

Internal distribution code:

- (A) [-] Publication in OJ
- (B) [-] To Chairmen and Members
- (C) [-] To Chairmen
- (D) [X] No distribution

**Datasheet for the decision
of 11 July 2017**

Case Number: T 1067/13 - 3.5.03

Application Number: 08011085.1

Publication Number: 2017685

IPC: G05B19/418

Language of the proceedings: EN

Title of invention:
Safety control system

Applicant:
Yokogawa Electric Corporation

Headword:
Safety control system/YOKOGAWA

Relevant legal provisions:
EPC Art. 56

Keyword:
Inventive step - (no)



Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Case Number: T 1067/13 - 3.5.03

D E C I S I O N
of Technical Board of Appeal 3.5.03
of 11 July 2017

Appellant: Yokogawa Electric Corporation
(Applicant) 9-32, Nakacho 2-chome,
Musashino-shi
Tokyo 180-8750 (JP)

Representative: Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München (DE)

Decision under appeal: **Decision of the Examining Division of the
European Patent Office posted on 22 November
2012 refusing European patent application No.
08011085.1 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman F. van der Voort
Members: B. Noll
P. Guntz

Summary of Facts and Submissions

- I. This appeal is against the decision of the examining division refusing European patent application No. 08011085.1. The refusal was based on the grounds that the subject-matter of claim 1 of a main request lacked novelty and the subject-matter of claims 1 of first and second auxiliary requests lacked inventive step (Articles 52(1), 54 and 56 EPC).
- II. With the statement of grounds of appeal, the appellant filed, by way of replacement, sets of claims of a main and an auxiliary request.
- III. In a communication accompanying a summons to oral proceedings, the board indicated the points to be discussed at the oral proceedings and gave a preliminary opinion on novelty and inventive step.
- IV. In a further letter, the appellant submitted further arguments in support of the patentability of claimed subject-matter according to the requests on file.
- V. Oral proceedings before the board were held on 11 July 2017.

The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the claims of the main request or the auxiliary request, both as filed with the statement of grounds of appeal.

At the end of the oral proceedings the chairman announced the board's decision.

- VI. Claim 1 of the main request reads as follows:

"A system, comprising:

a distributed control system (A) comprising a plurality of control stations (31, 32; 3) connected to a control bus (100); and

a safety control system (B) comprising a plurality of safety control stations (501-50n) connected to said control bus (100) to communicate with each other and to communicate with said distributed control system (A),

wherein

each of the plurality of safety control stations (501-50n) has an interface (601-60n) through which it is connected to the control bus (100) for transmitting own data of each safety control station (501-50n) to all other safety control stations (501-50n) by broadcasting at a fixed cycle via the control bus (100) and for receiving by each safety control station (501-50n) transmitted data from all other safety control stations (501-50n),

said interface implements a safety layer (700) used to generate and diagnose a safety information,

each safety control station (501-50n) is configured to add safety information to the own data and to transmit the own data together with the safety information to the control bus (100) at the fixed cycle, and

the control stations are configured not to add safety information to the own data when transmitting the own data to the control bus."

Claim 1 of the auxiliary request differs from claim 1 of the main request in that the last two paragraphs have been replaced by the following feature:

"each of the plurality of control stations and each of the plurality of safety control stations is configured to broadcast the same amount of 32 bytes within the fixed cycle, the amount of bytes transmitted by the control station being assigned to data, and the amount of bytes transmitted by the safety control station being shared by 16 bytes of data and by 16 bytes of the safety information."

Reasons for the Decision

1. *The application*

The application in suit relates to a distributed control system having safety characteristics. "Distributed" in this context means that the system comprises a plurality of ordinary control stations provided to control the equipment of a plant, rather than only a single central control unit. For the purpose of system safety, a safety control system is integrated into the control system. The safety control system includes a plurality of safety control stations. A function of a safety control station is to stop, upon a corresponding request, e.g. an emergency stop request received from the plant, operation of equipment in a controlled manner. Ordinary control stations and safety control stations communicate with each other over a single bus. Data exchanged between safety control stations is supplemented with safety information, e.g. a CRC (cyclic redundancy check) code, which enables the receiving station to make a diagnosis of the integrity

of the received data. Adding safety information in this way contributes to the safety of the system.

2. *Claim 1 of the main request - inventive step
(Article 56 EPC)*

2.1 D1 is in the same technical field ("... the technical field relates to systems and methods for controlling the functions and operation of safety instrument systems ...", cf. paragraph [0009]). The system includes SIS(safety instrument systems)-compatible field devices (cf. Fig. 1, devices 100', 105' and 110') and non-SIS compatible field devices (100, 105 and 110). In conventional language, field devices may be sensors or actors. However, considering paragraph [0042] of D1 which describes an implementation of a field bus according to the FOUNDATION fieldbus specification, field devices may also include control functions ("control is distributed into the fieldbus devices", see paragraph [0042], lines 13 to 17). This also applies to SIS-compatible devices, cf. paragraph [0083] stating in relation to the SIS function block (SISFB) 530' contained in the SIS-compatible field device as shown in Fig. 8B that "a SISFB enables the distribution of SIS control into and among fieldbus components connected to a fieldbus Architecture". Therefore, a SIS-compatible field device in D1 is a safety control station in the wording of the application in suit, and a non-SIS-compatible field device in D1 is a control station.

D1 thus discloses, using the wording of claim 1, a system comprising a distributed control system comprising a plurality of control stations (devices 100, 105, 110) connected to a control bus 120, 120', and a safety control system comprising a plurality of

safety control stations (devices 100', 105', 110') connected to the control bus to communicate with each other and to communicate with the distributed control system.

D1 further discloses that each safety control station, i.e. a SIS-compatible field device, includes an interface (cf. Fig. 7B, "communication stack" 205 and "SIS interface" 328). The station is connected through the interface to the control bus for transmitting data to and receiving data from the control bus (see the bidirectional arrows in Fig. 7B between blocks 120 and 200, blocks 200 and 328, and blocks 328 and 400 respectively). Since a SIS-compatible field device is connected to the control bus, data transmitted by a particular safety control station is broadcast to all other safety control stations, and each SIS-compatible field device receives data transmitted by each other SIS-compatible field device.

D1 further discloses that each safety control station is configured to add safety information to its own data and to transmit this data together with the safety information to the control bus. In particular, as shown in Fig. 16A, safety information (an "authenticator", which may be a CRC-32, cf. paragraph [0239], lines 9 to 14, and Fig. 16A, step 1616) is generated on the basis of that data (Fig. 16A, the data block 1606 "Data: Object value & status" on the right-hand side and the adjacent data blocks 1608, 1610 and 1612), is added to that data ("Actual Protocol Data Unit", Fig. 16B, Step 1618), and is transmitted over the control bus together with that data (Fig. 16B, step 1622; see also in paragraph [0243]: "... the data and information that is to be communicated over the black channel from the publisher to the subscriber"). Since safety information

is exclusively generated and added by SIS-compatible devices, the skilled person infers that non-SIS-compatible devices in D1 are not configured to add safety information to their own data transmitted over the control bus.

- 2.2 The appellant argued that D1 did not disclose that the interface implements a safety layer used to generate and diagnose safety information. In D1 safety information was added by the SIS-related protocol, which was part of the user layer.

The board does not agree. The word "interface" as used in the application in suit is understood by the skilled person as denoting the functionality in a station which enables the station to exchange data with the bus. The interface in the application is represented merely by a functional block which is present between the bus and the application of a control station, as shown in Fig. 1 (interfaces 601, 602, 60n). The interface as described in the application is therefore not limited to any particular - functional or structural - portion of a station which implements only a low-level, physical or data-link layer of the bus communication. The skilled person would therefore consider the "communication stack" 205 and the "SIS interface" 328 shown in Fig. 7B of D1 as an interface within the meaning of the application in suit, the SIS interface 328 in D1 implementing the SIS sublayer (cf. paragraph [0080]). Therefore, the feature that the interface implements a safety layer used to generate and diagnose safety information does not distinguish the claimed system from the system of D1.

- 2.3 Accordingly, the system of claim 1 differs from the system disclosed in D1 in that each safety control

station is configured for transmitting its own data to all other safety control stations by broadcasting at a fixed cycle via the control bus.

- 2.4 A technical effect of this feature is that the communication infrastructure in the system can be kept simple, since the control bus of the control system can also be used for exchanging safety information. Accordingly, the objective technical problem to be solved starting out from D1 may be seen as providing a simple communication architecture for a safety control system.
- 2.5 In D1, the bus 120, 120' is used for exchanging both ordinary and safety-related SIS-compatible information between stations. Further, in relation to one-to-many communications of data to be transmitted from a single station to a plurality of stations (cf. paragraph [0068]) D1 discloses that the exchange of data originating from a single station and directed to a plurality of stations may be arranged by configuring this exchange of data as a publisher/subscriber virtual communication relationship (VCR) data service. D1 further discloses that in a publisher/subscriber VCR service, by way of a supplementary safety measure in addition to using a SIS-related protocol, sequence number monitoring can be accomplished by publishing a message with each macro-cycle (paragraph [0267]). It would therefore have been obvious to the skilled person in view of the disclosure of D1 that the safety control stations are suitable for transmitting their own data in a fixed cycle via the control bus.
- 2.6 The appellant argued that D1 merely disclosed a toolbox with various tools in order to implement communication between stations. D1 did not however disclose or render

obvious any concrete system architecture in which a single safety control station broadcast messages to all other safety control stations in a fixed cycle.

Further, in D1 the transmission of one message with each macro-cycle did not necessarily mean that the message was transmitted in a fixed cycle, because the publisher/subscriber VCR scheme in D1 was based on a scheduler, whereas the broadcasting of data in a fixed cycle in the present application did not rely on a scheduler.

2.7 These arguments are not convincing. The skilled person would, as set out above, arrive at a concrete system which includes all the features of claim 1, by applying the suggestions made in D1, in order to arrive at a solution of the above-mentioned technical problem. As regards the transmission of a message in each macro-cycle in D1, the skilled person would know that a "macro-cycle" denotes a single iteration of all operations of a particular device which are repetitively executed according to the defined schedule for the particular device. Since the macro-cycle is iteratively executed, a particular operation defined in the macro-cycle, e.g. a transmission of data, is intrinsically repeated "at a fixed cycle".

2.8 For the above reasons, the system of claim 1 lacks inventive step. The main request is therefore not allowable (Articles 52(1) and 56 EPC).

3. *Claim 1 of the auxiliary request - inventive step (Article 56 EPC)*

3.1 The system of claim 1 of the auxiliary request is further distinguished over the system disclosed in D1 by the feature that each of the plurality of control

stations and each of the plurality of safety control stations is configured to broadcast the same amount of 32 bytes within the fixed cycle, the amount of bytes transmitted by the control station being assigned to data and the amount of bytes transmitted by the safety control station being shared by 16 bytes of data and 16 bytes of the safety information.

3.2 The appellant argued that this specification of amounts of data transmitted by a safety and an ordinary control station resulted in an equal amount of data being transmitted during a single cycle by the two stations. It enabled the use of the same data format for control and safety control stations and, therefore, made a further contribution to simplicity of the communication architecture of the claimed system. An additional effect, due to assigning equal portions to the amounts of data and safety information transmitted by a safety control station, was a high safety level of the information broadcast by the safety control station.

3.3 The board notes however that a particular effect of selecting exactly this amount of bytes and this apportionment of bytes is not disclosed in the application in suit. Further, it is noted that D1 discloses that the own data generated by a publishing station may be anywhere from 2 to 120 bytes of information (cf. paragraph [0240], penultimate sentence). The skilled person would therefore consider setting the amount of data within this range, 32 bytes being an arbitrary selection. D1 further discloses that the safety information is created using either a CRC-32 or a CRC-64 algorithm or "other" algorithms (cf. paragraph [0242]). Since it was well known that the more bytes were devoted to safety information the higher the safety obtained would normally be, the

skilled person would also have considered 16 bytes of safety information together with 16 bytes of data without the exercise of inventive skill. The board is therefore of the view that selecting an amount of 32 bytes of data and apportioning it into 16 bytes of data and 16 bytes of safety information would have been an obvious choice for the skilled person.

3.4 In view of the above and the reasons given in point 2, the subject-matter of claim 1 of the auxiliary request does not involve an inventive step (Articles 52(1) and 56 EPC). The auxiliary request is therefore not allowable either.

4. Since there is no allowable request, the appeal is to be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar:

The Chairman:



G. Rauh

F. van der Voort

Decision electronically authenticated