(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2024/0214351 A1**
PARK et al. (43) **Pub. Date:** **Jun. 27, 2024**

(54) **SECURITY SYSTEM, DEVICE, AND METHOD FOR PROTECTING CONTROL SYSTEMS**

(71) Applicant: **MISSION SECURE, INC.,** Charlottesville, VA (US)

(72) Inventors: **Daniel D. PARK**, Charlottesville, VA (US); **John Mark BAGGETT**, Deer Park, TX (US); **Edward C. SUHLER**, Earlysville, VA (US); **Rick A. JONES**, Charlottesville, VA (US); **Gary W. HUBAND**, Crozet, VA (US); **Paul D. ROBERTSON**, Shenandoah, VA (US); **Austin C. SUHLER**, Earlysville, VA (US); **Casey SILVER**, Forest, VA (US)

(21) Appl. No.: **18/483,806**

(22) Filed: **Oct. 10, 2023**

Related U.S. Application Data

(63) Continuation of application No. 17/475,674, filed on Sep. 15, 2021, now Pat. No. 11,818,098, which is a continuation of application No. 16/702,944, filed on Dec. 4, 2019, now Pat. No. 11,153,277, which is a continuation-in-part of application No. 15/414,441, filed on Jan. 24, 2017, now Pat. No. 10,530,749.

(60) Provisional application No. 62/412,143, filed on Oct. 24, 2016.

Publication Classification

(51) **Int. Cl.**
H04L 9/40	(2006.01)	
G06N 20/00	(2006.01)	
H04L 41/06	(2006.01)	
H04L 67/12	(2006.01)	

(52) **U.S. Cl.**
CPC *H04L 63/0245* (2013.01); *G06N 20/00* (2019.01); *H04L 41/06* (2013.01); *H04L 63/308* (2013.01); *H04L 67/12* (2013.01)

(57) **ABSTRACT**

A protection system, method, and a security device can protect an operational technology (OT) system having connected hardware equipment, including at least an interface that can receive a control communication and an industrial control device (ICD) for controlling at least one industrial device. They feature tasks/steps that receive control communication from the communication interface, determine whether the received control communication contains an undesirable control command, and either pass or block the received control communication to the ICD depending on whether the received control communication contains an undesirable control command. The security device can be disposed between a source of communication in an OT network and the ICD for protection.