Digital Forensic Readiness in Critical Infrastructures: A case of substation automation in the power sector

Asif Iqbal, Mathias Ekstedt

KTH Royal Institute of Technology,
School of Electrical Engineering, Stockholm Sweden
asif.iqbal@ee.kth.se , mekstedt@kth.se

Abstract. Increasing use of intelligent devices in the Critical Infrastructures has enabled a lot more functionality within several domains that of course has several advantages. But the same automation also brings challenges when it comes to malicious use, either internally or externally. One such challenge is to attribute an attack and ascertain what was the starting point of an attack, who did what, when and why? All these questions can only be answered if the overall underlying infrastructure supports answering such questions. The purpose of this study is to see if in the current setups we are provided within an environment supports forensic readiness in the power sector or not. In order to facilitate such a study our scope of work revolves around substation automation and devices called intelligent electronic devices (IEDs).

Keywords: Digital; Forensics; Forensic Readiness; Substation Automation; Critical Infrastructures;