

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
05 January 2023 (05.01.2023)



(10) International Publication Number
WO 2023/275859 A1

(51) International Patent Classification:

G06F 21/55 (2013.01) G05B 19/418 (2006.01)
G05B 19/042 (2006.01) H04L 9/40 (2022.01)

(21) International Application Number:

PCT/IL2022/050614

(22) International Filing Date:

09 June 2022 (09.06.2022)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

284559 01 July 2021 (01.07.2021) IL

(71) Applicant: **ELTA SYSTEMS LTD.** [IL/IL]; 100 Yitzchak
Hanassi Blvd., P.O.B. 330, 7710201 Ashdod (IL).

(72) Inventor: **ATZUR, Avi**; 41 Hatzionut, 5851426 Holon
(IL).

(74) Agent: **KRAVETZ, Yossi**; REINHOLD COHN AND
PARTNERS, P.O. Box 13239, 6113102 Tel Aviv (IL).

(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, IQ, IR, IS, IT, JM, 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.

(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,

(54) Title: CROSS-LAYER ANOMALY DETECTION IN INDUSTRIAL CONTROL NETWORKS

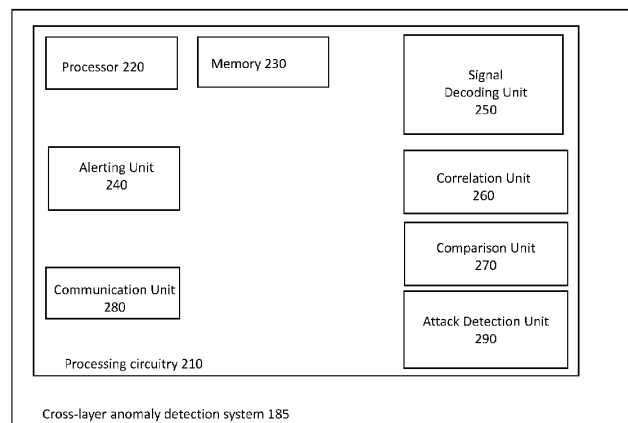


Fig. 2

(57) Abstract: A processing circuitry based method of detecting an anomaly in operation of an industrial control system (ICS), comprising: receiving first data derivative of signaling between a logic controller (LC) and an associated sensing/actuating component, wherein the signaling was detected by a sensor/actuator I/O line signal monitor 5 that is operably connected to a line of communication between a sensing/actuating component and an LC of the ICS; receiving, second data derivative of at least one of: one or more ICS network control packets, one or more statuses logged by an ICS application, and one or more commands entered to an ICS application; and determining whether there is inconsistency 10 between the first data and the second data.

[Continued on next page]

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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*