VICTORIA UNIVERSITY OF WELLINGTON TE HERENGA WAKA
Wellington Faculty of Engineering Te Wāhanga Ahunui Pūkaha
Ethics and Sustainability Symposium

Smart Grid Systems Code of Ethics

Mitchell Beserra

Abstract

The use of smart technology in the electrical distribution industry provides the opportunity to better support the addition of renewable technology. These smart grids utilise enhanced communication systems to enable an intelligent response to changes in the network. However, with them comes ethical concerns that should be addressed during development and operation. This paper investigates these concerns and aims to produce a code of ethics that can be used to guide decision making throughout the smart grid lifecycle. These principles draw from concerns around privacy, socio-political impacts, and safety and security. The result is a set of six principles that address these main issues and are demonstrated in a hypothetical case study.

Keywords: Smart Grid; Ethics; Renewable Energy.

1. Introduction

With pressure to decarbonise the economy, the penetration of renewable energy sources into the generation portfolio is increasing. These renewable energy (RE) sources are capable of greatly decreasing society's dependence on fossil fuels but come with several unique challenges. One such challenge is their often less dispatchable nature and de-synched production vs consumption profiles. Consequently, this can result in poor use of renewable energy or, in the worst case, heavy strain on the distribution network [1], [2]. While energy storage can help reduce these impacts it tends to be both costly and resource-intensive at larger scales [3]. As such, another common and arguably necessary technique is demand-side management (DSM). DSM pertains to adjusting the load consumption to more appropriately match the production profile such as scheduling devices to turn on during peak production. Unfortunately, due to the current architecture and technology in distribution networks, they are not suited for high RE penetration, greatly limiting both the use of DSM, energy storage solutions and other technologies [4], [5].

As a solution to RE integration, smart grids are often discussed and aim to address the present issues with the current distribution grid. While the definition of a smart grid is loose, the key difference is the inclusion of two-way communication between consumption and operation. This communication, as well as additional technology, enables the grid to respond intelligently to changes in the network. Additionally, there tend to be levels of automation and complex trading markets that come with the implementation. These smart grids can then enable the use of DSM and other technologies through this increased information flow and provide a more efficient, greener network [4]. However, as with most new technologies, smart grids bring a series of ethical questions that must be considered.

1.1. Objective

This paper aims to evaluate the ethical considerations that a smart grid requires and provide a code of ethics for those designing, developing, or deploying a smart grid. To meet this purpose a literature review is undertaken of existing ethical considerations. This is then followed by the code of ethics along with a discussion. Next, each principle is discussed in a case study context. Finally, the paper is concluded with recommendations for success.

2. Literature review

To develop a code of ethics the existing ethical concerns should first be identified. In order to ensure the code presented in this paper is applicable, a literature review of the existing recommendations and codes is presented. Smart grids are related to broader topics such as the Internet of Things, Smart Cities, and Artificial Intelligence (AI). As such, literature surrounding these topics will also be utilised. The review is broadly grouped into the following three main categories: privacy, socio-political, and safety and security.

2.1. Privacy

Of the ethical dilemmas that come with smart grids, privacy is of high concern and discussed throughout the literature [6]-[11]. Most of the public concern is around data collection and anonymity [7]. Through the collection of energy consumption data, information can be inferred about users. This includes whether the user is home, home appliance use, and potentially even the state of the appliances [6], [7]. As a result, consumers are worried about infringements upon their right to remain unidentifiable due to the intrusive data collection. However, in [7] the case is made that privacy, in the sense of anonymity, is no longer the issue. Rather, it is reachability (through name, address, email, etc) that must be preserved as the wide array of data already available makes it nearly impossible to remain anonymous [12]. With this as the case, the importance of privacy becomes to eliminate the ability for someone to be reached physically. This would help to eliminate issues such as advertisement, harassment, and other privacy breaches [7].

In addition to anonymity, control and access to data are other key concerns for smart grids. As large amounts of potentially intrusive data are being collected, users should have control over who is granted access to their data [7]. Control of data access is not a new concept in privacy and is often obtained through privacy agreements. However, in smart grids, the control of data takes on a much more important role. If the energy consumption data was provided to users, then their understanding of the risks involved is likely to improve [6], [7]. This in turn increases their ability to make educated decisions on who should have access to their data and overall improve acceptance [6], [7], [10].

Finally, an important ethical consideration is the potential monetization and exploitation of the collected data. The information derived from this data, such as appliance use and condition, can lend itself to targeted advertisements as well as other manipulation [7], [5], [11]. This topic is closely tied to data control and access, and so, by giving the consumers the ability to control their data, the risk of monetization and exploitation is mitigated. This is furthered by ideas such as network operators hosting the data or self-storage solutions [7], [11]. The argument for network operators relies on non-profit public organizations and thus any benefit from monetization would be reinvested into the network, however, this only discourages monetization rather than prevent it. Self-storage on the other hand may provide a better solution but requires more investment and engagement from the consumers [11]. Regardless, the importance of preventing monetization and privatization is critical [5], [7], [10], [11].

2.2. Socio-political

Arguably, one of the greatest changes that come with the move toward smart grids may be the societal and political aspects. Several papers point toward the need to move away from the traditional utility and consumer relationship and instead adopt a stakeholder mentality [7], [10]. That is to say that consumers should be supported in taking an active role in the development of smart grids. This transition is expressed in several forms such as increased transparency, prioritising end-user expectations, providing tools for increased understanding, and increased levels of communication [6]-[7]. Ultimately, these topics can be reduced to the ideology of including the consumers at each step of the process, which is critical to ensuring the acceptance of smart grids [6], [10]. The enabling technologies, such as DSM, require consumers to take a more active role in their energy consumption. This increased participation also compliments the ethical discussion around privacy which benefits from customer interaction [7], [8]. However, it is not just an increase in customer participation but also the utilities' transition towards customer-focused goals that is necessary [5].

The use of smart grids also comes with an array of changes to how electricity is billed as well as opportunities to sell and buy energy peer-to-peer (flexibility trading). These changes include incentive schemes, trade markets, micro-billing and more [6], [7], [13]. These changes come from a drive to encourage consumer participation as well as renewable energy accommodation strategies such as DSM [6], [7]. However, with these changes come the ethical concerns of discrimination and fairness. Issues such as determining which customer's energy resources are prioritised or who gets access to energy first when production is limited lead to the need for fair decision-making [6]. The use of artificial intelligence systems to help manage the network also requires fairness to be considered in the design [6]. Additionally, the change in the market leads to new types of customers, each with unique priorities and objectives for the. This new complex market may discriminate against certain groups of people, such as those unable to purchase energy resources [6], [7]. Thus, discrimination via both operation and policy must be avoided [7]. The risk of individuals or communities being exploited through these pricing schemes and network changes is a serious issue and must be considered carefully throughout the smart grid design [5], [7].

Smart grids also pose several questions around equity and parsimony. As the grid becomes more decentralised there is the need to define the structure in which it should operate. Flexibility trading, incentives, and tariffs increase the complexity of the system for a user. To limit this complexity and prevent users from falling behind, there should be careful consideration of the impact on the wider society [7]. As explained in [6], with this transition comes different types of stakeholders, those who simply utilise the grid for daily consumption and those who utilise it for profit. This means that to ensure a group or community isn't exploited, all consumers must be aware of their possibilities and options. This points to the need to appropriately inform users as well as provide tools to aid them in digesting these changes [6], [7].

2.3. Safety and Security

The critical nature of electrical networks brings serious concerns around safety and security, and with the digitisation of smart grids, this is increased. Cyber-attacks are becoming a serious concern due to increased connectivity presenting more opportunities for hackers to infiltrate [9]. These attacks can have a range of objectives from monitoring someone's data to physically crippling the network as was done to Ukraine in 2015 [9], [14]. Regardless of the cause, the possible impact that this can create is unquestionable. With so much of civilization relying heavily on the central network the need to ensure security is critical. Several papers have pointed out the lack of security protocol in many smart-meter and SCADA (supervisory control and data acquisition) systems devices and guide how this can be addressed [9], [15]. In the more specific case of smart grids, there should also be consideration around preventing energy theft and attacks on the underlying market [9].

In addition to the operation of the network, cyber-attacks may be done to acquire or leak user data. With the large amount and variety of data collected by smart grids, there is a serious risk to data security. The Cambridge Analytica Scandal provides an example of this risk where a breach of security resulted in large amounts of data being used to influence opinions [16]. As discussed in the section on privacy, collected data could provide insight into users' appliances and the state of these appliances. This could provide immense value to corporations for targeted advertising such as in the Cambridge Analytica Scandal [7]. Additionally, a breach of security could provide hackers with enough information to spatially locate a user, especially since only four data points are required to do so [7]. With the smart grid devices being often located in public spaces, this makes security concerns a critical aspect for ethical consideration.

In addition to cyber-attacks, the automation and control of smart grids pose safety concerns. With the use of such large amounts of data, the use of AI is almost required and with it comes questions around safe control of the network [6]. Several codes of ethics around AI place robustness and safety as key ethical considerations [17], [18], and in a smart grid context, this is no different [5], [8]. The ability for electric networks to cause physical harm is apparent, both from the failure of assets but also for medically dependent customers. Thus, the development of smart grids should hold safety at its core, including in the development of AI.

3. Code of ethics/sustainability

The following section presents a code of ethics for use within smart grid technology. For this purpose, a code of ethics is defined as, "A system of moral principles, which deals with what is good or bad for individuals and society" [8]. The code draws upon the three main areas discussed in the literature and uses inspiration from existing codes or discussions on ethical choices [5]-[8], [11], [17]. The following principles make up the code:

- Fellowship
- Transparent
- Privacy-conscious
- Cautious and conscientious
- Equitable and non-discriminate
- Safety focused

3.1. Fellowship

Fellowship refers to building a co-operative relationship between the communities and the electrical network operators. The overarching goal of smart grids is to provide a more efficient network capable of supporting decarbonisation and renewable energies. This is not a goal that can be achieved in isolation and instead requires contribution from the entire population. For customers, fellowship provides more say in how the network is developed, the impacts on them, and control over their privacy. For the developers of smart grids this relationship enables for a smooth transition while ensuring that the issues surrounding, privacy, fairness, discrimination, and safety can be properly addressed.

3.2. Transparent

The development of smart grids and how they are managed and operated should be transparent and explainable. This ensures that the systems are prevented from becoming overly complex and allows for the public to better understand how they function. Transparency encourages trust and connects closely with fellowship. This also aids in avoiding issues regarding privacy such as the collection of data as customers who understand the importance and what is involved may be more likely to contribute [7].

3.3. Privacy-Conscious

Smart grid systems should be privacy-conscious and follow good practices such as informed consent, consumer access and control over their data, and anonymity to prevent reachability. The granularity of data collected should be carefully assessed and appropriate aggregation methods used to prevent risks to consumers. Additionally, the collected data should be made available to the users to aid in informing their choices. Not only does this allow consumers to contribute to the smart grid in the form of DSM or conscious consumption, but it provides them with an understanding of what is being collected. Relevant data privacy legislation, such as the New Zealand Privacy Act 2020, should be followed.

3.4. Cautious and Conscientious

All decisions and changes, especially more significant ones such as incentive schemes, should be made cautiously and after extensive consideration. Criticism should be sought from a variety of sources including social sciences, subject matter experts, the public, and regulatory documents. All decisions should be implemented fully to ensure issues surrounding safety, security, privacy, and impact are eliminated or mitigated. In the case where negative consequences are inevitable these should be communicated to the public.

3.5. Equitable and non-discriminate

Care should be taken to ensure that ensure that the new technologies, markets, and controls are fair to all and are free of discrimination. With electricity being a necessity for most, it should be ensured that all customers have the same access. Additionally, the risk and rewards should be shared equally to avoid unfair pressure on specific communities or groups. All solutions should be evaluated in the context for which they will serve, that is to say one solution will likely not fit all situations.

3.6. Safety Focused

With the increased complexity involved in smart grids, it is critical to ensure that safety is always emphasised. The consequences that come with the failure of the network can be severe and, in some cases, can result in death. The design and operation of the grid should use a fail-safe mentality and a high emphasis should be placed on security to avoid the elevated risk of cyber-attacks.

4. Case study discussion

A case study is completed in this section to illustrate how the proposed code of ethics could be applied. The context for this study will be the transition of an urban-rural city from a traditional central distribution network towards a more decentralised smart grid. This will include the addition of smart meter technology, to communicate data regarding energy consumption, to a distribution system operator (DSO). There will also be the addition of distributed energy resources (DER), such as solar panels and batteries, throughout the network which are owned by consumers and corporations. To facilitate the addition of these DER, the network is to enable flexibility trading (peer-to-peer energy trading), incentive schemes, and more dynamic pricing. In this situation, the DSO will be the organization heading the transition to the smart grid architecture.

4.1. Fellowship

The first step for the DSO would be to develop infographics, reports, and other informative documents which could then be presented to the public. There should then be serious effort from the DSO to engage with members of the public with a goal to both inform and be informed as to the needs of all stakeholders. Topics such as maximising the use of their DER, what data will be collected, how pricing will change, and flexibility trading should be discussed. This would not only show the community that their interests are valued but also provide the DSO with meaningful input as to direct their developments. This communication should not end here, but instead should be continued during development. This could be in the form of a citizen council or other representative body.

4.2. Transparent

Throughout the deployment, the DSO should maintain a high level of transparency to maintain customer trust. This could be in the form of increased annual reporting, or simply regular progress updates published to their website or local news agency. There should also be thorough but concise documentation created continually to describe the decision-making process and functionality of the system. This documentation should be available for the public representative body to review and pose further questions. Key areas for transparency are pricing, data collection/privacy, and opportunities for consumer benefit such as energy trading.

4.3. Privacy Conscious

A heavy focus should be put on privacy policies and communication with users regarding the data collection. Applications that allow users to see their data and easily control who has access are very important. Additionally, technology installed on the network should maintain a minimum number of vulnerabilities such as connections to the internet and open ports. Encryption schemes, access log audits, and surveillance should be used where appropriate along with other mechanisms of ensuring security as discussed in [9].

4.4. Cautious and Conscientious

The entire process should place a focus on careful planning before execution. This planning process should incorporate the public representatives as well as subject matter experts and social scientists. Thorough testing and modelling should be utilised fully, and a risk assessment framework should be established. This is especially so when regarding system control and pricing schemes.

4.5. Equitable and non-discriminate

The use of social science will be key here as the social structures of cities are highly complex. The development of pricing schemes will be an area of focus as many factors such as income, location, religion, and age will affect customer expectations. There should be an emphasis on communication with customers during these decisions to ensure agreement and fairness. Caution should be taken to ensure groups, such as the rural customers, aren’t disadvantaged or discriminated against.

4.6. Safety Focused

The network’s safety should be a top priority as the consequences of asset failure can be severe. The DSO should ensure proper connection of any renewable energy systems to the network and that they do not negatively impact voltage quality and can be properly disconnected for maintenance. Additionally, any automated control should include human oversight and have built-in mechanisms to ensure safe operation. Contractors should be properly trained to understand how the network is controlled and what is required of them for safe operation.

5. Conclusion and recommendations

Overall, smart grids are something that society likely can’t avoid and the potential benefits that they bring are desirable [3], [4]. To ensure successful integration into society the development and deployment of the systems should follow a code of ethics that addresses the issue surrounding the technology [7]. Of these principles, the idea of fellowship and customer-centric practices is critical for their success. The use of public representatives, transparent communication, and privacy standards will aid in this goal. Additionally, careful consideration regarding pricing, control, and automation is needed as these areas can lead to social injustice [6], [7]. As such, the inclusion of social science is something that should be increased in the sector. The use of different viewpoints provides the ability to better develop the technology for its purpose. Finally, thorough effort should be invested into ensuring the security of the system. With the increased connectivity comes increased cyber threat and thus increased attention.

References

[1] M. D. Leonard, E. E. Michaelides, and D. N. Michaelides, “Substitution of coal power plants with renewable energy sources – Shift of the power demand and energy storage,” Energy. Convers. Manag., vol. 164, pp. 27-35, May. 2018, doi: 10.1016/j.enconman.2018.02.083.

[2] F. J. de Sisternes, J. D. Jenkins, and A. Butterud, “The value of energy storage in decarbonizing the electricity sector,” Appl. Energy, vol. 175, pp. 368-379, Aug. 2016, doi: 10.1016/j.apenergy.2016.05.014.

[3] I. Worighi, A. Maach, A. Hafid, and O. Hegazy et al., “Integrating renewable energy in smart grid system: Architecture, virtualization and analysis,” Sustainable Energy, Grids and Networks, vol. 18, Jun. 2019, Art no. 100226, doi: 10.1016/j.segan.2019.100226.

[4] N. Phuangpornpitak, “Opportunities and Challenges of Integrating Renewable Energy in Smart Grid System,” Energy Procedia, vol. 34, pp. 282-290, 2013, doi: 10.1016/j.egypro.2013.06.756.

[5] E. P. Goodman, “Smart City Ethics: How “Smart” Challenges Democratic Governance,” in The Oxford Handbooc of Ethics of AI, M. D. Dubber, F. Pasquale and S. Das, New York, NY, U.S.A.: Oxford Uni Press, 2020, doi: 10.1093/oxfordhb/9780190067397.013.53.

[6] V. Robu, D. Flynn, M. Andoni, and M. Mokhtar, “Consider ethical and social challenges in smart grid research,” Nat. Mach. Intell., vol. 1, pp. 548–550, Nov. 2019, doi: 10.1038/s42256-019-0120-6.

[7] G. Le Ray and P. Pinson, “The ethical smart grid: Enabling a fruitful and long-lasting relationship between utilities and customers,” Energy Policy, vol. 140, May. 2020, Art no. 111258, doi: 10.1016/j.enpol.2020.111258.

[8] S. G. Tzafestas, “Ethics and Law in the Internet of Things World,” Smart Cities, vol. 1, no. 1, pp. 98–120, Oct. 2018, doi: 10.3390/smartcities1010006.

[9] S. M. Abu Adnan Abir, A. Anwar, J. Choi, and A. S. M. Kayes, "IoT-Enabled Smart Energy Grid: Applications and Challenges," IEEE Access, vol. 9, pp. 50961-50981, Mar. 2021, doi: 10.1109/ACCESS.2021.3067331.

[10] C. Horne, B. Darras, E. Bean, A. Srivastava, and S. Frickel, “Privacy, technology, and norms: The case of Smart Meters,” Soc. Sci. Res., vol. 51, pp. 64-76, May. 2015, doi: 10.1016/j.ssresearch.2014.12.003.

[11] D. Helbing, F. Fanitabasi, F. Giannotti, and R. Hänggli, “Ethics of Smart Cities: Towards Value-Sensitive Design and Co-Evolving City Life,” Sustainability, vol. 13, no. 20, Oct. 2021, Art no. 11162, doi: 10.3390/su132011162.

[12] YA. de Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, “Unique in the Crowd: The privacy bounds of human mobility,” Sci. Rep., vol. 3, Art no. 1376, Mar. 2013, doi: 10.1038/srep01376.

[13] P. H. Nguyen, W. L. Kling, and P. F. Ribeiro, "A Game Theory Strategy to Integrate Distributed Agent-Based Functions in Smart Grids," IEEE Trans. Smart Grid, vol. 4, no. 1, pp. 568-576, Mar. 2013, doi: 10.1109/TSG.2012.2236657.

[14] R. M. Lee, M. J. Assante, and T. Conway, “Analysis of the Cyber Attach on the Ukrainian Power Grid,” E-ISAC, Washington, DC, USA, 2016/ Available:

https://africautc.org/wp-content/uploads/2018/05/E-ISAC_SANS_Ukraine_DUC_5.pdf

[15] E. Irmak and İ. Erkek, "An overview of cyber-attack vectors on SCADA systems," presented at the 2018 6th Int. Symp. Digit. Forensic and Secur. (ISDFS), Antalya, Turkey, Mar. 22-25, 2018, doi: 10.1109/ISDFS.2018.8355379.

[16] J. Hinds, E. J. Williams, and A. N. Joinson, ""It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal," Int. J. Human-Comp. Stud., vol. 143, Nov. 2020, Art no. 102498, doi: 10.1016/j.ijhcs.2020.102498.

[17] L. Floridi, "Establishing the rules for building trustworthy AI," Nat Mach Intell, vol. 1, pp. 261-262, May. 2019, doi: 10.1038/s42256-019-0055-y.

[18] Capgemini, "Our Code of Ethics for AI," Paris, France. Available: https://www.capgemini.com/wp-content/uploads/2021/03/Capgemini_Code_of_Ethics_for_AI_2021_EN.pdf