

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

FIELD OF THE INVENTION

5 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
10 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.

15 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

20 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;
- 25 - 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;

- 5 - 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.

10

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;
- 15 - 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;
- 20 - 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;
- 25 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.

30

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

Fig. 3 is a schematic block diagram illustrating an exemplary system employing further principles of the invention

Fig. 4 is a schematic flowchart illustrating principles of a method according to the invention.

- 5 Fig. 5 is a schematic block diagram illustrating an exemplary system employing principles of the invention, including safety related blocks and video session identification.

Fig. 6 is a schematic block diagram illustrating an exemplary system employing principles of the invention, including packet based safety barriers.

- 10 Fig. 7 is a schematic block diagram illustrating an exemplary protocol stack for use in a system or method according to the invention.

Fig. 8 is a schematic sequence diagram illustrating information transfer in certain aspects of the invention, including time-stamping features.

- 15 Fig. 9 is a schematic sequence diagram illustrating information transfer in certain aspects of the invention, including hardware barrier supervision.

Fig. 10 is a schematic sequence diagram illustrating information transfer in certain aspects of the invention, including connectivity supervision.

Fig. 11 is a schematic block diagram illustrating an exemplary system employing principles of the invention, including user arbitration features.

- 20 Fig. 12 is a schematic block diagram illustrating an exemplary system employing principles of the invention, including video distribution.

Fig. 13 is a schematic block diagram illustrating aspects relating to the modification of a previous system to include principles of the invention.

Fig. 14 is a schematic block diagram illustrating two barrier multiplexers.

25 **DETAILED DESCRIPTION OF THE INVENTION**

Fig. 1 is a schematic block diagram illustrating an exemplary context wherein the presently disclosed system and method may be employed.

Remotely controllable weapon stations, each including a power device, MPU, 10, 20 have been illustrated as examples of safety-critical devices located at a far location. Power inputs to MPU's 10, 20 are shown at 12, 22, respectively.

5 A gunner station 50 and a commander station 60 have been illustrated as examples of operating stations at a near location, to be operated by an operator. Each operating station includes operating input devices, e.g. weapon firing circuitry and/or weapon movement circuitry. 52 and 62 denote power.

A network 40, e.g. a vehicle network, has been schematically illustrated for providing communication between the near and far locations.

10 70 denotes crew display, connected to the network 40. 30 denotes other equipment connected to the network 40.

Some possible advantageous features of the presently disclosed method and system include:

- 15 - User arbitration: The controlling user (operator) of each weapon station should advantageously be established, and the system should advantageously be safe with respect to intentional tampering and unintentional user access.
- Video distribution: The controlling user (operator) should advantageously be able to see and control video data captured at a weapon station, and the system should advantageously be safe and therefore have a positive
20 confirmation that the user (operator) is viewing the correct video source if safety critical operations are to be allowed.
- Movement: The controlling user (operator) should advantageously be able to safely move the weapon station, and the weapon station must be safe with respect to unintended movements.
- 25 - Firing: The controlling user (operator) should be able to fire the weapons, and the weapon station should be safe with respect to unintended fire.
- Otherwise the system may advantageously allow:
 - A monitoring user to view any video source.

- The screens to be used for multiple purposes.
- The communication between the near and far locations to be packet based communication.

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

The system 100 is a system for operating, at a near location, a safety-critical device 180 located at a far location. The safety-critical device 180 may, e.g., be a weapon firing circuitry or a weapon movement circuitry, although alternatives exist.

10 The upper part of figure 2 represents the near location and the lower part of figure 3 represents the far location.

The system comprises a first operating input device 110 to be operated at the near location by an operator, providing a first barrier control signal 112. The system
15 further comprises a second operating input device 120 to be operated at the near location by an operator, providing a second barrier control signal 122.

Each operating input device 110, 120 may be, e. g., a weapon fire control device or a weapon movement control device, although alternatives exist.

20 The first 110 and second 120 operating input devices may be arranged to be operated by the same operator or by different operators.

Further in the system, the first barrier control signal 112 is communicatively connected to a near end of a first secure communication tunnel through a non-secure
25 communication network 140.

Likewise, the second barrier control signal 122 is communicatively connected to a near end of a second secure communication tunnel through the non-secure
communication network 140.

30 A far end of the first secure communication tunnel is communicatively connected to an activating input 152 of a first barrier circuit 150. Correspondingly, a far end of

the second secure communication tunnel is communicatively connected to an activating input 162 of a second barrier circuit 160.

5 The first 150 and second 160 barrier circuits are configured to enable operation of the safety-critical device 180 when both the first 150 and second 160 barrier circuits are activated.

Advantageously, separate hardware circuits are used for implementing the first 150 and second 160 barrier circuits.

10

In a particular aspect, not illustrated in fig. 2, the system may be configured for operating, at a near location, a plurality of safety-critical devices such as the safety critical device 180, located at the far location. In such an aspect, the system may further comprise a first multiplexer which multiplexes a plurality of first barrier control signals onto the first secure communication tunnel through the non-secure communication network 140. Further, the system may comprise a second multiplexer, multiplexing a plurality of second barrier control signals onto the second secure communication tunnel through the non-secure communication network. Further in this multi-safety-critical device aspect, the first barrier circuit 150 may include a first demultiplexer, and the second barrier circuit 160 may include a second demultiplexer. More detailed features relating to this aspect have been explained with reference to fig. 14 below.

25 The non-secure communication network 140 may advantageously be a packet based communication network, such as an Internet Protocol (IP) network. Each of the secure communication tunnels may be an IPsec tunnel. The IPsec tunnel may be configured in an integrity only mode. Advantageously, the system may be configured with a fixed IP addressing scheme.

30 Advantageously, the communication through the secure communication tunnel employs a protocol which includes time-stamping of data. Such aspects have been explained in closer detail i.a. with reference to fig. 8 below.

In a particular aspect, an operating input device may include a video session information device, and the safety-critical device may be a video confirmation device. In this aspect, the system may further comprise (not illustrated in figure 2) a video distribution device. The video distributing device is arranged to provide a video signal which is transferred through the non-secure communication network and displayed on a display screen at the near end. Further, the video session information device may be configured to derive video session information from the video signal and transfer the video session information through the secure communication tunnel. Also, the video confirmation device may be configured to confirm the authenticity of the video signal transferred through the non-secure communication network. These aspects of a video session information device have been explained in closer detail, i.a. with reference to fig. 5 and fig. 12 below.

Fig. 3 is a schematic block diagram illustrating an exemplary system employing further principles of the invention.

The system illustrated in fig. 3 corresponds to the system illustrated and described with reference to fig. 2 with some additional features described in the following: The system illustrated in fig. 3 further includes a third operating input device 130 to be operated at the near location by an operator. The third input device 130 provides a third barrier control signal which is connected to a near end of a third secure communication tunnel through the non-secure communication network 140. A far end of the third secure communication tunnel is connected to an activating input of a third barrier circuit 170. In this system, the first 150, the second 160 and the third 170 barrier circuits are configured to enable operation of the safety-critical device 180 when both the first 150, second 160 and third 170 barrier circuits are activated.

It should be appreciated that additional operating devices and barrier devices may be included in the system. Each barrier device provides the possibility to stop the execution of a function, or said another way – functions the user must activate to enable the use of the safety critical device.

The barriers should advantageously be independent so as to reduce the possibilities of common faults disabling multiple barriers.

Each barrier device may include a barrier control and a barrier circuit. The barrier control is the input from the user used to disable/activate the barrier. The barrier circuit is the actual circuit blocking/opening the use of the safety critical function.

5 In the system illustrated in figure 2, two barrier controls must be activated, with the result that both barrier circuits are opened – thus enabling the use of the safety critical function. In the system illustrated in figure 3, three barrier controls must be activated, with the result that all 3 barrier circuits are opened – thus enabling the use of the safety critical function.

10

Fig. 4 is a schematic flowchart illustrating principles of a method according to the invention. The illustrated method is a method for operating, at a near location, a safety-critical device located at a far location. The safety-critical device may, e.g., be a weapon firing circuitry or a weapon movement circuitry, although alternatives exist.

15

The method starts at the initiating step 210. First, in step 220, a first barrier control signal is provided from a first operating input device to be operated at the near location by an operator.

20

Next, in step 230, a second barrier control signal is provided from a second operating input device to be operated at the near location by an operator. Each operating input device may be, e. g., a weapon fire control device or a weapon movement control device, although alternatives exist.

25 Further, in step 240, the first barrier control signal is communicated to a near end of a first secure communication tunnel through the non-secure communication network.

30 Likewise, in step 250, the second barrier control signal is communicated to a near end of a second secure communication tunnel through the non-secure communication network.

In step 260, a signal is communicated from a far end of the first secure communication tunnel to an activating input of a first barrier circuit.

Likewise, in step 270, signal is communicated from a far end of the second secure communication tunnel to an activating input of a second barrier circuit.

- 5 Then, in step 280, operation of the safety-critical device is enabled by the first and second barrier circuits when both the first and second barrier circuits are activated.

It will be understood that the illustrated method largely corresponds to the system explained with reference to, i.a., fig. 2 and 3 above. Hence, the optional or
10 additional features described with reference to the system may also have their counterpart as optional or additional features of the method.

In an aspect, the method may further comprise steps (not illustrated, but corresponding to the additional system features explained with reference to fig. 3
15 above) of providing a third barrier control signal by a third operating input device to be operated at the near location by an operator, communicating the third barrier control signal to a near end of a third secure communication tunnel through the non-secure communication network, communicating, from a far end of the third secure communication tunnel, a signal to an activating input of a third barrier circuit, and
20 enabling, by the the first, second and third barrier circuits, operation of the safety-critical device when both the first, second and third barrier circuits are activated.

Separate hardware circuits may advantageously be used for implementing the first and second barrier circuits.

25

In a particular aspect, the method may be adapted for operating, at a near location, a plurality of safety-critical devices located at the far location. In such a case the method may further comprise multiplexing, by a first multiplexer, a plurality of first barrier control signals onto the first secure communication tunnel through the non-secure communication network, and multiplexing, by a second multiplexer, a
30 plurality of second barrier control signals onto the second secure communication tunnel through the non-secure communication network. In this aspect the first

barrier circuit may include a first demultiplexer, and the second barrier circuit may include a second demultiplexer.

5 The non-secure communication network 140 may advantageously be a packet based communication network, such as an Internet Protocol (IP) network. Each of the secure communication tunnels may be an IPsec tunnel. The IPsec tunnel may be configured in an integrity only mode. Advantageously, the system may be configured with a fixed IP addressing scheme.

10 Advantageously, the communication through the secure communication tunnel employs a protocol which includes time-stamping of data. Such aspects have been explained in closer detail, i.a. with reference to fig. 8 below.

15 In a particular aspect, an operating input device may include a video session information device, and the safety-critical device may be a video confirmation device. In this aspect, the method may further comprise providing, by a video distribution device, a video signal which may be transferred through the non-secure communication network. The video signal may be displayed on a display screen at the near end. The method may further include deriving, by the video session
20 information device, video session information from the video signal and transferring the video session information through the secure communication tunnel. Then the authenticity of the video signal may be confirmed by the video confirmation device. Certain aspects associated with a video session information device have been explained in closer detail, i.a. with reference to fig. 5 and fig. 12 below.

25 Fig. 5 is a schematic block diagram illustrating an exemplary system employing further principles of the invention, including safety related blocks and video session identification.

30 A user or operator 510 is established as a controlling user through the establishment of an IPsec tunnel 542. Each device to be controlled has one (or zero) tunnel and can thus only have one controlling user.

A user 510 has a set of operating input devices, e.g. for movement and firing purposes. Signals provided by the operating input devices are transported over the IP/Ethernet network 540 by the safety over packet module and thus interfaces to the remote remote weapon station (RWS) which includes corresponding firing and movement circuitry.

It should be understood that the IP/Ethernet network 540 referred to in e.g. figures 5, 6, 11, 12 and 13 and the remaining description, may be an example of the non-secure communication network 140 referred to previously, in particular with reference to figures 2, 3 and 4.

The video and session identification may be distributed according to some appropriate standard (e.g. DEF-STAN 00.82). The user subscribes to the video and displays it on his screen. The video session identification is fed back to the video confirmation function through the safety over packet modules where it is compared with the local session identification. If they match, the user views the correct video and the safety critical functions like movement and firing have fulfilled one of the safety criteria.

Further reference numerals in fig. 5 denote the following elements:

520: non safety critical functions, 522: fire control, 524: movement control, 526: video session info, and 528: screen, 530 and 550: safety barriers over packed based networks, 560: non safety critical functions, 562: weapon firing circuitry, 564: weapon movement circuitry, 566: video confirmation, and 568: video distribution.

Fig. 6 is a schematic block diagram illustrating an exemplary system employing principles of the invention, including packet based safety barriers.

Basic protocols and user arbitration

The basic structure consists of 2 main blocks, the barrier control transport circuits (BCTC) 610, 620, 670, 680, and the IPsec tunnel 542. In an advantageous embodiment there are normally 3 barriers, which may include two hardware barriers and one software barrier for safety critical functions. These barriers may be implemented and transported in separate circuits with no common logic so that a failure in one may not affect another.

The IPsec tunnel 542 may be a standard tunnel. In an advantageous embodiment it may be an integrity only tunnel which may be established through a standard Diffie-Hellman based key exchange over the non-safety critical Ethernet IP interface. It can however be any type of IPsec tunnel as long as it is tamper proof.

- 5 User arbitration may be achieved by the movement or re-establishment of the IPsec tunnel 542. The IPsec association between a WSCP 601 and an MPU establishes that position as a controlling user.

In fig. 6, the further reference numerals denote the following elements:

- 540: IP/Ethernet, 542 IPsec tunnel, 601: WSCP #n, 602: WSCP/Display #n, 603:
 10 Weapon Station #m, 604: Safety critical, 605: Non Safety critical, 610: Barrier Control Transport Circuit #1, 611: RTP/UDP IP addr x 1, 612: stat, 613: inp, 614: Weapon n Barrier Ctrl. 1, 615: stat, 616: inp, 617: Weapon 1 Barrier Ctrl. 1, 620: Barrier Control Transport Circuit #2, 621: RTP/UDP IP addr x2, 622: stat, 623: inp, 624: Weapon n Barrier Ctrl. 2, 625: stat, 626: inp, 627: Weapon 1 Barrier Ctrl. 2,
 15 630: SW, 631: TCP IP addr x3, 632: stat, 633: inp, 634: Weapon n Barrier Ctrl. 3, 635: stat, 636: inp, 637: Weapon 1 Barrier Ctrl. 3, 640: IPsec Circuit, 641: IPsec tunnel, 642 CTRL SW, 643: SW, 644: Box ID #n, 652: DDS/IP, 653: DDS/IP, 660: IPsec Circuit, 661: IPsec tunnel, 662: CTRL SW, 663: SW, 670: Barrier Control Transport Circuit #1, 671: RTP/UDP IP addr y1, 672: Weapon n Barrier
 20 Ctrl. 1, 673: Weapon 1 Barrier Ctrl. 1, 680: Barrier Control Transport Circuit #2, 681: RTP/UDP IP addr y2, 682: Weapon n Barrier Ctrl. 2, 683: Weapon 1 Barrier Ctrl. 2, 690: SW Barrier, 691: TCP IP addr y3, 692: Weapon n Fire break, 693: Weapon n Barrier Ctrl. 3, 694: Weapon 1 Barrier Ctrl. 3, 696: Weapon 1 Firing circuitry, 697: Weapon n Firing circuitry.
- 25 Fig. 7 is a schematic block diagram illustrating an exemplary protocol stack for use in a system or method according to the invention.

- The IPsec tunnel 542 is established and terminated at each unit (e.g. weapon station control panel, WSCP; main processing unit, MPU). The establishment of this tunnel 542 is following the network addressing scheme – the IP address which is the basis
 30 for routing between the units (e.g. WSCP, MPU).

The next layer is the IP layer between the barriers – this is a fixed addressing scheme where each barrier on each side has a fixed address:

WSCP barrier 1: addr x1

WSCP barrier 2: addr x2

5

MPU barrier 1: addr y1

MPU barrier 2: addr y2

....

10 Thus after the IPsec tunnel 542 has been established/moved the MPU barriers will always communicate with the same IP address. This means that the barrier multiplexing scheme in the IPsec module is simple and the design of the HW barriers are static and thus robust.

The RTP/UDP (Real Time Protocol/User Datagram Protocol) is a simple datagram protocol which includes time-stamping possibilities. This use is explained later.

15 The reference numerals in fig. 7 denote the following elements:

710: Transfer of safety critical signals and status, 711: SW barriers, 712: HW barriers, 713: Payload, 714: Payload, 716: HW barriers, 717: SW barriers, 718: Payload, 719: Payload, 720: Timestamping of data, 730: End-to-end payload supervision, 731: Barrier mux, 732: Barrier mux, 740: Network connectivity. Fig. 8
20 is a schematic sequence diagram illustrating information transfer in certain aspects of the invention, including time-stamping features.

A useful feature of the information transfer is that the main processing unit, MPU, establishes time slots, TS.

- 25 - The TS length may be defined by the frequency of barrier request messages from the MPU – denoted by x in figure 8.
- The barrier request message provides status information from the MPU.
- Within each timeslot the WSCP provides one message.

- The barrier reply message may be sent at any time during the TS. If an input changes state during the TS the WSCP may immediately send the barrier reply carrying the updated status of all inputs.
- If there are no changes during the TS the WSCP must provide a barrier reply to acknowledge connectivity at the reception of the next TS message (with the status of all inputs, so that the inputs become defined quickly at startup).
- The request contains a running sequence number so that the control panel may verify connectivity.
- The reply contains the sequence no. of the request, thus connectivity may be checked at the MPU.

This procedure may ensure certain advantages, including:

- No perception of absolute time required.
- The bandwidth between the MPU and WSCP may be constant and controllable (by changing the frequency of barrier request messages).
- A change in an input at the WSCP end may be signaled immediately. If 2 or more changes occur within the same TS, then the latest will be delayed on TS.
- The connectivity is supervised at both ends (reception of one message for each TS).

The reference numerals in fig. 8 denote the following elements:

- 801: Control panel #B, 802: MPU #A, 810: Control panel HW, 812: Barrier Ctrl. Transport Circuit #1b, 814: IPsec, 816: IPsec, 818: Barrier Ctrl. Transport Circuit #1a, 820: MPU HW, 822: Wait until $t=T$ $SNa=n$, 824: Current status, 826: Barrier request (SNa , status), 828: Encapsulated message, 830: Barrier request (SNa , status), 832: Current status, 834: $SNb=SNa$, 836: Input signal #1 change, 840: Sample current inputs, 842: Barrier reply (SNb , inputs), 844: Encapsulated message, 846: Barrier reply (SNb , inputs), 848: All inputs, 850: input signal #2 change, 852: input signal #3 change, 854: Wait until $t=T+x$, $SNa=n+1$, 856: Current status, 858: Barrier Request (SNa , status), 860: Encapsulated message, 862: Barrier request

5 SNa, status, 864: Current status, 866: S_{nb}=S_{Na}, 868: All inputs, 870: Sample current inputs, 872: Barrier reply (S_{nb}, inouts), 874: Encapsulated message, 876: Barrier reply (S_{Nb}, inputs), 878: All inputs, 880: Wait until $t=T+2x$, S_{Na}=n+2, 890: Ts, 892: Trigger immediate reply upon next request, 894: d=x msec, 896: d=x msec.

Fig. 9 is a schematic sequence diagram illustrating information transfer in certain aspects of the invention, including hardware barrier supervision. Fig. 9 illustrates different possible mechanisms involved in the supervision of the information transfer.

10 The relation to the protocol stack:

- RTP: Verify currentness and End to End connectivity
- UDP: Verify End To End payload integrity
- IP: Verify barrier number multiplexing integrity
- IPsec: Verify authenticity and payload integrity on network segment
- 15 • Ethernet: Verify segment integrity

Frames with any kind of error are advantageously discarded.

Note also that the concept of sending and receiving one message per TS per HW barrier control transport circuit is advantageous since it also provides the capability to detect loss of frames.

20 Payload integrity may be verified through:

- End to end:
 - UDP checksum and IP header checksum
- Network connection (IPsec tunnel): IPsec integrity verification
- Segments (internal HW errors):
 - 25 • BCTC to IPsec circuit: Ethernet CRC verification

Information currentness

In safety critical applications it is advantageous to verify that the information provided is current (up to date) so that the system is not acting on outdated information. In a packet based network data may be delayed significantly if the network is congested. Such situations should preferably be detected.

The MPU is basically requesting (barrier request) the WSCP to provide the input signals to the MPU every x msec. (Timeslot). The WSCP must provide the data at the end of the timeslot unless the signal changes state during the timeslot in which case the inputs may be provided immediately.

The MPU provides a Timestamp at each request. The reply must contain the timestamp so that it may be determined that the information is current. If 2 changes occur within one TS then the latter change will be reported at the next interval. The inaccuracy in the determination of currentness therefore determined by the length of the timeslot. The length of the timeslot also determines the accuracy by which frames delayed in the network may be measured.

The size of the timeslot should therefore advantageously be set to match the accuracy by which the currentness of the inputs must be measured.

The size of the timeslot may also determine the constant rate at which frames are transmitted through the network.

The reference numerals in fig. 9 denote the following elements:
 801: Control panel #B, 802: MPU #A, 810: Control panel HW, 812: Barrier Ctrl. Transport Circuit #1b, 814: IPsec, 816: IPsec, 818: Barrier Ctrl. Transport Circuit #1a, 820: MPU HW, 910: Wait until $t=T$ $SNa=n$, 912: Current status, 914: Sample current status, 916: Encapsulate status RTP(SNa)/UDP/IP(B,A)/Eth, 918: Barrier request (SNa , status), 920: Verify Eth. CRC, 922: Encapsulate in IPsec tunnel, 924: Encapsulated message, 926: Verify Eth. CRC, IPsec Integrity, Verify CRCs: IP Demux barriers on IP addsr., 928: Barrier request (SNa , status), 930: Verify CRCc: Eth, IP, UDP Verify SNa update, 932: Extract status, 934: Current status, 936: $SNb=SNa$, 938: Input change, 940: All inputs, 942: Sample current inputs, 944: Encapsulate inputs RTP(SNb)/UDP/IP/(A,B), Eth., 946: Barrier reply (SNb , inputs), 948: Verify Eth. CRC, 950: Encapsulate in IPsec tunnel, 952: Encapsulated

message, 954: Verify Eth. CRC, IPsec Integrity, Verify CRCs: IP header Demux barriers on IP addsr., 956: Barrier reply (TSb, inputs), 958: Verify CRC: Eth. IP, UDP, 960: If SNb=SNa-1 ... SNa Tick off connectivity, 962: Extract inpute, 964: All inputs, 966: Wait until $t=T+x$ SNa=n+1, 994: d=x msec.

- 5 Fig. 10 is a schematic sequence diagram illustrating information transfer in certain aspects of the invention, including connectivity supervision.

In safety critical systems it is advantageous to monitor connectivity between the units involved. Loss of connectivity shall render the system in a safe state. This is applied for each barrier so that a detected error places the signals carried by the
10 barrier in a safe state.

The MPU is requesting information at a regular basis (once per timeslot). Each request must be acknowledged through a reply message. The loss of a reply is interpreted as loss of connectivity.

- 15 In order to allow for a packet loss in a packet network the number of lost frames may be set to a ratio. Eg: a frame loss of 2 ppm (packets per million) before loss of connectivity is declared. An acceptance for packet loss should advantageously be accompanied by the tolerance for reduced accuracy in the determination for currentness and response to change.

- 20 Loss of end to end connectivity for the BCTCs results in the disabling of the affected barriers – thus placing the system in a safe state. Connectivity for the barrier circuits may automatically be reestablished when the packet loss and operation of the barrier circuits have been seen to be correct for a defined period (e.g. 10msec., 1sec., 10 sec...).

- 25 In certain aspects the system and method provide the standard detection of loss of carrier on physical interfaces.

Loss if IPsec connectivity may be repaired through a new arbitration sequence from the user.

The reference numerals in fig. 10 denote the following elements:

- 801: Control panel #B, 802: MPU #A, 810: Control panel HW, 812: Barrier Ctrl.
30 Transport Circuit #1b, 814: IPsec, 816: IPsec, 818: Barrier Ctrl. Transport Circuit

#1a, 820: MPU HW, 1010: Wait until $t=T$ $SNa=n$, 1012: Current status, 1014: Barrier request (SNa , status), 1016: Encapsulated message, 1018: Barrier request (SNa , status), 1020: Current status, 1022: $SNb=SNa$, 1024: No change on input signal, 1026: Wait until $t=T+x$ $SNa=n+1$, 1028: Current status, 1030: Barrier request (SNa , status), 1032: Encapsulated message, 1034: Barrier request (SNa , status), 1036: Current status, 1038: All inouts, 1040: Sample current inputs, 1042: Encapsulate inputs RTP(SNb)/UDP(inputs)/IP/(A,B), Eth., 1044: Barrier reply (TSb , inputs), 1046: $SNb=SNa$, 1048: Encapsulated message, 1050: Barrier reply (SNb , inputs), 1052: Verify CRC: Eth. IP, UDP, 1054: If $SNb=SNa-1 \dots SNa$ Tick off connectivity, 1056: All inouts, 1058: 966: Wait until $t=T+2x$ $SNa=n+2$, 1090: TS, 1094: $d=x$ msec, 1096: $d=x$ msec.

Fig. 11 is a schematic block diagram illustrating an exemplary system employing principles of the invention, including user arbitration features.

The user arbitration is a function which includes interactions between the WSCP and the RWS and between the non-safety-critical and safety-critical SW.

- The user requests access (or control) over an RWS.
- The arbitration logic decides whether to grant access or not.
- If access is granted:
 - The current connection is closed
 - The requesting WSCP is informed of the acceptance
 - On the RWS: The destination IP address of the IPsec tunnel 542 is changed to the new user position
 - On the WSCP: The destination IP address of the IPsec tunnel 542 is set/changed to the RWS
 - The IPsec key is generated through local action (random number gen) on both ends combined with the Diffi-Hellmann Key exchange protocol.
 - The hash of the key is set for the IPsec tunnel 542 at both ends.

- The tunnel 542 is operational and the barriers are connected.

In fig. 11, the reference numerals denote the following elements:

1, 2, 3, 4 are references used in element 1124. 540: IP/Ethernet, 542 IPsec tunnel,
601: WSCP #n, 602: WSCP/Display #n, 603: Weapon Station #m, 604: Safety
5 critical, 605: Non Safety critical, 610: Barrier Control Transport Circuit #1, 620:
Barrier Control Transport Circuit #2, 660: IPsec Circuit, 670: Barrier Control
Transport Circuit #1, 673: Weapon 1 Barrier Ctrl. 1, 680: Barrier Control Transport
Circuit #2, 696: Weapon 1 Firing circuitry, 697: Weapon n Firing circuitry, 1102:
Hash(Key), 1104: Gen Key, 1106: DH, 1108: Exchange keys, 1110: Accept/reject,
10 1112: Request access (pos), 1114: Arbitrate: based on Priority and state accept or
reject access, 1116: DH, 1118: Move (pos), 1120: Gen Key, 1122: Hash (Key),
1124: If accept: 1. Close current connection; 2. Change IP addr; 3. Change Keys, 4.
Open new connection.

Fig. 12 is a schematic block diagram illustrating an exemplary system employing
15 principles of the invention, including video distribution.

Video data may be distributed to the user screen(s) by some standardized or
proprietary communication means and protocol. The video may be distributed with
an identification of the video stream (e.g. SAP/SDP protocols for DEF-STAN 00-
82). The session id is fed back to the MPU through the video session id function.
20 The video confirmation function in the MPU compares the id of the distributed
video with the received video id and thus confirms that the user views the correct
video for the control of the safety critical functions.

In fig. 12, the reference numerals denote the following elements:

542 IPsec tunnel, 601: WSCP #n, 602: WSCP/Display #n, 603: Weapon Station #m,
25 604: Safety critical, 605: Non Safety critical, 610: Barrier Control Transport Circuit
#1, 620: Barrier Control Transport Circuit #2, 673: Weapon 1 Barrier Ctrl. 1, 683:
Weapon 1 Barrier Ctrl. 2, 692: Weapon n Fire break, 1202: Display unit, 1204:
Displayed video, 1206: Source IP Addr, 1208: Session ID: - Seq no.; - Source IP
addr, 1201: Seq No., 1212: Other Display units, 1214: SAP. Session ID; - Seq. no.;
30 - Source IP Addr, 1216: Encapsulate e.g. DEF-STAN 00.82, 1218: Source IP Addr,
1220: Verify Correct video on display, 1222: Video. Fig. 13 is a schematic block

diagram illustrating aspects relating to the modification of a previous system to include principles of the invention.

Migration from previous designs

The system and method may advantageously be enabled to reuse safety mechanisms and barriers already present in an existing or previous system. It may also be made so as to reuse the same BCTC HW and SW components for independent safety critical functions, e.g. use BCTC#1 for both movement and missile firing.

Figure 13 illustrates how the presently disclosed system may be achieved by inserting novel elements and/or features between existing firing and movement barriers. The existing barriers between the firing control and the firing circuitry may be bridged over a packet based network 540.

In fig. 13, the further reference numerals denote the following elements:
540: IP/Ethernet, 1302: Fire control, 1304: Movement control, 1306: Weapon Firing circuitry, 1308: Weapon Movement circuitry, 1310: Old solution, 1312: New solution, 1314: SEL, 1320: Safety barriers over packed based networks, 1330: Safety barriers over packed based networks.

Fig. 14 is a schematic block diagram illustrating two barrier multiplexers.

Multiplexers of the type shown here should advantageously be designed as independent functions so as to maintain independence between the barriers.

In fig. 14, the reference numerals denote the following elements:
1402 Packet barriers 1, 1404: Barrier Control Transport Circuit #1, 1406: RTP/UDP IP address, 1408: Hardwired barriers 1, 1410: Barrier #1 Sel Packet/HW, 1412: Weapon n Barrier 1, 1414: Weapon 1 Barrier 1, 1422 Packet barriers 2, 1424: Barrier Control Transport Circuit #2, 1426: RTP/UDP IP address+1, 1428: Hardwired barriers 2, 1430: Barrier #2 Sel Packet/HW, 1432: Weapon n Barrier 2, 1434: Weapon 1 Barrier 2.

The disclosed system and method may provide numerous advantages, including at least one of the following:

- Provides separate barriers as required by the safety community
- May be applied to existing hard-wired solutions – easy migration of existing solutions
- Combines supervision and information transfer – low and controllable bandwidth
- Is tailorable to response times and bandwidth
- May be transported over standard IP networks with standard protocols
- Provides a safe mechanism for multiuser configurations
- Barriers may be reused for multiple functions – reduces cost and complexity
- Provides a total solution for safety critical systems
- Is a simple HW solution – simple addressing and information transfer
- Few and well defined safety critical components
- No synchronization required between MPU and WSCP (no common and accurate Time Of Day)
- Good supervision for faults
- Immediate response to change (first change in a TS)
- Predictable worst case response
- May be tailored to run on low quality networks (high packet loss)
- May be combined with networks according to ongoing standardization (GVA, DEF-STAN 00-82)
- May be applied to a large variety of applications

Although the invention has been described by example for control of weapons, the skilled person will readily understand that the system and method may have a more general application area, and that remotely controlled weapon stations have been mentioned merely as an illustrative example of conceivable safety-critical devices. The principles of the invention may thus be applied to any safety critical field, e.g. control of industrial or scientific processes, power plants or remotely operated oil-wells.

30

Acronyms and Abbreviations

CRC	Cyclic Redundancy Check
IPSEC	Internet Protocol SECurity

	KPS	Kongsberg Protector Systems
	MPU	Main Processin Unit – The controlling unit in a RWS system
	RTP	Real Time Protocol
	RWS	Remotely operated Weapon Station
5	SAP	Session Announcement Protocol
	SDP	Session Description Protocol
	TCP	Transmission Datagram Protocol
	TS	Time Slot
	UDP	User Datagram Protocol
10	WSCP	Weapon Station Control Panel

CLAIMS

1. 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,
 - 5 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;
 - 10 - 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;
 - 15 - 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.
- 20 2. System according to claim 1, wherein separate hardware circuits are used for implementing the first and second barrier circuits.
3. System according to claim 1, further comprising
- 25 - a third operating input device to be operated at the near location by an operator, providing a third barrier control signal;
 - the third barrier control signal being connected to a near end of a third secure communication tunnel through the non-secure communication network;
 - a far end of the third secure communication tunnel being connected to an
 - 30 activating input of a third barrier circuit;

- the first, second and third barrier circuits are configured to enable operation of the safety-critical device when both the first, second and third barrier circuits are activated.

5 4. System according to claim 1, for operating, at a near location, a plurality of
safety-critical devices located at the far location, the system further comprising
a first multiplexer, multiplexing a plurality of first barrier control signals onto the
first secure communication tunnel through the non-secure communication network;
a second multiplexer, multiplexing a plurality of second barrier control signals onto
10 the second secure communication tunnel through the non-secure communication
network;
the first barrier circuit including a first demultiplexer; and
the second barrier circuit including a second demultiplexer.

15 5. System according to one of the claims 1-4, wherein
the non-secure communication network is a packet based communication network.

6. System according to claim 5, wherein the non-secure communication
network is an IP network and the secure communication tunnel is an IPsec tunnel,
20 e.g. configured in an integrity only mode.

7. System according to one of the claims 5-6, wherein
the communication through the secure communication tunnel employs a protocol
which includes time-stamping of data.

25

8. System according to one of the claims 6-7, wherein
the system is configured with a fixed IP addressing scheme.

9. System according to one of the claims 1-8, wherein
30 the safety-critical device includes at least one of
a weapon firing circuitry, a weapon movement circuitry, and a video confirmation
device.

10. System according to one of the claims 1-9, wherein
the at least one operating input device includes at least one of:
a weapon fire control device, a weapon movement control device, and a video
session information device.

5

11. System according to one of the claims 1-10, wherein
the operating input device includes a video session information device, and
the the safety-critical device includes a video confirmation device,
the system further comprising
10 a video distribution device providing a video signal, the video signal being
transferred through the non-secure communication network and displayed on a
screen at the near end;
the video session information device being configured to derive video session
information from the video signal and transfer the video session information
15 through the secure communication tunnel,
the video confirmation device being configured to confirm the authenticity of the
video signal transferred through the non-secure communication network.

12. Method for operating, at a near location, a safety-critical device located at a
20 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;
25 - 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
30 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.

13. Method according to claim 12,
5 wherein separate hardware circuits are used for implementing the first and second barrier circuits.

14. Method according to claim 12, further comprising
- providing a third barrier control signal by a third operating input device to be
10 operated at the near location by an operator,
- communicating the third barrier control signal being to a near end of a third secure communication tunnel through the non-secure communication network;
- communicating, from a far end of the third secure communication tunnel, a signal to an activating input of a third barrier circuit;
15 - enabling, by the the first, second and third barrier circuits, operation of the safety-critical device when both the first, second and third barrier circuits are activated.

15. Method according to claim 12, for operating, at a near location, a plurality of safety-critical devices located at the far location, the method further comprising
20 multiplexing, by a first multiplexer, a plurality of first barrier control signals onto the first secure communication tunnel through the non-secure communication network;
multiplexing, by a second multiplexer, a plurality of second barrier control signals onto the second secure communication tunnel through the non-secure
25 communication network; and wherein
the first barrier circuit including a first demultiplexer; and
the second barrier circuit including a second demultiplexer.

16. Method according to one of the claims 12-15, wherein
30 the non-secure communication network is a packet based communication network.

17. Method according to claim 16, wherein the non-secure communication network is an IP network and the secure communication tunnel is an IPsec tunnel, e.g. configured in an integrity only mode.
- 5 18. Method according to claim 16 or 17, wherein the communication through the secure communication tunnel employs a protocol which includes time-stamping of data.
- 10 19. Method according to one of the claims 17-18, wherein the method employs a fixed IP addressing scheme.
- 15 20. Method according to one of the claims 12-19, wherein the safety-critical device includes at least one of a weapon firing circuitry, a weapon movement circuitry, and a video confirmation device.
- 20 21. Method according to one of the claims 12-20, wherein the at least one operating input device includes at least one of: a weapon fire control device, a weapon movement control device, and a video session information device.
- 25 22. Method according to one of the claims 12-21, wherein the operating input device includes a video session information device, and the the safety-critical device includes a video confirmation device, the method further comprising
- providing, by a video distribution device, a video signal;
 - transferring the video signal being through the non-secure communication network;
 - displaying the video signal on a screen at the near end;
 - 30 - deriving, by the video session information device, video session information from the video signal;
 - transferring the video session information through the secure communication tunnel; and

- confirming, by the video confirmation device, the authenticity of the video signal transferred through the non-secure communication network.