

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
20 January 2022 (20.01.2022)



(10) International Publication Number
WO 2022/015246 A1

(51) International Patent Classification:

G05B 19/05 (2006.01) H04L 12/00 (2006.01)
G06F 21/57 (2013.01) G06N 20/00 (2019.01)

Singapore 487372 (SG). **ZHOU, Jianying**; c/o Singapore University of Technology and Design, 8 Somapah Road, Singapore 487372 (SG).

(21) International Application Number:

PCT/SG2021/050415

(74) Agent: **VIERING, JENTSCHURA & PARTNER LLP**; P.O. Box 1088, Rochor Post Office, Rochor Road, Singapore 911833 (SG).

(22) International Filing Date:

15 July 2021 (15.07.2021)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

10202006737U 15 July 2020 (15.07.2020) SG

(71) Applicant: **SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN** [SG/SG]; 8 Somapah Road, Singapore 487372 (SG).

(72) Inventors: **AHMED, Chuadhry Mujeeb**; c/o Singapore University of Technology and Design, 8 Somapah Road,

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(54) Title: METHOD AND SYSTEM FOR CHARACTERISING A PROGRAMMABLE LOGIC CONTROLLER (PLC) AND/OR ATTACK DETECTION IN A NETWORKED CONTROL SYSTEM

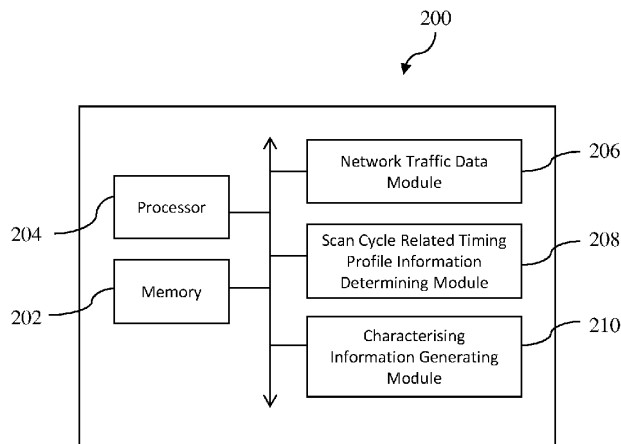


FIG. 2

(57) Abstract: There is provided a method of characterising a programmable logic controller (PLC) in a networked control system. The networked control system includes a plurality of programmable logic controllers (PLCs), including the above-mentioned PLC, and a communication network layer based on which the plurality of PLCs communicate with each other. The method includes: obtaining network traffic data from the communication network layer; determining scan cycle related timing profile information associated with the PLC based on the network traffic data obtained; and generating characterising information associated with the PLC based on the determined scan cycle related timing profile information for characterising the PLC. There is also provided a corresponding method of attack detection in the networked control system, including detecting whether the networked control system is subject to an attack in relation to the PLC based on second characterising information associated with the PLC and reference characterising information associated with the PLC. There is further provided a corresponding system for characterising a PLC and/or attack detection in a networked control system.

[Continued on next page]

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

- *with international search report (Art. 21(3))*
- *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*