Monitoring in the Control System of Robotized Medical X-ray Device for High Functional Safety

Milun S. Jevtić and Goran S. Đorđević

***Abstract*—Robotized medical x-ray system must operate as a high safety device during its lifetime. Therefore the control system should include a safety monitoring module. One such safety monitoring module is described in this paper. The module design is based on the microcontroller with increased dependability. The main task of the module is to monitor the correctness of the tasks performances during regular or irregular operation. It accepts all the commands and all the signals from the sensors, safety components and from inverters, to detect possible dangerous events. By monitoring and by exchange of the messages the safety module also detects malfunctioning in each of the motion control components. In the event of a failure, the module activates the process to guide the x-ray device into the safe state. Altogether, the controller and the safety monitoring module provide fully reliable and predictable operation of the robotized x-ray device.**

***Index Terms*—Control, monitoring, safety, dependability, robot, x-ray.**

I. Introduction

CURRENT trends in design of bulky medical devices for x-ray diagnostics are mostly relying on solutions developed for industrial robotics. Automated movements of heavy diagnostic tools such as x-ray tubes, collimators and bucky assembly reaching 100kg payload with sub-millimeter precision might be very useful in diagnostic procedures to replace presence of operator thus decreasing the level of accepted radiation and increasing the number of patients examined in the same time. An automated, preprogrammed movement of heavy medical equipment on the other hand rises a question of patient safety due to uncontrolled movements or collisions with objects in working area. This paper proposes one solution of this topic.

Global structure of x-ray device is given in [1] and corresponding block diagram of control system is given in Fig.1. This particular x-ray system has four degrees of mobility but in application it is a redundant 2dof system. It is designed to position and orient x-ray receptor, a bucky assembly, in a vertical plane while at the same time it aligns x-ray tube with collimator, which is source assembly, to it, allowing controlled distance between source and bucky.

The movements are produced with AC drives controlled with standard, low-cost inverters. Inverters are controlled digitally with standard PLC system. User interface is organized through touch panel and corresponding keyboards according to medical standards. It can be used for steering the unit into programmed positions in the factory or into the new positions stored during operation. Keyboards and touch panel are connected to PLC via multipoint RS485 connection. This connection is essential for commanding the motions controlled by PLC hence a Monitoring Safety Module (MS Module) is designed to monitor its healthy status. Its task is to ensure high functional safety of the system, i.e. its predictable and safe behavior even in the event of input error or malfunction in the control system. Therefore we have placed various sensors on the x-ray positioned to detect motion limits, collisions and failure of vital mechanical and electrical components. These sensors are not shown in the Block diagram in Fig. 1 but their function will be described in details later in the paper.

II. MS Module Functioning

The most important function of the MS module is monitoring of all processes that may impend the safe functioning of the device and navigating the system into one of the safe states defined during the design process. The MSM Module may function into two modes:

- Service mode, or S-mode,
- Functional Safety mode or FS-mode.

Entering the S-mode is allowed only to authorized personnel. In the S-mode service engineer may set up parameters of the system such as parameters for motion sequences, software limits of motions for each mobility axis, etc., and to start inherent procedures of interactive testing. Besides, the MS module does a safety monitoring in both of the modes of operation. However, in the S-mode it does permit motion beyond standard safety limits. This is to enable thorough testing of all hardware devices such as all limit switches, optical switches, bumper sensor, potentiometers, and force sensor for rope break detection.

M. S. Jevtić is with the Department of Electronics Faculty of Electronic Engineering, University of Niš, Serbia, 18000 Niš, A. Medvedeva 14 (corresponding author; e-mail: milun.jevtic@elfak.ni.ac.rs).

G. S. Đorđević, is with the Department of Automation Faculty of Electronic Engineering, University of Niš, Serbia, 18000 Niš, A. Medvedeva 14 (e-mail: goran.s.djordjevic@elfak.ni.ac.rs).

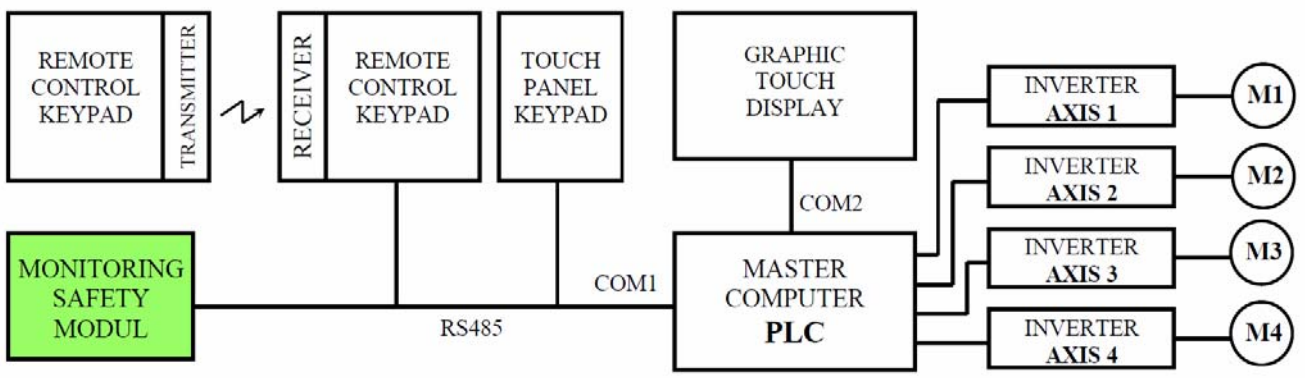

Fig. 1. Block diagram of control system in X-ray medical device.

The MS module in FS-mode gives high safety in the functioning of the x-ray positioning system through the following tasks:

- Upon power up it enables operation of the system i.e. overrides the Unconditional Stop (US) only after checking if there exist no single STOP condition.
- Monitors if all devices of the control subsystem are connected and properly functional via multipoint connection through perfect failure detector [3, 4]. This way we detect possible malfunctioning of the MS module and PLC control unit which are two vital components of the safety system.
- In periodic messages exchange the MS module recognizes motion command for each axis generated by PLC control unit and sends status word of the whole system from all sensors in the system and the correctness of motion outcome.
- Detects all hazardous events on time and undertakes proper actions to guide the system into the safe states.
- Generates US state for some hazardous events thus stopping all movements and override further manual commands from keyboards.
- Generates US state for some hazardous events thus stopping all movements and enables further manual commands from keyboards, if and only if hazardous event is not observed anymore.
- In the case of bumper activation event the MS Module stops the motion and it reverts the movement in the two axes of the system.
- Provides inherent self-testing procedures of the whole system.

III. MS Module Structure

The MS Module is designed as microcontroller system based on model of dedicated operative systems for real-time operation. Its architecture represents the block diagram in Fig. 2. It is based on microcontroller PIC 16F887 with integrated watchdog time and oscillator. This enables reliable detection of correct program execution as well as testing the watchdog timer itself. 24 digital inputs with optocouplers are grouped into three groups with the possibility of using separate power supply for each group. Nine DI can generate CPU interrupt with their active state. Conditioning of analog signals is also designed. They handles four analog signals from positioning potentiometers and one from force sensor for collision detection. Full range of AD converter is engaged with customized reference voltage generated as Vref+ and Vref-, as well as referent voltage for force sensor and positional potentiometers. USART and RS485 drivers are used to establish communication channel with PLC. Power unit also supply voltage to digital and analog circuitry. The PCB design digital and analog circuitry is carefully located to minimize the interference of digital noise to AD accuracy. Two relay outputs are with Normally-closed and Normally-open contacts.

Serial connection of relay active contact and two passive contacts of the Emergency Switch (ES) we define so called

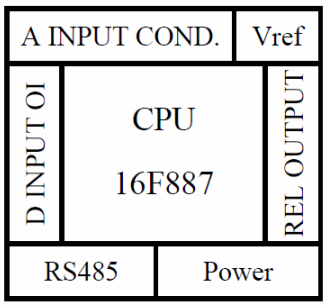

Fig. 2. Block diagram of MS module hardware.

safety loop which deactivates power supply to motor inverters. Active contact of the other relay output is used for power supply needed to deactivate electromagnetic brakes for all mobility axes. The MS module activates relay outputs thus enabling motion further controlled via PLC DO module, but only upon:

- Successful self-initialization,
- Establishing the communication with PLC,
- No active input demanding STOP action exists,
- Checking if a previous hazardous action did not produce persistent STOP condition requiring only service personnel for recovery.

Sensors used in this system are purposefully chosen. In the case of contact loss in wirings and connectors, or power loss, or sensor malfunction, the MS Module reverts to excess

situation assuming the motion should be prevented until service personnel overrides operator limitations.

The MS Module software is designed so to follow strict timing conditions. The communication is handled via interrupts and threads activation when a message is accepted in pre-specified timing interval. In periodically activated threads we handle groups of sensors, while those sensors that may result unconditional STOP are handled with highest priority.

IV. PLC TO MS MODULE MESSAGE EXCHANGE PROCEDURE

The message exchange between PLC unit and other slave units connected to a common half duplex communication channel is based on message sending from PLC as master unit and on reply from the slave units in specified time interval.

Basic message the MSM receives periodically every T*mes*=100ms is shown in Fig. 3. The beginning of the message starts with byte 0xFF, that cannot be part of the message, except at the end of the message as CRC code for error correction. This does not interfere correct detection of the message beginning as the byte 0xFF can be repeated several times. The message gives status information on axes movements. Based on that, the MSM validates motion correctness. One STOP/ START enable bit per axis marks the status of the motion per each axis thus leading to motion disable/enable signal to the inverters. This is not to be confused with safety loop STOP action in the case of emergency or Emergency Stop button activation.

If after time out T*out* > T*mes*, the MSM does not receive message from the PLC unit, all movements are disabled activating the STOP command. Upon the new message arrival the system functioning is enabled. Two consecutive errors in transmission-reception are detected as CRC Error and loss of communication is declared. In this case all of the movements are disabled and the system is navigated into STOP state.

The response of the MSM to each received message from the PLC unit follows the completion of the reception and shout timeout for line revert. The structure of the reply message is shown in Fig. 4. The message embodies limit switches status as well as software limits status and other errors detected during operation.

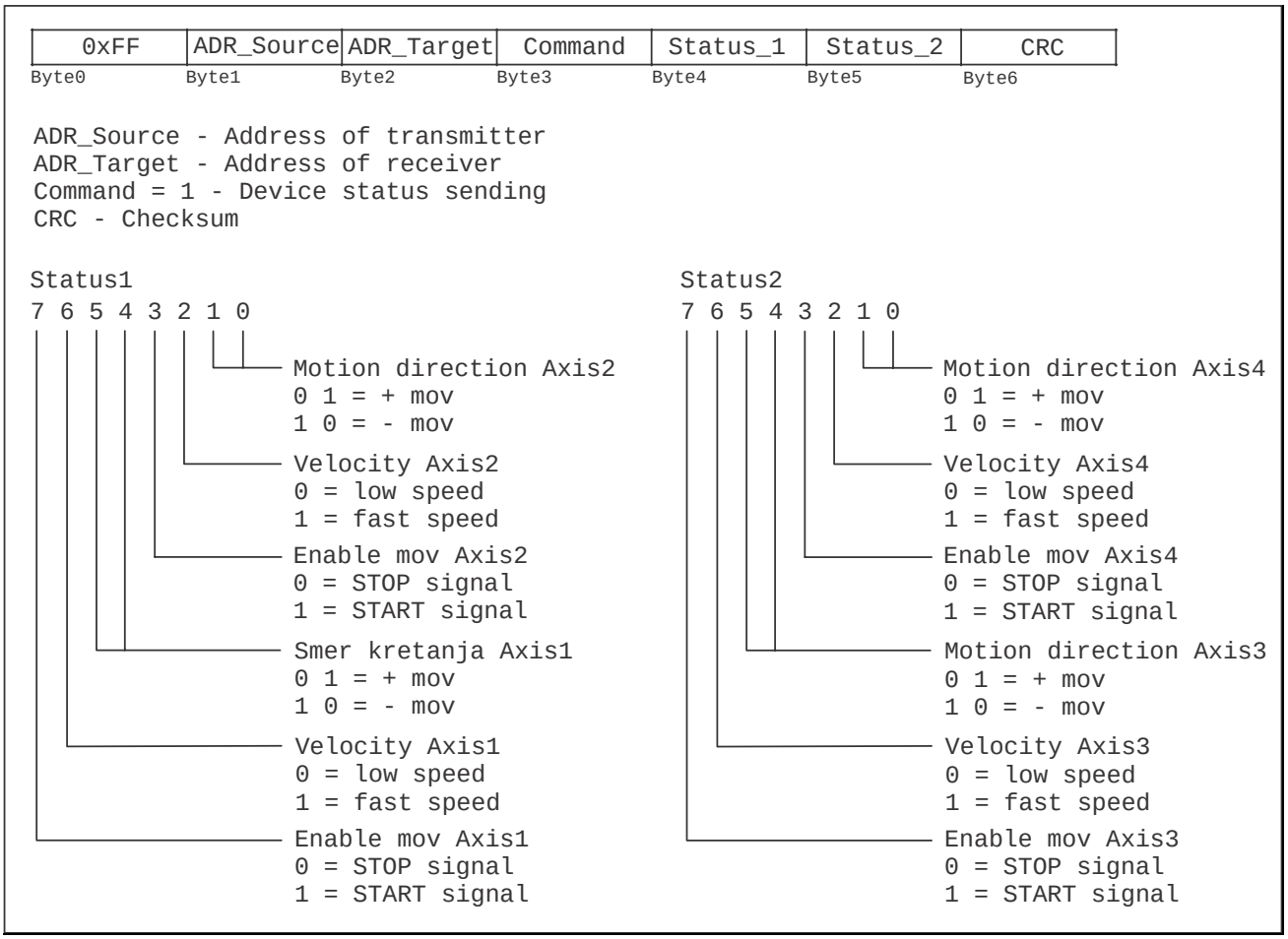

Fig. 3. Structure of PLC to MS Module Message.

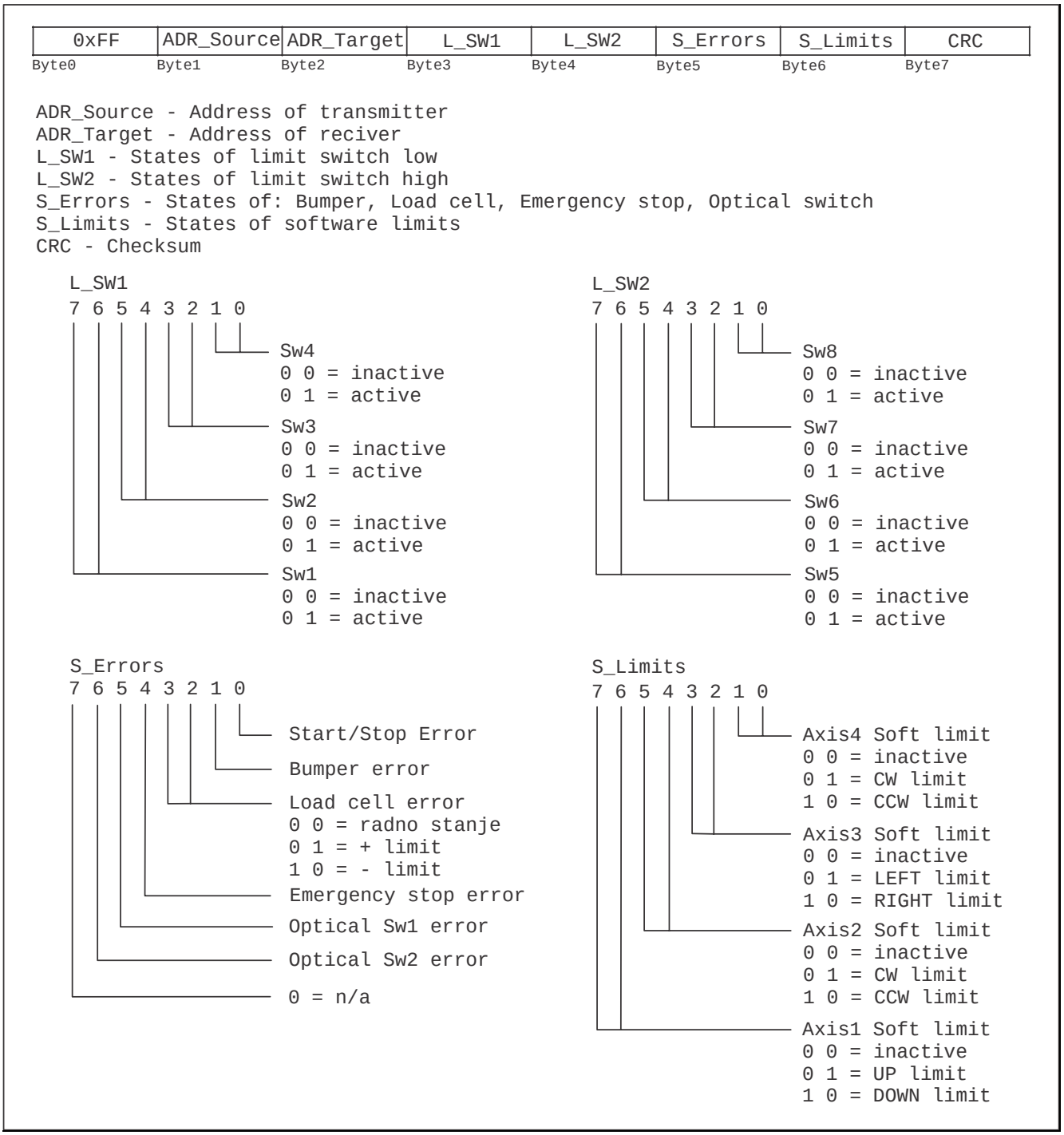

Fig. 4. The MSM to PLC Reply Message.

V. Errors Detected by MSM and MSM Activities in That Case

Sensors in the robotized medical roentgen device whose states are provided to PLC and MSM (**M**onitoring **S**afety **M**odule), are used to detect the errors and start the security activities as foollows:

A. Limit switch errors

If anyone of limit switches (*Sw1* to *Sw8*) is activated, the following MSM activity is performed:

- Unconditional safe STOP activated: OUT1_OFF, OUT2_OFF – all movements in system are suspended (the robotized medical roentgen device is stopped - system functioning is suspended by putting the releys outputs to off state);
- Refunctioning of the system is enabled by the service skilled worker.

B. Start/Stop error

This error appears if PLC has generated the command for the end of motion (MSM received the information through the

STATUS_1 and STATUS_2 that there is no motion) but still there is the motion. When MSM detects the move more than 1 cm after T*stopm* time (time to hold up because of inertia) after the end of move status is received, MSM starts the following activities:

- Unconditional safe STOP is activated – system functioning is suspended by putting the releys outputs to off state (OUT1_OFF, OUT2_OFF);
- Refunctioning of the system is enabled by the service skilled worker.

C. Bumper error

If the Bumper sensor is activated during the movement on *Axis_1* downward or on *Axis_2* in + direction (counterclockwise), PLC starts the inverse movement to safe position – back. At the same time, MSM reacts with following activities:

- Starts the timer Tbump (Tbump is the time needed for putting the robotized medical roentgen device to safe position – back by the movement in the opposite direction);
- If the bumper sensor is stil active after Tbump has passed, Unconditional safe STOP is activated – all movements in system are suspended;
- Refunctioning of the system is enabled by the MSM (Unconditional safe STOP is deactivated) when the Bumper sensor become inactive and there is no other STOP condition.

D. Load cell errors

The error is detected by comparing the state of the force sensor *Vr_FS* with the limit values.

- If Vr_FS < LDVr_FS is detected during the moving downward the Axis_1 and/or in – direction (clockwise) on the Axis_2 (low limit – minimal load with no colision and no rope break) with duration more than Tcoli (colision), MSM generates Unconditional safe STOP and sets the error Load_Cell_Error = 10;
- If Vr_FS < LDVr_FS is detected in any other situation with duration more than Tcb (rope break), MSM generates Unconditional safe STOP and sets the error Load_Cell_Error = 10 (rope unload);
- If Vr_FS>LUVr_FS is detected during the moving upward the Axis_1 (high limit – maximal load with no damage in mechanics), MSM generates Unconditional safe STOP and sets the error Load_Cell_Error = 01 (rope overload);
- The oscillations Vr_FS coused by starting and stopping the movement, or coused by other reasons, have no affect since they are in the range below the value limit;
- Unconditional safe STOP is deactivated (refunctioning of the system is enabled by the message fromPLC) if the condition that coused STOP doesn't exist anymore, and there are not other conditions that could activate STOP.

E. Emergency stop error

Activating the Emergency stop switch couses this error. MSM reaction is as follows:

- Unconditional safe STOP is activated: OUT1_OFF, OUT2_OFF – all movements in system are suspended (the robotized medical roentgen device is stopped);
- After the Emergency stop switch is deactivated, MSM cheks the state of the system. If no one sensor is active, i.e. there is no one condition to generate STOP, the functioning of the equipment is enabled – STOP is deactivated after received the message from PLC;
- If any of sensors is active, i.e. there is some error, system functioning is not enabled.

F. Optical SW1 error

If *Optical_SW1* is active, MSM reaction is as follows:

- After receiving the message from PLC, MSM analizes STATUS_1 and STATUS_2 to check if too low speed is established;
- If too low established speed is not detected after next received message (two successive), MSM activates Unconditional safe STOP;
- This STOP can be deactivated when Optical_SW1 become inactive and when there are no other conditions to activate STOP.

G. Optical SW2 error

If Optical_ SW2 is active during the movement of Axis_1 downward and/or Axis_2 in + direction (counterclockwise) MSM reaction is as follows:

- After time Tstopm activates Unconditional safe STOP (PLC stops the movement);
- This STOP can be deactivated when Optical_SW2 become inactive and when there are no other conditions to activate STOP.

H. Soft limits errors

If the positional potentiometer state is equal to the soft limit values or it exceeds the limit values for that axis, MSM reaction is as follows:

- Check in next received STATUS_1 and STATUS_2 if the movement is stopped (established to no move),
- If stopping the movement is not detected after next received message (two successive), MSM activates Unconditional safe STOP.
- If MSM detects the movement by the positional potentiometer state change for more than 1 cm after the time Tstopm passed from the Soft_limit detection, MSM activates Unconditional safe STOP,
- If the movement is stopped and there is no move after Tstopm, MSM doesn't make any action.
- If Unconditional safe STOP is activated, refunctioning of the system is enabled by the service skilled worker.

VI. Conclusion

Increasing hardware complexity in robotized medical devices for x-ray diagnostics inevitably means higher probability of hardware failure and corresponding functional

safety issues. We overcome this problem by complementary monitoring module for safety. This reduces chances for error and increases patient's security in the working area of the system. The functions of the MSM are designed to ensure reliable and always predictable operation of the system. All possible failures or combination of events are predicted and consistent actions are planned so to reduce the risks even in the case of errors due to mistakes in manual operation.

REFERENCES

[1] Svemir Popić, Srđan Mladenović, Goran S. Đorđević, "Final prototype of robotized x-ray device for medical applications", *Proceedings of INFOTEH-JAHORINA 2009*, Vol. 8, Ref. E1-9, ISBN-99938-624-2-8, pp. 824-828, March 2009. (in serbian)

[2] M. Božić, Miljan Milanović, "Control interface for universal x-ray positioner", *Proceedings of INFOTEH-JAHORINA 2009*, Vol. 8, Ref. E1-1, ISBN-99938-624-2-8, pp. 786-789, March 2009. (in serbian)

[3] Milun Jevtić, Bojan Jovanović, Sandra Brankov, Marko Cvetković, "One realization of fault detector in robot control systems", *Proceedings of INFOTEH-JAHORINA 2009,* Vol. 8, Ref. E1-7, ISBN-99938-624-2-8, pp. 814-818, March 2009. (in serbian)

[4] C. Fetzer, "Perfect Failure Detection in Timed Asynchronous Systems," *IEEE Trans. Computers,* vol. 52, No. 2, pp. 99-112, Februar 2003.