Fusion robotics safety; the emergency management system for the remote handling robots of JET

Zoulias I.D[1]., Preston B[1]., Howell R[1]., Houghton N[1]., Blackburn J[1]., Weerasooriya L[1]., Blake J[1]., Thomas J[1]., Hermon G[1]., Reece D[1].

[1] United Kingdom Atomic Energy Authority

KEYWORDS: Telerobotics Safety, Multidisciplinary safety design, Risk Assessment for robots, Human Factors, Functional safety, Fusion

ABSTRACT

The Joint European Torus (JET) is a large fusion experiment tokomak. Over the last 27 years of its operations, it has been remotely maintained with a telerobotic system – the JET Remote handling system. The JET Remote handling system comprises two 11+ meter articulated robotic booms which can transfer robotic systems and tools in the heart of the JET machine for intricate operations. One such telerobotic tool, the MASCOT 6 tele-manipulator is a 14-axis local-remote telerobotic device that enables precise operations with high fidelity of feedback to the operator. Using this remote handling system, operators have performed over 35000 hours of operations using over 950 tools for handling, cutting, bolting, welding, grinding, inspecting, and cleaning within the JET tokamak. The JET Remote handling system is being upgraded to address obsolescence and reliability issues and to prepare the system for the next phase of remotely decommissioning the JET machine. Here we present the new safety system for the JET remote handling system that ensures human operator safety and asset protection across the entire system and during all project phases from development to decommissioning. We describe the challenges of integrating to and updating a legacy safety system, the innovations afforded by new safety technologies, and the architectural and operational recommendations for large robotic systems with integrated humans in the loop. After describing the overall safety infrastructure, the risks from the remote handling system, the intended operations, and the safety objectives, we focus on two main safety technical challenges.

First, we describe how an active zoning system was developed to adapt to the agile operation of the JET remote handling system without compromising safety. The physical rearrangement of the JET remote handling system within and between buildings means that different parts of the JET remote handling system need to be active at different times, and the safety objectives and identified risks require integration between working systems. We detail the operations that required an active zoning system, we describe the design and its implementation, and discuss the human factors considered and the human-interfaces created to aid with the understanding of the state of a complex and agile system by the operators. This includes the integration with non-safety control systems to aid in overall operability of the remote handling system by the operational team. Second, we describe the risk analysis and the full risk mitigation and engineering measures for the MASCOT 6 telemanipulator that poses a constant risk to the human operator; telemanipulators are always in collaborative mode. We discuss the hazard identification and the safety functions that were designed, their implementation with new hardware, and the challenges and recommendations on implementing safety on telemanipulators. We frame this work with the recommendation of ISO 13849 and ISO TS 15066 and present how the working system was designed according to these standards. We conclude this work with a presentation of data from 1000 hours of operation post commissioning and present our findings from the early operational feedback and the recommendations on safety design for large telerobotic installations.

1 INTRODUCTION

1.1 JET Remote Handling System

The JET Remote Handling System (RHS) is a platform for a diverse range of remote handling operations inside the JET Tokamak [1]. The design philosophy has resulted in a modular remote handling core system where the main elements are not required to change for each application. The system comprises two booms which access the Tokamak through the main horizontal ports at Octants 5 and 1 (see Figure 1). The control systems and network infrastructure extend to the RH Control Room, from where all operations are controlled (see Figure 1C). The Octant 5 Boom (Figure 1A, left side) carries the remote Mascot telemanipulator, part of a dexterous, force reflecting local-remote manipulator system. The Octant 1 Boom (Figure 1A, right side) delivers interchangeable multi-drawer modules, or end effectors which carry tools and components to the in-vessel work area.

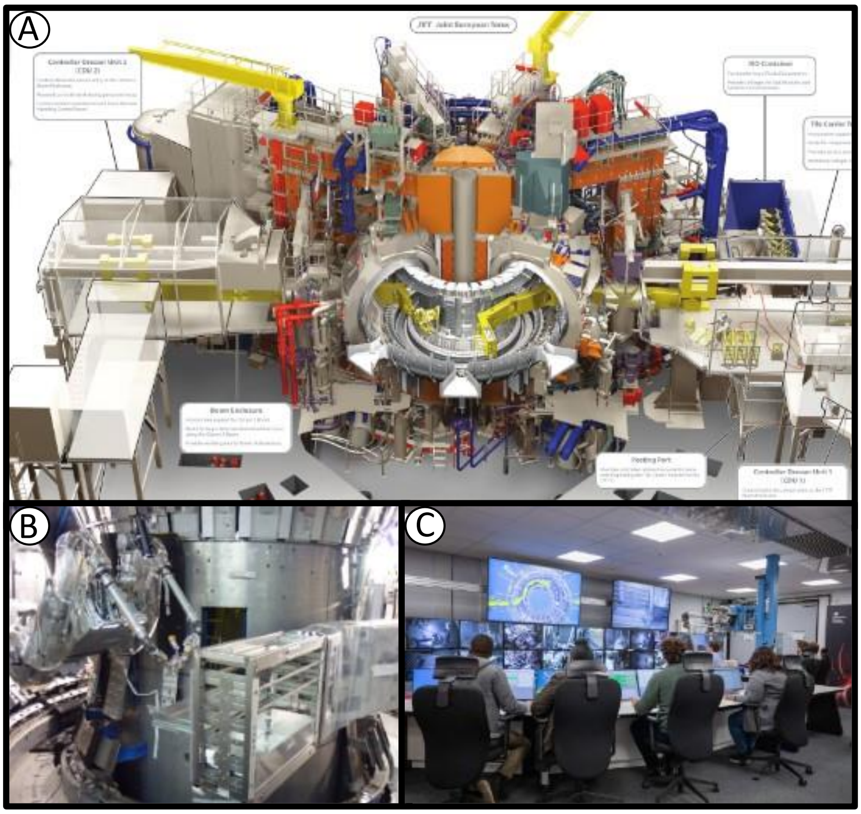

A
JET Joint European Torus
Controller Dresser Unit 2 (CDU 2)
Boom Enclosure
Docking Port
Controller Dresser Unit 1 (CDU 1)
B
C

Figure 1. *JET Remote handling system. A) The two booms with Mascot deployed in the JET machines during remote operations. B) Close up of the Mascot and Boom during training operations in the mock-up facility. C) Control room showing users of the JET RHS and the Mascot operator, using the local manipulator (right).*

1.2 Legacy Emergency Stop System

The Legacy Emergency Stop System (ESS) is a centralised safety system designed in early 2000s. Its function is to bring various JET RHS systems to a safe state in response to inputs from Emergency Push Buttons (EPBs) and other systems/devices. The legacy ESS consists of three central Emergency Stop Relays (ESRs); the High-Level Relay operates an independent loop and can cut off the incoming power to all RH cubicles. The remaining two relays function at a higher level related to the two zones of interest, Octant 1, and Octant 5.

During normal operation the outputs of the central ESRs allow RHS operation via energised contactors. To reconfigure the JET RHS, some outputs can be overridden via switches or relays to de-energise contactors regardless of the outputs of the ESRs. If any of the emergency stops or other emergency devices are actioned, the corresponding ESR stops receiving that input. Failure to receive one input within an ESR will open all the outputs of that ESR and therefore stop providing all the output signals or supplies to the corresponding systems.

The existing ESS, whilst functional, cannot be assigned a Performance Level (PL) according to ISO 13849[2]. Several issues exist; some EPBs are out of reach whilst others are within locked enclosures (contrary to ISO 13850[3]). Resetting the system is also nonconformant to ISO 14118[4]; systems can automatically reset with motion enabled on release of an EPB, rather than having a reset/restart function. Furthermore, expanding the existing system to include new functions and equipment is very complex due to its architecture.

1.3 JET RHS and EMS Upgrade

The design of the JET RHS is over 30 years old. After more than 35,000 hours of in-vessel operations and 80,000 hours of training operations, significant elements of the JET RHS are no longer supportable, and continued operation cannot be guaranteed. The JET RHS is upgraded to address the systems obsolescence issues and to ensure there is a high level of RH systems availability during remote operations for the next decade of sampling and decommissioning of the JET Tokamak. To this end, along with the upgrade of the JET RHS, the legacy ESS is updated to a compliant modern system that is fit for purpose for the diverse remote handling operations.

2 EMERGENCY MANAGEMENT SYSTEM DESCRIPTION

2.1 EMS Design Description and Architecture

The Emergency Management System (EMS) has been designed to upgrade the legacy ESS. The primary safety function of EMS is to communicate emergency stop and reset commands to all systems and sub-systems of the JET RHS. Beyond this, the EMS builds upon the legacy ESS by providing a full management solution for the emergency stops, emergency functions, and configuration management of the JET RHS. This is achieved through three main functions.

Firstly, the EMS supports the JET RHS multi-configuration setup in a safe and controlled manner, using a build-for-purpose safety rated zoning system. This function allows the operational of the system in all permissible configuration and the safe maintenance and commissioning of the JET RHS. Secondly, the EMS is designed to provide the framework for propagating sub-system safety functions of the JET RHS subsystems, where the sub-system safety functions are within the scope of each sub-system (for example, see Section 3, Mascot 6 Safety System). Finally, the EMS provides a real-time display of the entire safety system allowing management of configuration and monitoring of normal and abnormal situations of the system.

The EMS architecture, shown in Figure 2, is divided in four zones. The main EMS cubicle, installed in the RHCR Zone, acts as the central safety hub for all RH equipment and end effectors/attached equipment (whilst in use). A single reset button within the RHCR enables a controlled and deliberate reset of the entire EMS. This reset button resets all integrated sections and systems of the plant, however, affect any isolated sections of plant; during maintenance, further local reset buttons shall be online in their respective zones to enable local resetting of any EPB pressed during commissioning and maintenance activities only.

The EMS network architecture is connected in a star configuration, with a PILZ® PSS4000 PLC header at the centre (acting as the central hub, see Figure 2). An identical header module is installed on each major section of plant to act as the zone hub, as detailed: RHCR, Octant 1, RHMF, Posting Port, IVTF, and the Mascot local and remote station. These modules hold the high-level functions required for the configuration of the system. Where a permanent connection is required, a PILZ® PSS4000 I/O header is installed which controls the local cubicle safety systems. The overall JET RHS hazard identification and risk assessment required a performance rating of the EMS system to PLd (ISO 13849[2]), and the system has been designed to this performance level.

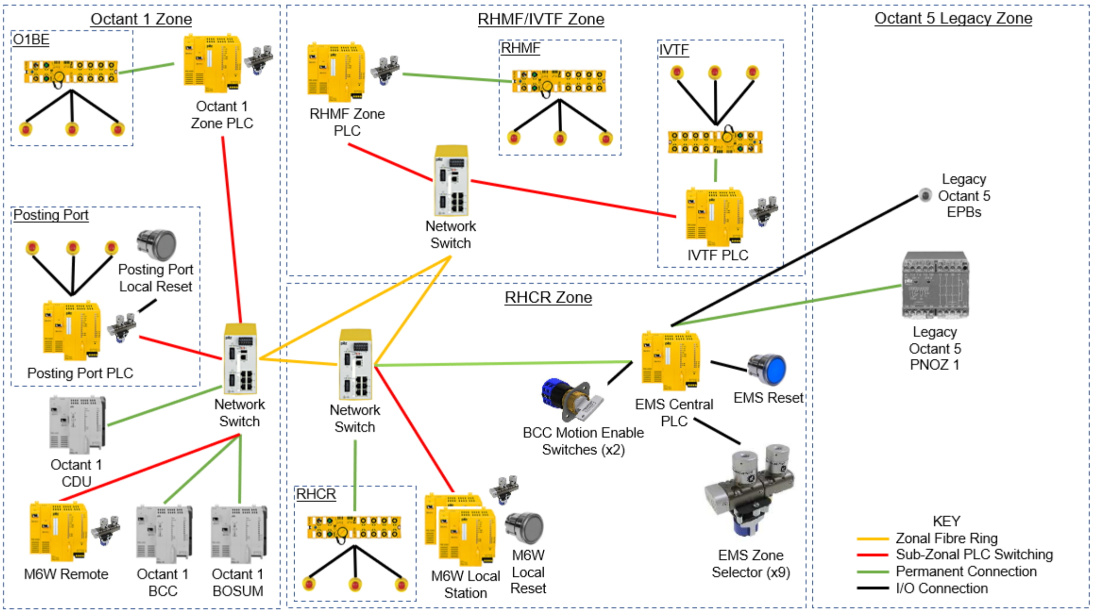


***Figure 2**. Architecture and topology of the EMS system. The EMS system is divided in 4 main zones; the Remote Handling Control Room (RHCR) Zone which is the main control area, the Octant 1 zone, the maintenance and training facility zone, and the Legacy Octant 5 zone. Each main zone can have sub-systems within that have their own zone (e.g. the posting port zone within the Octant 1 main zone). The legacy Octant 5 zone allows temporary integration with a part of the system that is scheduled to be updated in the coming years. Sub-systems within a zone can be zoned-out to allow for configuration of the system (shown in red links). Other sub-systems are permanently connected to the EMS (shown in green links).*

2.2 Zone Switching

The zoning of JET RHS sections is designed to provide the EMS architecture with a modifiable span of control where required. An EMS zone is an area which contains different sub-systems (e.g. Octant 1 or Octant 5). All EPBs within a zone will initiate an emergency stop on all systems connected to that zone. For example, if an Octant 1 EPB is activated the Octant 1 Boom and any tools connected to it will be stopped. A zone can be configured to either operate on its own (local mode) or as a part of the wider EMS (remote mode).

To enable RH operators to reconfigure the system, a bank of reconfiguration switches is installed in the RHCR. The purpose is to allow local transport, commissioning, and maintenance of zones of the JET RHS that would cause major disruption to operations if the entire JET RHS was disabled. When a boom enclosure is moved between buildings for operations in JET, the associated control cubicles, boom, and all other services are offline for weeks before being reconnected. To allow safe continuation of operations in the rest of the system, a zone can be 'switched out' from the EMS. Each switch effectively integrates or isolates a zonal PLC header, such as Octant 1, and its associated sub-systems. As soon as the zone is ready for operations, it is 'switched in' to EMS.

As soon as the switch has been activated to isolate part of the JET RHS, an emergency stop is actioned. If there is a mismatch between the state of the connection and the switches, i.e. a system is connected when it shouldn't be, or a system that should be connected isn't, a fail-safe operation is actioned where no machinery on the network can start until the discrepancy is resolved. The EMS system can be restarted only once it is properly reconfigured. Isolated zones of EMS can operate locally, but strictly for maintenance and commissioning only.

The physical switching in and out of a zone is carried out using a Fortress key system. This system provides safety-rated inputs to the EMS software, enforcing a fail-safe mode should a failure in the switching procedure happen. Interlocking is a safe method of controlling two or more interdependent operations which must take place in a pre-determined sequence. The control of the switching process is required to ensure personnel safety during the process and provide the system with safety-rated interlocks to prevent unwanted machinery operation. To facilitate true multizone capability, each zone has its own separate intervention key. These keys are kept in a locked key blister, access to which is controlled. Control of the intervention keys ensures process security and prevents unauthorised alterations to the EMS. An example of the procedure is shown in **Table 1** and Figure 3.

***Table 1**. Step by step zoning out process*

Step	Action	Rationale
1	EMS cubicle powered down	All switching of zones must be carried out in a powered down state.
2	Switch out authority granted	Responsible officer unlocks the key press, retrieves the required Zone Intervention Key (orange in **Figure 3**), and locks the key press.
3	Zone interlock key released	The Zone Intervention Key mechanically unlocks Zone Interlock Key (blue in **Figure 3**) and breaks the interlock signal to the EMS
4	Corresponding zone switched out	Zone Interlock Key inserted into a local key exchange, releasing a Zone Control Key (green, **Figure 3**) and breaking the local interlock signal to the EMS.
5	Ops RO takes possession of control key	The Zone Control Key is locked in the key press to complete the switch out process.
6	Switch out complete	EMS powered up, system self-checks are carried out to ensure all zone switches are correct and corresponding. RH plant operational.

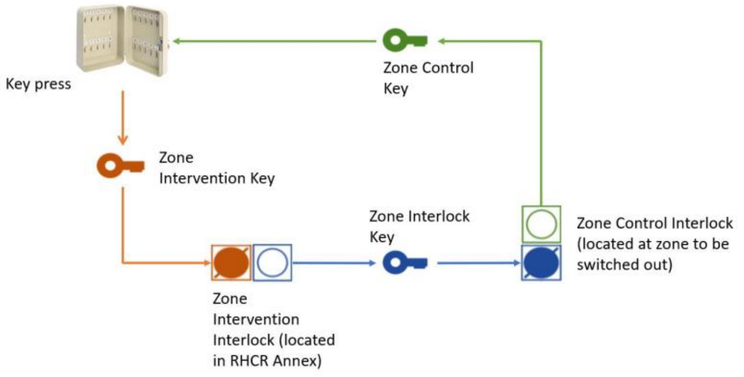

Key press
Zone Control Key
Zone Intervention Key
Zone Interlock Key
Zone Control Interlock (located at zone to be switched out)
Zone Intervention Interlock (located in RHCR Annex)

***Figure 3**. Key exhance process for zonining out. The reverse of the process is followed for zoning in.*

2.3 HMI

2.3.1 Reset button

The main physical interface in the RHCR besides the zoning system and the EPBs is the reset button. This is a blue illuminated button with 4 states: 1) on, 2) slow flashing (1Hz), 3) fast flashing (5Hz), and 4) off. The state of the reset button indicates to the operators the state of the EMS system as follows. “On” indicates that the EMS system is functioning as intended. “Slow flashing” indicates that the EMS system is ready to reset (by pressing the reset button). “Fast flashing” indicates that there is an activated trip on the system (e.g. a pressed EPB) and the system cannot be reset, but there is no fault. “Off” indicates that the EMS system is inactive or has a fault.

Each local reset button operates in the same way when the local system it is connected to is in Local mode. When in Remote mode, the local reset button is off, indicating that it is not active, and any interaction with the button is completely ineffective to the EMS.

2.3.2 EMS HMI

The HMI gives an overview of the EMS system to operators, maintainers, and commissioners. It shows the entire system, allowing a user to see which areas are connected and if and where there are any faults or EPBs depressed. It also shows the state of the RHCR reset button as a virtual quick indicator of the system state. The HMI is a read-only system that is connected to the PILZ® SafetyNET p network via a read-only data diode.

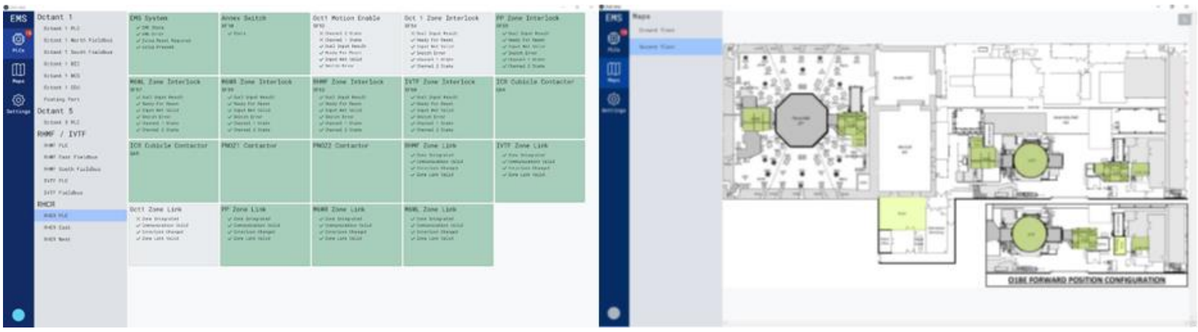
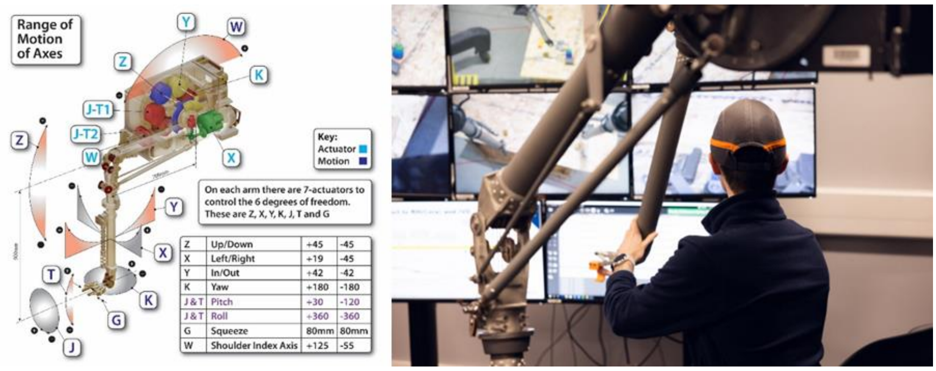


Figure 4. The EMS HMI. On the left, the system is healthy with the Octant 1 zoned out (zone out parts shown in grey). On the right the map of the relevant areas is shown, whilst the HMI indicates a fault with the EMS system (the virtual reset button at the bottom left of the screen is grey).

3 MASCOT 6 SAFETY SYSTEM

3.1 Contact with Operators and Safe Speed Monitoring Function

The Mascot 6 system is the upgrade to the JET Mascot 4.5 local-remote telemanipulator [1]. The system can be seen in **Figure 5**. As it is a telemanipulator, the local side of the Mascot 6 system is in constant physical contact with the operator during remote operations. To protect the operator, a risk assessment and input from ISO TS 15066[5] was used to define the contact forces and resulting speeds of the Mascot 6 system beyond which the system would not be allowed to operate. The PILZ® PSSu K F EI speed modules were used in the mascot safety in conjunction with a Kübler® Sendix 5883FS3 safety rated encoder to monitor and action overspeed events of the manipulator. After risk assessment, only the axis that contribute to major motion of the arm were shown to require risk mitigation. Based on the above, an end effector speed of 1000 mm/s was decided to be used as the limit of the device. This is an upgrade of safety to the Mascot 4.5 system that had no safe speed monitoring.



On each arm there are 7-actuators to control the 6 degrees of freedom. These are Z, X, Y, K, J, T and G

Z	Up/Down	+45	-45
X	Left/Right	+19	-45
Y	In/Out	+42	-42
K	Yaw	+180	-180
J & T	Pitch	+30	-120
J & T	Roll	+360	-360
G	Squeeze	80mm	80mm
W	Shoulder Index Axis	+125	-55

***Figure 5**. Mascot 6. Left, mechanical architecture and joints. Right, close up of Mascot 6 user in operations.*

3.2 Kinematics and Analytical workspace solution

The kinematic solution ensures that the target end-effector velocity will never be exceeded, whilst allowing motion just below target velocity homogeneously in the entire workspace. This calculates the X, Y, and Z joint velocity and limits the end-effector speed the target velocity of 1000mm/s. The end effector velocity can be found as $v = \sqrt{\dot{x}^2 + \dot{y}^2 + \dot{z}^2}$, *where* $\dot{x}$, $\dot{y}$, and $\dot{z}$ are the velocity components as defined below:

$$\dot{x} = -l_z \sin \theta^{\circ}_z w_z - l_y \sin(\theta^{\circ}_z + \theta^{\circ}_y)(w_z + w_y) + l_y ((1 - \cos \theta^{\circ}_x)(\cos \theta^{\circ}_y \sin \theta^{\circ}_z w_y + \sin \theta^{\circ}_y \cos \theta^{\circ}_z w_z) + \sin \theta^{\circ}_x \sin \theta^{\circ}_y \sin \theta^{\circ}_z w_x)$$

$$\dot{y} = l_z \cos \theta^{\circ}_z w_z + l_y \cos(\theta^{\circ}_z + \theta^{\circ}_y)(w_z + w_y) - l_y ((1 - \cos \theta^{\circ}_x)(\cos \theta^{\circ}_y \cos \theta^{\circ}_z w_y - \sin \theta^{\circ}_y \sin \theta^{\circ}_z w_z) + \sin \theta^{\circ}_x \sin \theta^{\circ}_y \cos \theta^{\circ}_z w_x)$$

$$\dot{z} = l_y(\cos \theta^{\circ}_x \sin \theta^{\circ}_y w_x + \sin \theta^{\circ}_x \cos \theta^{\circ}_y w_y)$$

with, l_i, θ°_i, and w_i the corresponding link length, joint angle, and velocity for the i-th joint of Mascot, respectively. However, this could not be programmed in the PILZ® PLC as a safety function. This is due to the joint speed not being a speed module safe variable and the complex mathematical operations within each safe cycle. Instead, an analytical solution was developed that produced joint speed limits that bound the maximum velocity within the acceptable range, using the kinematic equations in the analysis rather than the runtime. The analytical solution exhaustively searched discreet points in the workspace for the resulting worst-case velocity given a set of joint speed limits. This produced the following conservative floor for joint speed limits: X: 37.5 RPM, Y: 78.97 RPM, Z:30.84 RPM. These limits can cause the system to trip in end-effector velocities well bellow the maximum of 1000 mm/s, and don't allow end effector speeds larger than 1000 mm/s anywhere in Mascot 6's workspace. These limits are being tested in operations to ensure safe and efficient operations, with the option to increase these limits if normal use leads to false trips (i.e. the limits impede normal operation).

4 CONCLUSION - FEEDBACK FROM OPERATIONS

The new EMS system has been in operation for over 900 hours to stress test the updates to the JET RH system. The following operator feedback provided as a conclusion to this report with recommendation for improvement.

4.1 HMI feedback

Having an immediately available status is a significant improvement. EMS is normally a sleeping service and only infrequently used to understand the status, especially when equipment and cell configurations are changing within a complex overall system. Improvement action identified to provide a simpler visual schematic display for the operators' team and with an option for system maintainers to toggle the view for all technical details.

4.2 Single reset button

This is the heart of the system when in an operational state. During design evolution, the button location moved from an annex to a central area of the control room at operators' request. It provides an "at a glance" visual status of the EMS system from the entire control room. In the event of a fault condition, local or remote button press or other event, provides immediate preliminary feedback. Single press resets the entire system, with immediate visual feedback works well. This is a major improvement in the efficiency from ESS to EMS.

4.3 Flashing indicator feedback

The most beneficial aspect from an operator's point of view. Its working principle is highly simple to train to 20+ operators and more importantly retained by personnel without periodic refresher training.

5 REFERENCES

1 Skilton R., Hamilton N., Howell R., Lamb C., Rodriguez J., *MASCOT 6: Achieving high dexterity tele-manipulation with a modern architectural design for fusion remote maintenance*, Fusion Engineering and Design, Vol. 136, Part A, 2018, pp 575-578, https://doi.org/10.1016/j.fusengdes.2018.03.026.

2 International Organization for Standardization, *Safety of machinery - Safety-related parts of control systems*, 13849, Part 1, 2023.

3 International Organization for Standardization, *Safety of machinery - Emergency stop function - Principles for design*, 13850, 2015.

4 International Organization for Standardization, *Safety of machinery - Prevention of unexpected start-up*, 14118, 2017.

5 International Organization for Standardization, *Robots and robotic devices — Collaborative robots*, 15066, 2016.