4.11 Priedas. IDS sensoriaus projektavimui.

I. Bendra dalis

Pastotės duomenų srautų stebėsenai ir kenkėjiškų srautų aptikimui kiekviename 330kV, 220kV ir 110 kV pastotės valdymo pulte (PVP) turi būti suprojektuotas įsibrovimo aptikimo sistemos sensorius (angl. intrusion detection system (IDS) sensor), kuris turi būti suderinamas su esama Litgrid IDS sistema.

IDS (angl. Intrusion Detection System) sensorius – fizinis įrenginys, į kurį nukreipiama duomenų srauto kopija iš tinklo komutatorių, maršrutizatorių. Sensorius analizuoja srautą pasyviai, ieškodamas kenkėjiškų ar anomalinių paketų. Aptikus grėsmę ar anomaliją, informacija siunčiama į centrinį IDS serverį.

II. IDS sensoriaus techniniai reikalavimai

1. IDS sensorius turi būti suderinamas su esama Litgrid IDS sistema bei užtikrinti sklandžią integraciją;
2. IDS sensorius turi palaikyti pramoninių tinklo protokolų analizę, įskaitant, bet neapsiribojant, šiais protokolais: IEC 61850 (MMS), IEC 60870-5-104, DNP3, Modbus (TCP), HTTP, FTP, Telnet.
3. IDS sensorius turi veikti pasyviu režimu – duomenys į jį turi būti pateikiami per SPAN (port mirroring) jungtis, be įtakos aktyviam tinklo srautui.
4. Turi būti suprojektuotos duomenų srautų perdavimas į IDS sensorių iš bendrapastotinio komutatoriaus, maršrutizatoriaus ir PDT komutatorių į kuriuos jungiasi TSPĮ;
5. IDS sensorius turi turėti integruotą out-of-band valdymo modulį, leidžiantį nuotoliniu būdu stebėti ir valdyti, įskaitant galimybę perkrauti ar įjungti sensorių net kai jis yra išjungtas;
6. IDS sensoriui turi būti suprojektuotas rezervuotas elektros maitinimas, užtikrinantis nepertraukiamą veikimą;
7. IDS sensoriaus aparatinė įranga turi būti pritaikyta darbui aplinkos sąlygose, esančiose projektuojamų pastotės valdymo pultų (PVP) patalpose, užtikrinant patikimą veikimą esant temperatūros svyravimams, drėgmei, dulkėtumui ir elektromagnetiniams trikdžiams.