
Design2
Program2.1 Development
Safety check
Program2.1
Program2.2 Development
Safety check
Program2.2
Module2 Test (Safety check and V&V)
Module2 Test (Safety check and V&V)
Software test (Safety check and V&V)
System test (Safety check and V&V)

Figure 2. The V&V and design method of the software for medical robot

0-7803-6465-1/00/$10.00 ©2000 IEEE