The upgrade of energy infrastructures by the incorporation of communication and Internet technologies might introduce new risks for the security and for the smooth operation of electricity networks. Exploitation of the potential vulnerabilities of the heterogeneous systems used in smart energy grids (SEGs) may lead to the loss of control of critical electronic devices and, moreover, to the interception of confidential information. This may result in the disruption of essential services or even in total power failures. Addressing security issues that can ensure the confidentiality, the integrity, and availability of energy information is the primary objective for a transition to a new energy shape. This research paper presents an innovative system that can effectively offer SEG cybersecurity. It employs soft computing approaches, fuzzy cognitive maps, and a Mamdani fuzzy inference system in order to model overall security level. Three of the 27 scenarios considered herein have low overall security level, 21 of them have middle overall security, whereas only 3 are characterized as secure. The system automates the strategic planning of high security standards, as it allows a thorough audit of digital systems related to potential infrastructures and it contributes towards accurate decision-making in cases of threats.