



(51) International Patent Classification:

H04L 9/40 (2022.01) H04L 67/12 (2022.01)
G01D 4/00 (2006.01)

(21) International Application Number:

PCT/US2024/022965

(22) International Filing Date:

04 April 2024 (04.04.2024)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/496,530 17 April 2023 (17.04.2023) US

(71) Applicant: **LANDIS+GYR TECHNOLOGY, INC.**
[US/US]; 30000 Mill Creek Avenue, Suite 100, Alpharetta,
Georgia 30022 (US).

(72) Inventor: **WIEDMAN, Todd**; 228 Parkwood Ave, Char-
lotte, North Carolina 28206 (US).

(74) Agent: **HARRIS, Christopher P.** et al.; 950 Main Avenue,
Suite 710, Cleveland, Ohio 44113 (US).

(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, CV, 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, MG, MK, MN, MU, 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, CV,
GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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).

(54) Title: SMART INFRASTRUCTURE CONTROL SYSTEMS (SICS) SECURITY MONITORING AND DEFENSE

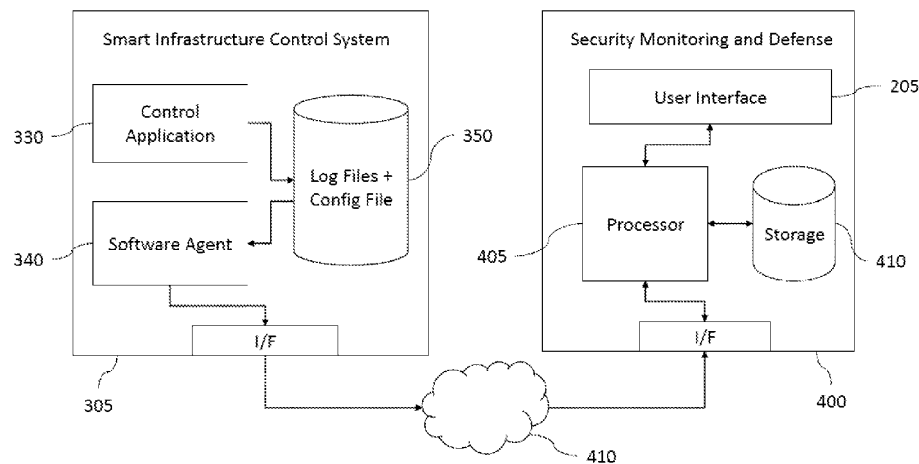


Figure 4

(57) Abstract: The control application generates log files that provide information about the management of the plurality of devices it is responsible for. The information in the log files is dependent upon the messages received from the devices or the commands issued to the devices. For example, in the case of smart meters, the log files generated comprise meter readings, firmware changes, firmware updates, indications as to whether or not the meter has been opened up, indications of overheating at the meter. A software agent extracts information from the log files that may be analysed to determine any anomalies that may be associated with an attack on the system. The analysis performed may comprise pattern matching against the information obtained from the log files, performing an AI analysis of the information obtained from the log files, identifying a signature, etc.

[Continued on next page]

Published:

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