(19) REPUBLIKA HRVATSKA
DRŽAVNI ZAVOD ZA
INTELEKTUALNO VLASNIŠTVO

(10) Identifikator dokumenta: **HR P20220802 T1**

HR P20220802 T1

(12) PRIJEVOD PATENTNIH ZAHTJEVA EUROPSKOG PATENTA

(51) MKP:
G05B 19/418 (2006.01)
H04L 67/01 (2022.01)

(46) Datum objave prijevoda patentnih zahtjeva: 14.10.2022.

(21) Broj predmeta: P20220802T

(22) Datum podnošenja : 28.12.2018.

(96) Broj europske prijave patenta: EP 18248124.2
Datum podnošenja europske prijave patenta: 28.12.2018.

(97) Broj objave europske prijave patenta: EP 3674823 A1
Datum objave europske prijave patenta: 01.07.2020.

(97) Broj objave europskog patenta: EP 3674823 B1
Datum objave europskog patenta: 30.03.2022.

(73) Nositelj patenta: **Nozomi Networks Sagl, Via Maria Ghioldi-Schweizer 2, 6850 Mendrisio, CH**

(72) Izumitelji: **Andrea Carcano, 21100 Varese, IT**
Moreno Carullo, 21026 Gavirate, IT

(74) Zastupnik: Odvjetnica Danija Budimir, 10000 Zagreb, HR

(54) Naziv izuma: **POSTUPAK I UREĐAJ ZA OTKRIVANJE NA JEDNOJ INFRASTRUKTURI**

HR P20220802 T1

PATENTNI ZAHTJEVI

1. Postupak za detektovanje anomalija na fizičkoj infrastrukturi (1), pri čemu je pomenuta fizička infrastruktura opremljena sa jednim ili više aktivatora (10, 20) i/ili senzora električno spojenih na jedan ili više logičkih kontrolera (12, 22, 32), pri čemu pomenuti logički kontroleri (12, 22, 32) regulišu, u upotrebi, vrednosti promenljivih svojstava koje se odnose na fizičko stanje aktivatora (10, 20) i/ili senzora, barem jednu nadzornu jedinicu (52) pomenutih logičkih kontrolera (12, 22, 32), telekomunikacioni sistem između pomenutih logičkih kontrolera i/ili između pomenute nadzorne jedinice (52) i pomenutih logičkih kontrolera (12, 22, 32), pri čemu pomenuti telekomunikacioni sistem može da razmenjuje pakete podataka (PD) koji obuhvataju pomenute vrednosti promenljivih svojstava koje se odnose na fizičko stanje pomoću mrežnih protokola komunikacije,
   pri čemu pomenuti postupak za detektovanje anomalija obuhvata korake:
      - analiziranja, pomoću mrežnog analizatora (101) priključenog na pomenuti telekomunikacioni sistem, svakog od pomenutih razmenjenih paketa podataka (PD) u pomenutom telekomunikacionom sistemu;
      - identifikovanje, pomoću pomenutog mrežnog analizatora (101), za svaki od pomenutih analiziranih paketa podataka (PD) svih korišćenih mrežnih protokola i svih polja svakog od pomenutih protokola;
      - generisanje, kroz kompjuterizovanI uređaj (102) za obradu podataka, virtuelnog predstavljanja pomenute infrastrukture (1) za svaki od pomenutih izmenjenih paketa podataka (PD) i na bazi identifikovanih protokola i polja;
      - pohranjivanje, u jednom prvom nepostojanom memorijskom uređaju (103), pomenute virtuelne predstave generisane za svaki od pomenutih razmenjenih paketa podataka (PD);
      - upoređivanje, pomoću pomenutih kompjuterizovanih uređaja za obradu podataka, pohranjenog pomenutog virtuelnog predstalvjanja sa najmanje jednim elementom za poređenje, identifikovanje najmanje jednog kritičnog stanja pomenute infrastrukture na temelju razlika i/ili sličnosti između pomenute pohranjene virtuelne predstave i pomenutih elemenata za poređenje;
      - signaliziranje, pomoću pomenutih kompjuterizovanih uređaja za obradu podataka, anomalije pomenute infrastrukture kada se najmanje jedno od pomenutih kritičnih stanja identifikuje u pomenutoj virtuelnoj predstavi
   pri čemu je pomenuti postupak za detektovanje anomalija **naznačen time što** pomenuti korak poređenja još obuhvata poređenje dve ili više pomenutih virtuelnih predstava generisanih jedne za drugom, pri čemu se vrši identifikovanje jedne ili više sekvenci komunikacije i frekvencija komunikacije između pomenutih logičkih kontrolera i/ili između pomenutih logičkih kontrolera i pomenutih senzora ili aktivatora i/ili između pomenutih logičkih kontrolera i pomenute nadzorne jedinice, pri čemu pomenuti korak poređenja identifikuje najmanje jedno kritično stanje pomenute infrastrukture u razlikama između pomenutih naknadnih virtuelnih predstava i pomenutih elemenata za poređenje,
   pri čemu pomenuti elementi za poređenje obuhvataju nedopustive sekvence komunikacije ili vrednosti praga frekvencija komunikacije između dve ili više od pomenutih naknadnih virtuelnih predstava, i
   pri čemu pomenuta kritična stanja jesu identifikovana kada najmanje jedna identifikovana sekvenca komunikacije odgovara nedopustivoj sekvenci komunikacije ili kada najmanje jedna vrednost praga detektovane frekvencije komunikacije jeste prekoračena.
2. Postupak prema patentnom zahtevu 1, pri čemu pomenuti elementi za poređenje obuhvataju jednu ili više dozvoljenih prethodno definisanih predstava pomenute infrastrukture, i pri čemu pomenuti korak poređenja identifikuje najmanje jedno od pomenutih kritičnih stanja kada se pomenuta sačuvana virtuelna predstava razlikuje od pomenutih dozvoljenih prethodno definisanih predstava.
3. Postupak prema jednom ili više patentnih zahteva 1 ili 2, pri čemu pomenuti elementi za poređenje obuhvataju jedan ili više pragova pomenutih vrednosti promenljivih svojstava koja se odnose na fizičko stanje pomenutih aktivatora i/ili senzora, i
   pri čemu pomenuti korak poređenja identifikuje najmanje jedno od pomenutih kritičnih stanja kada najmanje jedna od pomenutih vrednosti pomenute pohranjene virtuelne predstave prekoračuje relativni prag vrednosti.
4. Postupak prema jednom ili više patentnih zahteva 1 do 3, pri čemu pomenuti elementi za poređenje obuhvataju jedan ili više protokola za komunikaciju koji nisu dozvoljeni za pomenutu mrežnu komunikaciju, i
   pri čemu pomenuti korak poređenja identifikuje najmanje jedno od pomenutih kritičnih stanja kada pomenuta pohranjena virtuelna predstava obuhvata jedan ili više protokola za komunikaciju koji nisu dozvoljeni za pomenutu mrežnu komunikaciju.
5. Postupak prema jednom ili više patentnih zahteva 1 do 4, pri čemu pomenuti elementi za poređenje obuhvataju jedno ili više polja koja nisu dozvoljena za pomenute protokole za komunikaciju, i pri čemu pomenuti korak poređenja identifikuje najmanje jedno od pomenutih kritičnih stanja kada se pomenuta pohranjena virtuelna predstava sastoji od jednog ili više polja koja nisu dozvoljena za pomenute protokole za komunikaciju.
6. Postupak prema jednom ili više patentnih zahteva od 1 do 5, pri čemu pre pomenutog koraka poređenja pomenuti postupak obuhvata korak definisanja pomenutih kritičnih stanja, pri čemu pomenuti korak definisanja kritičnih stanja obuhvata sledeće korake:
      - analiziranje, pomoću pomenutog mrežnog analizatora priključenog na pomenuti telekomunikacioni sistem, svakog od pomenutih paketa podataka razmenjenih u unapred određenom vremenskom intervalu;

- identifikovanje, pomoću pomenutog mrežnog analizatora, za svaki od pomenutih analiziranih paketa podataka, svih korišćenih mrežnih protokola i svih polja pomenutih protokola;
- generisanje, kroz pomenute kompjuterizovane uređaje za obradu podataka, agregatne virtuelne predstave pomenute infrastrukture u pomenutom unapred određenom vremenskom intervalu zasnovanom na pomenutim protokolima i poljimaa pomenutih protokola identifikovanih sa svakim razmenjenim paketom podataka;
- pohranjivanje, u drugom memorijskom uređaju koji je trajnog tipa, pomenute agregatne virtuelne predstave;
- identifikovanje pomenutih kritičnih stanja kao virtuelnih predstava nesadržanih u pomenutoj agregatnoj virtuelnoj predstavi.

7. Postupak prema jednom ili više patentnih zahteva od 1 do 6, pri čemu pomenuti postupak još obuhvata korak definisanja vrednosti rizika za svaki od pomenutih senzora i/ili aktivatora i/ili nadzornu jedinicu i/ili vrednost i/ili protokol za komunikaciju i/ili polje protokola, pri čemu se pomenute vrednosti rizika pohranjuju na prvom ili drugom memorijskom uređaju,
pri čemu pomenuti korak generisanja virtuelnih predstava obuhvata još jedan korak dodeljivanja pomenutih vrednosti rizika svakoj od virtuelnih predstava, čime se generiše virtuelna predstava rizika.
8. Postupak prema patentnom zahtevu 7, pri čemu pomenuti postupak još obuhvata korak automatskog izračunavanja pomenutih vrednosti rizika, pomoću pomenutog kompjuterizovanog uređaja za obradu podataka, na bazi frekvencije komunikacije između pomenutih industrijskih komponenata i/ili između pomenutih nadzornih jedinica i/ili između pomenutih industrijskih komponenata i pomenutih nadzornih jedinica i/ili na osnovu pomenute vrednosti korišćenih promenljivih svojstava i/ili protoka i/ili svojstava pomenutog identifikovanog protokola pomoću pomenutog mrežnog analizatora.
9. Postupak prema jednom ili više patentnih zahteva od 1 do 8, pri čemu pomenuti paketi podataka (PD) obuhvataju najmanje jedno polje protokola koje se odnosi na adresu pošiljaoca i najmanje jedno polje protokola koje se odnosi na adresu primaoca, i
pri čemu se pomenuta virtuelna predstava generisana za svaki od pomenutih analiziranih paketa podataka (PD) dobija definisanjem pomenutih polja koja se odnose na pomenute adrese kao čvorova, konekcija između pomenutog pošiljaoca i pomenutog primaoca kao lukova i preostalih polja ekstrahovanih iz pomenutih paketa podataka kao vrednosti pomenutih čvorova i lukova.
10. Aparat (100) za detektovanje anomalija u infrastrukturi (1) opemljen sa:
- jednim Ili više aktivatora (10, 20) i/ili senzora funkcionalno priključenih na jedan ili više logičkih kontrolera (12, 22, 32), pri čemu pomenuti logički kontroleri (12, 22, 32) regulišu, pri upotrebi, vrednosti promenljivih svojstava koja se odnose na fizičko stanje pomenutih aktivatora i/ili senzora;
- najmanje jednu nadzornu jedinicu (52) pomenutih logičkih kontrolera (12, 22, 32);
- telekomunikacioni sistem između pomenutih logičkih kontorlera i/ili pomenute nadzorne jedinice (52) i pomenutih logičkih kontrolera (12, 22, 32), pri čemu pomenuti telekomunikacioni sistem može da razmenjuje pakete podataka (PD) koji obuhvataju pomenute vrednosti promenljivih svojstava fizičkog stanja pomoću mrežnih protokola za komunikaciju,

pri čemu pomenuti aparat (100) za detektovanje anomalija obuhvata:
- mrežni analizator (101) koji može da se priključi na pomenuti telekomunikacioni sistem, pri čemu pomenuti mrežni analizator (101) može da analizira svaki od pomenutih paketa podataka (PD) razmenjenih u pomenutom telekomunikacionom sistemu i da identifikuje kompletan korišćeni mrežni protokol za svaki od pomenutih paketa podataka (PD) i sva polja pomenutog protokola;
- komputerizovani uređaj (102) za obradu podataka funkcionalno povezan na pomenuti mrežni analizator (101), pri čemu pomenuti kompjuterizovan uređaj (102) za obradu podataka može da generiše virtuelnu predstavu pomenute infrastrukture (1) na bazi pomenutih protokola i polja pomenutih protokola identifikovanih pomenutim mrežnim analizatorom (101) na svakom razmenjenom paketu podataka (PD);
- prve nestalne memorijske uređaje (103) funkcionalno povezane na pomenuti kompjuterizovani uređaj (102), pri čemu pomenuti prvi memorijski uređaji (103) memorišu pomenutu virtuelnu predstavu generisanu za svaki razmenjeni paket podataka (PD);
- druge trajne memorijske uređaje (104) funkcionalno priključene na pomenuti kompjuterizovani uređaj (102), pri čemu pomenuti drugi memorijski uređaji (104) obuhvataju u svojoj memoriji jedan ili više elemenata za poređenje;

pri čemu pomenuti kompjuterizovani uređaji za obradu podataka, koji se koriste, upoređuju pomenutu virtuelnu predstavu sa najmanje jednim od pomenutih elemenata za poređenje, i
pri čemu kompjuterizovani uređaj za obradu podataka identifikuje i signalizira najmanje jedno kritično stanje pomenute infrastrukture iz pomenutih razlika i/ili sličnosti između pomenute pohranjene virtuelne predstave i pomenutih elemenata za poređenje,
pri čemu je pomenuti aparat (100) za detektovanje anomalija **naznačen time što** pomenuti kompjuterizovani uređaj za obradu podataka, koji se koristi, upoređuje dve ili više uzastopnih virtuelnih predstava generisanih i identifikuje komunikacionu frekvenciju i jednu ili više sekvenci komunikacije između pomenutih logičkih kontrolera i/ili između pomenutih logičkih kontrolera i pomenutih senzora ili aktivatora i/ili između pomenutih logičkih kontrolera i pomenute nadzorne jedinice,

pri čemu kompjuterizovani uređaji za obradu podataka identifikuju i signaliziraju najmanje jedno kritično stanje infrastrukture iz pomenutih razlika između pomenutih sledećih virtuelnih predstava i pomenutih elemenata za poređenje

pri čemu pomenuti elementi za poređenje obuhvataju

nedozvoljene komunikacije ili vrednosti praga za pomenute frekvencije komunikacije između dva ili više pomenutih sledećih virtulenih predstava, i

pri čemu pomenuti kompjuterizovani uređaj za obradu podataka identifikuje najmanje jedno od pomenutih kritičnih stanja kada najmanje jedna identifikovana sekvenca komunikacije odgovara nedozvoljenoj sekvenci komunikacije ili kada je najmanje jedna vrednost praga pomenute detektovane frekvencije komunikacije prekoračena.