SYSTEM AND METHOD FOR OPERATING A SAFETY-CRITICAL DEVICE OVER A NON-SECURE COMMUNICATION NETWORK

FIELD OF THE INVENTION

The present invention relates to a system and method for operating a safety-critical device over a non-secure communication network.

BACKGROUND OF THE INVENTION

The defense industry is moving towards standardized platforms and infrastructures. In these platforms all systems are required to interoperate over packet based networks. The operator positions become multipurpose operator positions shared between several systems. The interface between the system and the operator positions thus changes.

Similar requirements are also present in other safety critical application fields.

Hence, there is a need for a system and method for providing a method and system for operating, at a near location, a safety-critical device located at a far location.

In particular, there is a need for such a system and method which may utilize certain aspects of already existing, hard-wired solutions, fulfil relevant safety requirements, provide a secure, tamper proof and supervised connection, and which make use of standard protocols and networking elements.

SUMMARY OF THE INVENTION

The invention is defined by the appended claims.

According to an aspect, there is provided a system for operating, at a near location, a safety-critical device located at a far location, the system comprising

- a first operating input device to be operated at the near location by an operator, providing a first barrier control signal;
- a second operating input device to be operated at the near location by an operator, providing a second barrier control signal;
- the first barrier control signal being communicatively connected to a near end of a first secure communication tunnel through the non-secure communication network;

- the second barrier control signal being communicatively connected to a near end of a second secure communication tunnel through the non-secure communication network;
- a far end of the first secure communication tunnel being communicatively connected to an activating input of a first barrier circuit;
- a far end of the second secure communication tunnel being communicatively connected to an activating input of a second barrier circuit;
- the first and second barrier circuits being configured to enable operation of the safety-critical device when both the first and second barrier circuits are activated.

According to another aspect, there is provided a method for operating, at a near location, a safety-critical device located at a far location, the method comprising
- providing a first barrier control signal from a first operating input device to be operated at the near location by an operator;
- providing a second barrier control signal from a second operating input device to be operated at the near location by an operator;
- communicating the first barrier control signal to a near end of a first secure communication tunnel through the non-secure communication network;
- communicating the second barrier control signal to a near end of a second secure communication tunnel through the non-secure communication network;
- communicating, from a far end of the first secure communication tunnel a signal to an activating input of a first barrier circuit;
- communicating, from a far end of the second secure communication tunnel, a signal to an activating input of a second barrier circuit;
enabling, by the first and second barrier circuits, operation of the safety-critical device when both the first and second barrier circuits are activated.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic block diagram illustrating is a schematic block diagram illustrating a context wherein the disclosed system and method principles may be used.

Fig. 2 is a schematic block diagram illustrating an exemplary system employing basic principles of the invention.