Analysis of past security incidents using Bayesian Network analysis

Matteo Iaiani, Alessandro Tugnoli & Valerio Cozzani

LISES – Department of Civil, Chemical, Environmental, and Materials Engineering, Alma Mater Studiorum – University of Bologna, via Terracini n.28, 40131 Bologna (Italy)

E-mail: matteo.iaiani@unibo.it

The storage and processing of large quantities of hazardous materials in chemical, process, and Oil&Gas industries (offshore and onshore) can lead to significant incidents such as releases, explosions, and fires, resulting in severe consequences for human life, the environment, and the assets. These events can be triggered by internal system-related factors (safety) or intentional attacks (security), and their proper identification and quantitative assessment is of paramount importance to enhance safety and security and to prevent potential disasters.

A common high-level approach to gather valuable insights supporting existing qualitative and quantitative risk analysis procedures (e.g., safety QRA studies, security vulnerability assessment (SVA) methodologies) is the analysis of past incidents (PIA) that occurred in similar facilities (e.g., belonging to the same industrial sector). In fact, PIA can provide reference scenarios (chain of events from the origin of the risk to the final outcomes suffered by the affected facilities) that can be used by practitioners and authorities as the basis to undertake case-specific assessments. The detailed examination of past incidents plays a crucial role in understanding the multifaceted nature of these events, identifying, e.g., common causes of events, systemic vulnerabilities of the systems, and potential consequences.

Exploratory Data Analysis (EDA) is conventionally employed in PIA; however, it has limitations in systematically analyzing incident datasets and prioritizing relevant incidental chains of events. Specifically, traditional EDA approaches may struggle to capture the complex interdependencies between various factors contributing to incidents, not allowing to properly represent incident causation and evolution. Moreover, EDA often faces challenges related to data availability, quality, and consistency.

To overcome these limitations, the present study proposes a Bayesian Network modelling-based methodology, alternative to canonical EDA, for the systematic identification of the most relevant incidental chains, that serve as reference scenarios, from safety/security incident datasets. This methodology leverages probabilistic models to explicitly represent and quantify the uncertainties and causal relationships between different variables involved in incidents. The use of the Bayesian Network modelling allows for the integration of both quantitative data and qualitative expert judgments, enhancing the robustness and relevance of the analysis in the face of data limitations. The proposed innovative approach is illustratively applied to a case study concerning a dataset of security-related incidents occurred in offshore Oil&Gas fluid production facilities, providing reference security scenarios to be used in the context of security studies of offshore critical infrastructures.

Keywords: *Past incident analysis, Bayesian Network, Security, Reference scenarios, Process industry*