1.4 – Impact of security on safety

Practical guidance – cobots (collaborative robots)

Author: Panayiotis Karachristou and John Clark, University of Sheffield

This document specifies the security measures and security configurations which users and IT administrators are required to apply in order to ensure the confidentiality, integrity and availability of a collaborative robot (cobot) system at an arc-welding company, hereinafter referred to as ***organisation***.

This acts as a key policy document that all staff and contractors must be familiar with and outlines the actions and guidelines that all users must obey. The policy offers guidelines and guidance to the managers within the organisation on the appropriate use of any cobot equipment, research technology equipment, information processing, e-mail, internet connectivity, voice mail, facsimile and any potential technology tools.

The policy specifications and restrictions set out in this document shall extend to: network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations and all other methods used to communicate information and ideas through all hardware, software and data transmission mechanisms. All staff or temporary workers at all locations and contractors working with the system as subcontractors must abide by this policy.

After the policies are applied certain aspects of the organisations aspects should be maintained and all forms of information and related assets should be appropriately protected.

These include:

- **Confidentiality** is the property of keeping private and confidential information that should be kept as such and making sure that is not in any way disclosed to unauthorised individuals, entities, or processes.
- **Integrity** is the characteristic of being accurate and complete.
- **Availability** is the property of being available and accessible by an approved entity whenever it is required.

Scope

This policy document defines common security requirements for all personnel and systems that create, manage, store, access, process or transmit information. This policy also applies to information resources owned by others, such as contractors of the organisation, entities in the private sector, in cases where the organisation has a legal, contractual or fiduciary duty to protect said resources.

In the event of a conflict, more restrictive measures shall apply. This policy applies to the cobot system consisting of various hardware, software, communication equipment and other devices designed to assist the organisation in the creation, receipt, storage, processing and transmission of information. This description includes equipment connected

to any system domain or LAN, either hardwired or wireless, and includes all stand-alone equipment installed by the organisation at its office or remote locations.

User/employee responsibilities

The very first line of cybersecurity defence in any system is the individual user. The users of the system are responsible for all aspects of any data and tools that may come to them in any format. The organisation is responsible for coordinating ongoing training programs in order to educate all users of these requirements.

Employee requirements

1. **Challenge unrecognised personnel.** It is the responsibility of all staff of the organisation to take positive action to ensure physical security. If a member of the staff encounters an unrecognized person at a restricted office location, they should challenge them as to their right to be there. Any person visiting the organisation should sign at the front desk, showing a form of identification. In addition, they should be provided with a visitor badge. All other personnel should be employees of the Company wearing their respected badges. Any person in question who fails to respond appropriately should be immediately reported to the supervisory staff.
2. **Use of cooperate equipment**. Only computer hardware and software owned and approved by the organisation may be connected, installed or mounted on the organisation's equipment. Only software that has been certified for corporate use by an organisation can be installed on corporate equipment. Personal computers or equipment provided by the company shall be used exclusively for business purposes.
3. **Retention of ownership**. Any software programs and documents produced or created by staff, consultants or contractors for the benefit of the organisation are the property of the organisation, unless they are subject to a contractual arrangement. Nothing in this section refers to software purchased by employees of the company at their own expense.

Prohibited activities

Personnel are prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document.

1. **Crashing software.** Crashing the cobot software. It is strictly illegal to deliberately crash an information system. Users may not be sure what caused a device to crash, but if it is revealed that the crash happened as a result of a user action, a repeat of that action by that user can be perceived as a deliberate act, this is strictly prohibited.
2. **Hacking.** Trying to hack into an information system or circumvent a security function. This involves running password-cracking programs or sniffer programs, and trying to override file or other access permissions. The use, or the attempt to introduce, malicious code into the system like viruses or Trojan horses.

   Exception: Approved support staff or others approved by the organisation may test the durability of the system.

3. **Software use.** The use of personal software shall be forbidden. All software used must be certified by the organisation. Breach or attempt to breach the terms of use

or licence agreement of any software product used by the organisation is strictly prohibited. It is strictly forbidden to participate in any activity for any reason that is unlawful or does not adhere to the policies, procedures or commercial interests of the organisation.

4. **System use.** It is strictly forbidden to engage in any activity for any reason which is illegal or contrary to the policies, procedures or commercial interests of the Company.

Reporting software/system malfunctions

Users must notify the required personnel when a program/cobot/system does not seem to be operating correctly. A malfunction whether accidental or intentional poses a security risk to information as well as a safety risk to the personnel. If the user, manager or supervisor of the user suspects an infection from a computer virus, the computer virus management protocol should be followed, and the following steps taken immediately:

1. Stop using the device/cobot
2. Do not execute any commands, including data saving commands.
3. Do not terminate any running software.
4. Do not turn off the device.
5. Physically disconnect the device from any network to which it is connected, if possible.
6. Inform the relevant personnel as soon as possible.
7. Make notes of any unusual behaviour of the system, including the time they occurred (e.g. unusual responses to commands, any screen messages/errors, unexpected disk access)
8. Take notes of any changes in hardware, software that preceded the malfunction.
9. Don't try to remove the suspected virus.

Reporting security incidents

Each employee is responsible for reporting any suspected safety incidents to the appropriate supervisor or security individual on an ongoing basis.

Any person allowed to access an information resource (database) or otherwise known as a user shall be responsible for the day-to-day, security protection of that resource. Users must notify immediately of any incident or breach of a security policy. Users should notify any potential security issue either to their immediate boss or to their department manager.

Any security incident reports should be escalated as quickly as possible. Each incident should be analysed carefully and efficiently to determine whether and what changes to the existing security structure are needed.

All of the incidents and their mitigations must be documented.

Transfer of sensitive/confidential information

In the occasions where confidential or sensitive information is received by another individual while during the course of official business, the recipient must maintain the privacy and sensitivity of the information under the terms given by the provider of the information. The sensitive nature of the data maintained by the organisation shall be

recognised by all employees and all data should be kept in strict confidence. Any deliberate disclosure of information is a violation of the policy and may result in legal action.

Building security

The organisation should provide access in the building in a secure manner. Understandably, each site has its own unique aspects, in terms of building ownership, safety requirements, entrance access and more. These aspects should be taken into consideration but the organisation is required to make sure that every section of the building follows the following security requirements in some way.

1. The reception area shall be staffed at all times during working hours.
2. A security code system controls the entrance to the building during non-working hours.
3. Only staff members that should be allowed should be given the security code to the entrance, disclosure of this code to anyone else should be strictly prohibited.
4. These codes should be renewed periodically as well as when a staff member is terminated access to that entrance. The update should be done in a secure manner, e.g. it is emailed to the employees that require it, or an app is developed for this purpose.
5. The reception area is staffed at all times during the working hours.
6. Any person in restricted areas, that unrecognized, or thought not to be allowed in that location must be confronted and questioned by staff as to whether they have the right to be in that location.
7. All visitors of the organisation must be signed in and given a badge at the reception desk. The badge should be worn at a visible location at all times. Visitors should also be accompanied by staff at all times.
8. Access to all doors is controlled with swipe cards. Each card should allow each individual access to specific areas based on their job.
9. Sensors/cameras:
    a. The inside of the building is fitted with motion detectors and cameras, to be used for after hours. Any motion should activate alarms.
    b. Outside of the building is fitted with cameras as well as glass breakage sensors, if a glass breaks it should activate the alarms.
    c. Parking lot is fitted with cameras.
    d. All cameras are recording 24/7.
    e. If alarms are activated the police should be notified and the camera recordings should be annotated.

Collaborative-robot specific security

Authentication

Each cobot operator should be continuously authenticated while around the cobot system.

In order to achieve this the user/system must:

1. Log in to the system with his credentials at the beginning of the session on the Teach pendant. All login information should be strictly confidential and unique to each person.
2. At all times wear the smart bracelet given to him.

3. The user should manually log out the cobot system whenever leaving the cobot system untenanted.
4. The system should automatically timeout and log out whenever it is not receiving a response from the smart bracelet after a set amount of time, e.g. 1min
5. The cobot system should be unusable if the bracelet is not in range, including any ports on the main computing device.

Communications

1. All private and confidential information should be encrypted, password protected and only accessible to authorised users.
2. All network communications should be encrypted.

Intrusion detection system

1. The system should be fitted with an intrusion detection system, which can detect and alert any anomalous behaviour.