Possible countermeasures for protection against industrial incidents caused by cyber-attacks in the process industry

Gabriele Baldissone [a], Salvina Murè [a], Chidera Winfred Amazu [a], Huxiao Shi [a], Davide Fissore [a] & Micaela Demichela[a]

[a] Politecnico di Torino, Torino, Italy

E-mail: gabriele.baldissone@polito.it

The computerization of the control and management of chemical plants and the spread of the Internet of Things is bringing production and environmental advantages. At the same time, this revolution can bring critical issues. One of these critical issues is that it makes plants vulnerable to cyber-attacks. Cyber-attacks can have various consequences, ranging from data loss to more serious consequences such as releases of energy or dangerous substances. The management of cyber-attacks on process plants cannot be just IT, given the possible consequences.

In addition, cyber-attacks that can have effects on process plants can be of many types (e.g. denial of service, man-in-the-middle or replay attacks), each of which requires an appropriate response.

The last line of defence in the event of a cyber-attack on process plants is the control room operator. As the operator must be able to realize that he is under attack and act appropriately, also by collaborating with operators in the field. The first step in the event of an attack is for the control room operator to identify the variation from normal operations. Once the anomaly has been identified, the operator is required to understand whether it is caused by a fault or a cyber-attack. In the event of a cyber attack, in collaboration with IoT personnel, the operator must identify the level of compromise of the control system and adopt appropriate procedures. The procedures to be adopted can allow the system to continue operating or to safely stop. In the event of the absence of adequate procedures or their ineffectiveness, the operator is required to secure the system, also working with operators in the field.

The operator's ability to react appropriately and safely depends on many conditions, such as experience and specific training.

In this context, we intend to study the preparation of control room operators to identify and react to cyber attacks. To study this aspect, we intend to use a control room simulation. In the simulation of the control room operation, participants will be presented with various scenarios containing possible cyber attacks. In this way, it will be possible to evaluate the participants' behaviour, estimating the parameters that can influence the reaction to cyber attacks (e.g. procedures or training).

At a later stage, the simulation system could be used to train operators to detect and react to cyber attacks.

Keywords: Cyber attack, Safety, Process plant