Medical Robotics

Safety

Marilena Vendittelli

*DIAG, Università di Roma “La Sapienza”*
requirements for miniaturization, safety, sterility, adaptation to changing conditions are peculiar to surgical robots and present a unique set of challenges in

- kinematic architecture
- electromechanical design
- sensing and actuation
- registration
- user interfaces
- system design

**Safety** is a primary and transversal design requirement
there exist several techniques to improve safety of medical systems, among these

- intrinsic safety: reduce the maximum level of risk by construction
- redundancy: increase amount of information, improve control
- reliability of design at electromechanical hardware and software level

intrinsically safe electromechanical components

- limited actuators velocity and power (only the “necessary” to accomplish the task)
- high reduction ratios (e.g., harmonic drives) when possible (lead to irreversible structures!)
- appropriate mechanical design (e.g., “mechanical fusible”) enables the tool to be quickly dropped when exchanged forces are excessive
- mechanical torque limiters mounted on the motor shaft: when a link collides with an obstacle during a motion, it stops moving while the motor shaft still rotates
- reliable parking brakes (electromagnetic brakes, for instance) mounted on selected joints prevent the robot from falling down under gravity effect
- gravity compensation may be fulfilled by a passive counterbalancing payload or by a full irreversible structure
- recently, robotic devices with variable actuation/transmission compliance
redundancy of sensors

- In image-guided surgery applications, both independent active and passive marker-based tools may improve the reliability of the tracking system.
- Cameras coupled with a computed tomography system may also increase safety by redundancies and improvements of information.
- To avoid time-consuming and potentially hazardous initialization procedures, use absolute encoders or a combination of:
  - Two relative encoders
  - Two resolvers (e.g., in SCALPP)
  - One incremental encoder and one absolute encoder (e.g., ROBODOC)
  - One incremental encoder and one potentiometer (e.g., SCALPP, NeuroSkill)
- One mounted on the motor shaft, the other at the end of the transmission chain for consistency check (redundancy avoids sensor failure but single point of failure should be avoided!)

![Diagram of a medical robotics system](image-url)
mechanical design

- to avoid the risk of wrenching or cutting wires, all the leads must be shielded and integrated inside the links of the robot arm
- mechanical joint limits increase safety by limiting the working envelope
- shocking or collapsing motions can be detected by checking the current loop in the motors; if the current increases abnormally, one can deduce that the robot has collided with an unexpected object and that the power has to be switched off
- dedicated CAD can be used to determine the optimal position of the robot in the operating room and w.r.t. the patient and the medical staff
- minimum number of dof necessary to suit the task, when possible (redundancy is however useful for obstacle avoidance and dexterity)
- link dimensions must be computed to preserve patient and clinical staff safety by just fitting to the required task workspace
- analytical methods for resolution should be preferred to numerical procedures
- wrist and shoulder singularity configurations should be avoided or rejected out of the workspace as much as possible (e.g., SCALPP)
electrical safety

- Dead Man Switch (DMS): requires that the user exerts a continuous positive action to allow the motion of the arm; by releasing the switch (generally a pedal), the robot is stopped or decelerated.
- Redundancy of components (watchdog, emergency switches, ...)
- A dedicated watchdog board allows checking the software process activity while position sensors and actuators should be wired on to different powering lines.
software safety

- the controller should be designed as concurrent processes dedicated to specific tasks: security (highest priority), Cartesian control, joint control, communication with peripheral units and sensors (one by units), HMI communication

- alternative solution: duplicate the CPU

- process activities are checked by a dedicated watchdog process

- software joint position and velocity limits lower than the mechanical ones (limit the workspace according to the operating mode)

- software thresholds on critical signal (exchanged forces, penetration limit, abnormal movements)

- variable time consumer procedures should be avoided (real-time programming!), sequential motions of the axes or smooth path should be preferred
comments

- redundancy increases system complexity possibly deceasing its reliability while increasing its cost

- depending on the occurring event and its hazard, several actions may be engaged
  – arm deceleration until the motion stops
  – current action cancellation
  – the system is placed in a waiting position with immobile arm until the problem is solved
  – emergency stop with power off; the arm and the hardware controllers are stopped; variables are reinitialized and power can be turned on as soon as the problem is solved
• proper safety design begins with a risk analysis

  – Failure Mode Effects Analysis (FMEA): bottom-up analysis, where potential component failures are identified and traced to determine their effect on the system; methods of control are devised to mitigate the hazards associated with these failures

  – is this system safe? depends on the task!

• $E$: error threshold
• $V_{\text{max}}$: maximum velocity
• $\Delta T$: control period
• $\Delta P_{\text{off}}$: robot joint stopping distance
- the FMECA (Failure Mode Effects and Critical Analysis) adds the criticality assessment: the severity (S), occurrence (O), and detectability (D) of the failure; a risk priority number (RPN) is computed from the product of these parameters, which determines whether additional methods of control are required.

- Fault Tree Analysis (FTA): a topdown analysis generally more appropriate for analyzing a system failure after the fact.

- In some cases, UML model have been used (e.g., safety analysis of the tele-echography system TER).
regulatory requirements

to maintain high quality standard various regulatory agencies have been put into place (e.g., FDA, UL), for standards development (e.g., UL, ISO, ANSI, ...), marks guaranteeing the respect of a set of norms (e.g., CE, HIPAA)

EU rules

- the ISO 9000 norm has been modified to include directives on medical devices included in the EU norm 93/42/CEE

- to obtain the CE mark (conformity to european norms), EN 46000 certification uses criterion necessary to classify medical devices in 4 risk classes: low, medium, high, very high

- classification of medical devices depends on
  - life-span use: from a few minutes (temporary) to several years (implantable)
  - invasiveness or noninvasiveness
  - surgical or nonsurgical use
  - activeness or inactiveness
  - vital or nonvital body parts concerned by the device
US rules

there are several categories within the FDA's regulatory system

- FDA Premarket Approval (PMA): the FDA's PMA process is designed to ensure the safety and effectiveness of Class III medical devices (those that support or sustain life or which present a potential risk for causing illness or injury to a patient)
  - extensive documentation of product design, testing, and manufacturing
  - thorough hazard analysis demonstrating that the product is single-component fail-safe
  - scientifically rigorous clinical trials performed under an FDA approved Investigational Device Exemption (IDE)—usage of the candidate system under carefully controlled and monitored conditions—with hypothesis testing and statistically analyzed end results
  - final review by a scientific advisory panel
  - strict regulations on manufacturing facilities, parts quality assurance, packing, storage, installation, and other aspects of overall product quality, . . .

the FDA will review a PMA submission within 180 days, but the process usually extends much longer due to the duration of the clinical trial and the requirement that clinical trials must be performed using the final version of the equipment being offered for premarket approval (ROBODOC and Cyberknife went through this process)

- FDA 510 K: for devices that can be shown to be substantially similar to already-approved devices
  - for many 510 K clearances, an FDA-approved IDE clinical study, much like that used for a PMA, may still be required; both the minimally invasive surgical robots ZEUS and da Vinci required clinical trials in order to obtain 510 K clearance from the FDA
**privacy standards and rules**

- Underwriters Labs (UL Listing): independent, nonprofit organization providing world-wide conformity assessment programs and services
  
  - the UL listing mark on a product indicates that the completed product has been tested by UL to recognized safety standards and found to be free from reasonably foreseeable risk of fire, electric shock, and related hazards
  
  - UL1740: safety standard for robotic devices in the medical context (surgery, diagnostics, drug synthesis and delivery, . . .)


- Health Insurance Portability and Accountability Act (HIPAA): passed by the U.S. government in 1995, compliance with HIPAA requires that all regulated entities must securely store, maintain, and transmit private health information
Bibliography

