

Faktablad

Avdelningen för cybersäkerhet och säkra
kommunikationer

Publ.nr MSB1761 – maj 2021

Sjävlärande driftstödssystem för cybersäkerhet

Maskininlärning skapar möjligheter att bättre skydda samhällets kritiska infrastruktur. I detta projekt utvecklas en prototyp till ett självlärande driftstödssystem för cybersäkerhet.

Industriella styrsystem kontrollerar elkraftnät, trafiksystem, vattendistribution och många andra fysiska processer. Dessa system är därför av avgörande betydelse för samhällets kritiska infrastruktur. Liksom andra IT-system är de emellertid sårbara för cyberangrepp. Föreliggande projekt syftar till att utveckla en prototyp till ett självlärande driftstödssystem för cybersäkerhet (ett Security Operations Center-system), med förmågan att förutse och besvara cyberangrepp mot industriella styrsystem. Med hjälp av förstärkningsinlärning tränas systemet i en simulerad miljö för att på så vis lära sig att identifiera och på lämpligt vis besvara angrepp. Prototypen kommer att utvärderas i Totalförsvarets forskningsinstitutets cyberträningsanläggning, CRATE.

Projekttitel

SENTIENCE – Simulation-based reinforcement-learning security operations center

Projektorganisation

KTH Kungl Tekniska Högskolan
FOI, Totalförsvarets
forskningsinstitut

Koordinator

Prof Pontus Johnson, KTH
Telefon: 08-7906825
pontusj@kth.se