Roadmap on Digitalisation for Energy Efficiency in Buildings

Background

This roadmap was developed by the Digitalisation Working Group (DWG) of the Energy Efficiency Hub. The roadmap identifies near-term, medium-term, and long-term approaches to address key barriers associated with implementing digitalisation policies and programs to drive energy efficiency in buildings. The IEA estimates that digital technologies have the potential to save 10 percent of energy use in buildings,[1] and therefore can be an important part of an emissions reduction strategy.

The roadmap connects to a report prepared by the DWG entitled, "Digitalisation for the Energy Efficiency of Buildings Operations", released in September 2022.[2] The report describes key digital technologies and approaches relevant to improving building energy efficiency. Studies[3] suggest that these technologies and approaches can be cost-effective and generally have a fast return on investment. However, barriers related to interoperability, data availability and analysis, privacy, and cybersecurity can reduce the energy savings potential of these solutions. The report examines case studies from several countries and identifies common challenges encountered during program implementation.

The roadmap lists key objectives for addressing each barrier related to *interoperability, data availability and analysis, privacy*, and *cybersecurity* and lays out a pathway to achieving these objectives through the use of appropriate practices during program design and implementation. The pathway is split into three phases or steps, where each phase roughly corresponds to:

- **Phase 1:** Development and design of practice(s)
- **Phase 2:** Pilot testing of practice(s)
- **Phase 3:** Large scale adoption of practice(s)

Based on case studies and experiences noted in the DWG report, challenges that may be encountered within each phase are listed, together with recommended practices that can potentially help mitigate them. References to specific examples and case studies in the report are made, wherever applicable. Public and private stakeholders[4] responsible for implementing the practices are also indicated by the following icons:

---

[1] https://www.iea.org/reports/digitalisation-and-energy

[2] The report can be downloaded from the Energy Efficiency Hub website: https://energyefficiencyhub.org/wp-content/uploads/2022/09/DWGReport-1.pdf

[3] Kramer, H., Lin, G., Curtin, C., Crowe, E., & Granderson, J. (2020). Proving the business case for building analytics. Lawrence Berkeley National Lab. (LBNL), Berkeley, CA (United States); and Tricoire, J.-P. (2021, February 22). Buildings are the foundation of our energy-efficient future. World Economic Forum. Retrieved July 7, 2022, from https://www.weforum.org/agenda/2021/02/why-the-buildings-of-the-future-are-key-to-an-efficient-energy-ecosystem/

[4] Private stakeholders may include private industry, trade associations, standard-issuing organizations, and non-profits dedicated to buildings energy efficiency. The authors recognize that there is significant nuance in how stakeholders interact, with high variability from country to country. For example, there may be variations in regulatory oversight and license to operate.

Public

Private

The DWG hopes that the roadmap will be a useful resource to guide policymakers and other stakeholders in their efforts to design programs that promote the use of digital technologies to improve energy efficiency in buildings. The roadmap serves as an overview and quick guide for policymakers and other stakeholders on buildings digitalisation policy tools and levers practiced around the world, common pitfalls related to implementing those digitalisation programs and policies, and possible solutions based on international experience.

The roadmap and linked report can inform multiple stakeholders' needs. For example, **policymakers, program managers** and **utility companies** can explore the various digitalisation policy and program examples referenced in the roadmap (for instance, examples of utility programs that require the use of certified smart thermostats in incentive programs) to help inform their own programs that can motivate businesses and individuals to adopt digital technologies with the potential to enhance energy efficiency in buildings. Practices related to data availability and analytics can equip policymakers and **consumers** with relevant information on cost-effective energy management in buildings. The technology examples embedded in the roadmap and summarized in Section 3.0 of the report can help utility companies and **building energy managers** to make data informed decisions about energy consumption reduction. **Digital technology vendors and service providers** can explore challenges experienced in case studies and use this information to inform the design of products and services.

The roadmap should be broadly applicable internationally as it is based on the insights and experience of several DWG member countries.[5]

[5] United States (lead), Australia, Brazil, Canada, Denmark, European Union, France, Germany, and Japan

Interoperability

Barrier Description: Interoperability refers to the ability for software products and devices to communicate with each other within a building, among other buildings, and with the electric grid and its components.

Phase 1: *Develop and align technical standards and communication protocols*		**Phase 2:** *Deploy policies/programs for technical standards and market facilitation*		**Phase 3:** *Adapt to changes in technology deployment, standards, or policy*	
Challenges	**Practices**	**Challenges**	**Practices**	**Challenges**	**Practices**
Government program managers and industry service providers are not collaborating Government officials and industry service providers must work together to ensure that technology and policy standards align	**Establish government-supported industry task forces** that can play a role in developing technical standards that drive policy. Examples of this include the *Interoperability Steering Committee* [1] in Australia and the *Smart Community Alliance* (JSCA) [2] in Japan.	**Resources are lacking for monitoring effectiveness:** Programs should ensure that customers are receiving competitive energy services.	**Deploy automated communication modules** that can minimize human interaction in communicating energy use data with external market participants and deliver competitive rates in an automated fashion [3].	**Devices and systems can become outdated and may lack necessary functionalities as technology develops:** Devices and systems must adapt to changes in standards or the energy system.	**Develop semantic models capable of processing and analyzing data** in a manner that can be consistently understood by third-party applications.
New digital standards are not compatible with existing protocols: Technical standards must be compatible with existing protocols, particularly regarding cybersecurity and privacy.	**Create multi-sectoral working groups** to ensure that technical standards are being developed in parallel with existing cybersecurity and privacy protocols. For example, Australia's *Cyber Working Group* works in parallel with interoperability policy development to ensure that interoperability is accompanied by robust cybersecurity and privacy measures [1].	**Establishing building connectivity can be expensive when done in isolation:** Efforts should take place to reduce these costs.	**Establish building connectivity as part of normal equipment lifecycle investments** to lower costs [4]. **Coordinate with industry** [4].	**Stacking technologies can lead to conflicting actions taken by digital devices.** For example, there may be a trade-off between temperature control and CO_2 detection in the operation of a smart window [6].	**Improve data dashboards and visualization.** This approach increases device interoperability by more effectively storing, processing, and filtering data. In combination with artificial intelligence technologies, these approaches can ensure that the proper action is taken by smart devices.
		Accessibility to relevant data and tools is low: Without robust incentives, installing and operating technologies can be difficult.	**Create digital hubs for sharing data and monitoring energy use.** This approach can improve consumer access to standards, empower users to understand their energy use across multiple services, and enhance competition between service providers. Several examples have accomplished this [4] [5].		

Key Objectives

- Equip consumers with actionable energy use information.
- Ensure clear communications protocols between consumers and the external market.
- Develop policies compatible with interoperability standards.

Description of Phases

Phase 1: *Develop technical standards and communication protocols*

Achieving the interoperability of digital devices requires a convergence of policy, technology, and infrastructure. Energy efficiency practices such as demand response that are supported by improvements in digital technologies are more likely to succeed. Similarly, deployment of advanced technologies could be accelerated through government incentives or mandates. During the development of standards, we recommend creating task forces that bring together industry experts and policymakers to ensure there is robust technology and consumer support underpinning these policies.

Phase 2: *Develop policies that facilitate market adoption*

Currently, consumers must contend with the expense and complexity of connecting and managing disparate –and oftentimes incompatible—building systems. Interoperability ensures the market for energy services is both competitive and accessible to consumers. Industry and government must work in tandem to make it easy for consumers to compare energy efficiency incentive programs (e.g., rebates on the purchase and installation of smart thermostats) provided by different energy service providers.

Phase 3: *Adapt to changes in technology, standards, or policy*

Digital building systems must adapt to rapid changes in technologies, standards, and policies. Semantic models capable of interpreting a range of data in a standardized format are key to enabling the inclusion of new data in building energy systems. Another concern is that devices may perform conflicting actions in response to certain indicators. The rise of smart building devices necessitates easy-to-read dashboards that can curate data from multiple sources. Additionally, technologies that display energy use data in real time can further incentivize consumer adoption.

Examples cited in the report and other sources:

[1] Distributed Energy Integration Program (DEIP) Interoperability Steering Committee, https://arena.gov.au/knowledge-innovation/distributed-energy-integration-program/

[2] Japan: Universal Home Network Connection Standard Development (Report section C.5) and Information Technology Services Industry Association's Smart House Standardization Study Group Report, https://www.jisa.or.jp/it_info/engineering/tabid/1635/Default.aspx and

[3] Germany: Smart Meter Gateways (Report sections 5.7, C.4)

[4] Australia: The Innovation Hub for Affordable Heating and Cooling (*i*-Hub) (Report sections 5.1, C.1)

[5] Japan: HEMS Dashboard (Report section 3.1.4)

[6] Data availability, quality, and analysis barrier (Report section 4.4)

Data Availability and Analysis

Barrier Description: Data availability refers to the need to have spatiotemporal data and/or device-specific data on building energy use available to end users, digital applications, and service providers. Some datasets are low quality due to a lack of robustness, missing entries, or poorly calibrated sensors (accuracy issues). Data are not intrinsically valuable without analysis that informs and enables program implementation, from automated load shifting to behavioral change.

Phase 1: *Data acquisition, infrastructure, and pilot project implementation*		**Phase 2:** *Adoption through policy and augmentation*		**Phase 3:** *Quality assessment and optimization*	
Challenges	**Practices**	**Challenges**	**Practices**	**Challenges**	**Practices**
Data collection infrastructure is underdeveloped: Smart metering networks must have the capacity to collect large sums of data at high resolution across many devices in a secure and interoperable manner. In addition, behind-the-meter data is also challenging to collect. *[For information on smart meters, see Section 3.1.2 of the report.]*	**Subsidize installation of smart metering networks to incentivize participation.** For example, Brazil has implemented several subsidized pilot projects aimed at integrating smart metering systems in buildings [1]. **Develop secure information exchange technologies.** For example, Germany's Smart Meter Gateway (SMGW) program has successfully secured data sharing among devices [2] [3].	**End-user data sharing may not exist:** Encouraging users to share energy consumption data can help drive policy and contribute to greater understanding of the energy system.	**Introduce data release mandates** and **data sharing incentives.** Denmark has implemented data release mandates that have proven effective for extensive data collection across the building energy system [7]. Additional incentives for building renovation include tax deduction schemes for the inclusion of new energy-saving smart devices [8]. **Establish public-private partnerships** around data sharing that consider behind-the-meter data. These partnerships can involve **building owners** and **tenants** [9] [10].	**Current datasets may be too broad or lack the resolution needed for some analysis:** Improvement of data granularity is key to improving the ability for new policy, technology, and research domains.	**Deploy new technologies, incentives, and comprehensive certification schemes** that can help improve the granularity of energy consumption monitoring.
Data analysis methods are not standardized: Methods must be developed to analyze large quantities of data and to enact the appropriate analysis.	**Support machine learning and advanced control algorithms R&D** to ensure data can be analyzed to accurately inform how consumers use energy [4]. **Develop energy certification schemes** to ensure there are standardized methods for implementing policy based on energy consumption data [5].	**Consumer awareness is low:** Consumers may not know how to use and interpret their energy consumption data in accordance with existing policies and practices.	**Carry out information awareness campaigns** to help improve the accessibility of energy consumption data and ensure consumers know how to adequately make dynamic decisions on energy use based on their consumption data [8].	**Necessary data for building energy efficiency policy is unavailable or kept private:** Data must be accessible to adequately inform large-scale policy.	**Improve privacy and cybersecurity measures** to ensure data can be transmitted and used at large scale to inform new policy decisions.
Computational infrastructure is insufficient: Infrastructure to store and transmit large amounts of data in a way that is accessible to **utilities**, **consumers**, and **policymakers** must exist.	**Develop databases that host analytics of building energy usage from a broad range of devices** to make building energy use information more accessible and meaningful [6].	**Cooperation between public and private sector is lacking:** These partnerships are required to ensure that policy is backed by technology.	**Incentivize industry-led participation in the development of new energy data management technologies** to help improve technological development and ensure that policy and technology are aligned [11].		

Key Objectives

- Develop infrastructure capable of accommodating many devices across the energy system and delivering granular data in real time.
- Equip consumers with the data and resources to make decisions regarding their energy consumption.
- Incentivize government-industry partnerships to lead improvements in data availability, quality, and analysis.

Description of Phases

Phase 1: *Data acquisition, infrastructure, and pilot project implementation*

Government and industry must collaborate to develop infrastructure capable of collecting, analyzing, certifying, and distributing data from a wide range of devices across the energy system. Computing power is also needed to process large quantities of information and make it actionable to consumers and policymakers.

Phase 2: *Adoption through policy and augmentation*

Policy mandates must support meaningful data collection and analysis procedures. Data-release mandates are vital in ensuring that relevant data can be collected and distributed to all parties who need access to it.

Phase 3: *Quality assessment and optimization*

Greater deployment of energy use monitoring devices will improve the granularity and quality of data. Additionally, new energy use certification schemes can ensure data is being applied in a useful manner.

Examples cited in the report and other sources:

[1] Brazil: Law 9991 of 2000 (Report sections 5.2, C.2)
[2] Germany: Smart Meter Gateways (Report sections 5.7, C.4)
[3] Australia: NatHERS (Report section: 5.0)
[4] Australia: i-Hub (Report sections 5.1, C.1)
[5] Germany: AI Strategy of the Federal Government (Report section 5.7)
[6] Denmark: Energy Performance Certificate database (Report sections 5.5., C.3)
[7] Denmark: Releasing Electricity Distribution Data (Report sections 5.5., C.3)
[8] Denmark: Implementation of the "Energy Performance of Buildings Directive" in Denmark, https://epbd-ca.eu/ca-outcomes/outcomes-2015-2018/book-2018/countries/denmark
[9] United States: Smart Energy Analytics Campaign, https://betterbuildingssolutioncenter.energy.gov/alliance/technology-campaigns/smart-energy-analytics-campaign
[10] New York State Energy Research and Development Authority (NYSERDA) Real Time Energy Management, https://www.nyserda.ny.gov/All-Programs/real-time-energy-management
[11] United States: Green Button Initiative (Report sections 5.9, C.6)

Privacy

Barrier Description: Privacy refers to consumer concerns about the mass collection of granular data on energy use and associated personal information. Consumers are worried about how data will be used, where the data are stored, and who can access the data.

Phase 1: *Planning of infrastructure for data handling and transmission*		**Phase 2:** *Pilot-scale implementation of privacy protection procedures*		**Phase 3:** *Wide-scale deployment of privacy protocols and data handling procedures*	
Challenges	**Practices**	**Challenges**	**Practices**	**Challenges**	**Practices**
Data on energy consumption is very sensitive: However, state of the network, generation, and consumption data are necessary for system functions [1].	**Determine the data retention period, where data is stored, and how often data is transmitted** based on the time resolution of measurements and data type [2]. Each actor (e.g., **utility company**, **building manager**, **building owner**, **government official**) should only receive the data needed to carry out its tasks [1]. **Enact data handling regulations** that includes data protection, data security, and data sovereignty [1].	**Smart meter data from individuals can lead to privacy and physical security concerns:** sensitive consumption data must be adequately protected [4] [5].	**Collect smart meter data via joint meter reading** to connect equipment owned by externally connected **businesses** and smart meters [2]. Each actor (**building owner and utility company**) should receive data directly from devices when relevant [1]. **Anonymize and pseudonymize measurements** [1]. **Aggregate measurements in the SMGW** [1]. **Aggregate metering data on a building level** that is shared by **utility companies** with building owners or managers [5]. **Allow entities that are not energy service providers to access smart meter data only through an accreditation process** [6].	**Consumers worry about misuse of their data:** consumers should feel confident about data handling practices employed after the consumers agree to share their data [1].	**Create logbooks for data processing steps that are accessible by consumers** [1]. **Require data owners (e.g., utility companies) to gain consumer permissions** prior to sharing data with third-party service providers [3]. **Require consumer facing tools to provide data only post-authentication of the user** [3].
				Certifications of some products and software require data from real-world tests: The certification process itself should adhere to appropriate privacy measures [3].	**Only transfer aggregated data to a certification group** [3].

Key Objectives

- Address consumer protection. Consumers should feel that their data is safe from misuse and unauthorized access. To achieve greater market penetration consumers must be able to trust the companies that manage their data. Government entities can reduce this current lack of trust by enacting and enforcing clear regulations on data storage, handling, and transmission.
- Use smart meter data responsibly. Smart meter data often contains very granular energy consumption information which can convey socioeconomic and occupancy information of end consumers. Smart meter data should be used responsibly with strong privacy protections in place to protect end users from social engineering, blackmail, and physical security threats.
- Protect proprietary information. Companies that feel their proprietary information is protected may be more likely to cooperate in digitalization efforts and share data essential to energy.

Description of Phases

Phase 1: *Planning of infrastructure for data handling and transmission*

Design of privacy protocols requires proper planning and coordination of data handling. Planning must be standardized and regulated to ensure that data is transmitted to the appropriate parties.

Phase 2: *Pilot-scale implementation of privacy protection procedures*

Pilot testing requires collection of individual energy consumption data, requiring concerted efforts to ensure that data is anonymized and transmitted in a secure manner.

Phase 3: *Wide-scale deployment of privacy protocols and data handling procedures*

At the large-scale level, consumers may be worried about the misuse of data. This phase often requires real-world data to appropriately certify products. At large scale, there must be particular attention to how energy certification schemes interact with individual privacy protection.

Examples cited in the report and other sources:

[1] Germany: Act on Digitalisation for the Energy Transition (Report section C.4)
[2] Japan: Next Generation Smart Meter System Study Group Summary (Report section C.5)
[3] United States: Green Button Initiative (Report sections 5.9, C.6)
[4] Privacy barrier (Report section 4.1)
[5] France overview (Report section 5.6)
[6] Japan: Electricity Business Act, https://www.meti.go.jp/english/press/index.html

Cybersecurity

Barrier Description: Cybersecurity refers to risks associated with digital technologies for building energy efficiency relying on internet connections and computer networks. All digitally connected devices are at risk for attacks, from building management systems to smart appliances.

Phase 1: *Planning and design of cybersecurity frameworks*		**Phase 2:** *Pilot-scale implementation of cybersecurity frameworks and "security by design"*		**Phase 3:** *Continued maintenance of cybersecurity frameworks for wide-scale deployment*	
Challenges	**Practices**	**Challenges**	**Practices**	**Challenges**	**Practices**
A single set of technical security standards may not be implementable by all digitally connected devices and tools: Security standards should be adequately flexible and allow for various technical implementations [1].	**Create and use protection profiles** [1].	**Smart meter functions might accidentally result in energy supply disruptions that affect operations within buildings:** Unintended consequences and malfunctions should be avoided [1].	**Set a minimum service level/set of functionalities that must be met by business operators and ensure their security framework allows this level to always be met** [2].	**Security incidents, implementation problems, needs for updates, and/or data leaks may occur:** Cybersecurity planning and implementation should be a continuous, iterative process [1].	**Implement continuous improvement for threat and leak monitoring** [2]. **Require secure software updates** [1]. **Certify software updates before implementing** [1]. **Certify hotfixes after implementing** [1]. **Encourage manufacturers to show ability to update software without replacing hardware** [1].
Security standards may be decentralized and vary between manufacturers: Security standards should instead be centralized and uniform [1].	**Create a rigorous federal certification process that includes annual surveillance audits and recertifications** [1].	**Connected devices and networks can serve as access points for attackers:** Safeguards should be enacted to prevent connected devices and networks from being access points to other devices and systems in the building [3].	**Practice secure design** [1]. Separate internal and external connection networks [1] [2]. **Monitor external communication logs** [2]. For external connection providers, **assign responsibility to report incidents and conduct risk assessments** [2]. **Use certified smart meter gateways** (SMGWs) as the communication platform [1]. **Encrypt communication channels** [1].	**Consumers are concerned about third-party theft of their data:** Consumers should be able to have confidence that their data is protected from unauthorized third parties [1].	**Use electronic identifiers and allow only known participants/devices to access data** [1]. **Use public key infrastructure for data sharing to enable mutual authentication** [1]. **Encrypt communication channels** [1]. **Secure communication paths cryptographically** [1].

Key Objectives

- Secure operation and data transmission. Vulnerabilities, according to the United States Department of Homeland Security, are physical features or operational attributes that render an entity open to exploitation or susceptible to a given hazard. Connected devices and networks, which can be infiltration points, should be secured and data transmission should occur in a manner that mitigates risk of a cyberattack on a building or building system occurs.
- Incorporate security into all digitalization tool lifecycle phases. Technical and regulatory decisions can be impactful across sectors and shape market design. To reduce unintended consequences and unaddressed security concerns, cybersecurity awareness should begin with policy planning and the design of digitalization tools, consider future technology developments and needs, and continue through all remaining phases of the policy and tool life cycles.

Description of Phases

Phase 1: *Planning and design of cybersecurity frameworks*

Design of cybersecurity protocols are challenging due to the variable nature of devices and technologies which make it difficult to implement universal standards. Developing approaches to cybersecurity design, including protection profiles and a rigorous certification process are key to building effective cybersecurity frameworks.

Phase 2: *Pilot-scale implementation of cybersecurity frameworks and "security by design"*

Smart meters and connected devices can be points of vulnerability for cybersecurity attacks. Coupling policy with technological development (cybersecurity by design) can lower risk associated with these points of vulnerability.

Phase 3: *Continued maintenance of cybersecurity frameworks for wide-scale deployment*

At the large-scale level, there must be a variety of initiatives to monitor security breaches and appropriately respond to them. Cybersecurity frameworks must be dynamically updated to respond to threats in real time, requiring innovations in both technology and policy.

Examples cited in the report and other sources:

[1] Germany: Act on Digitalisation for the Energy Transition (Report section C.4)
[2] Japan: Next-Generation Smart Meter Study Group Summary (Report section C.5)
[3] Cybersecurity barrier (Report section 4.2)