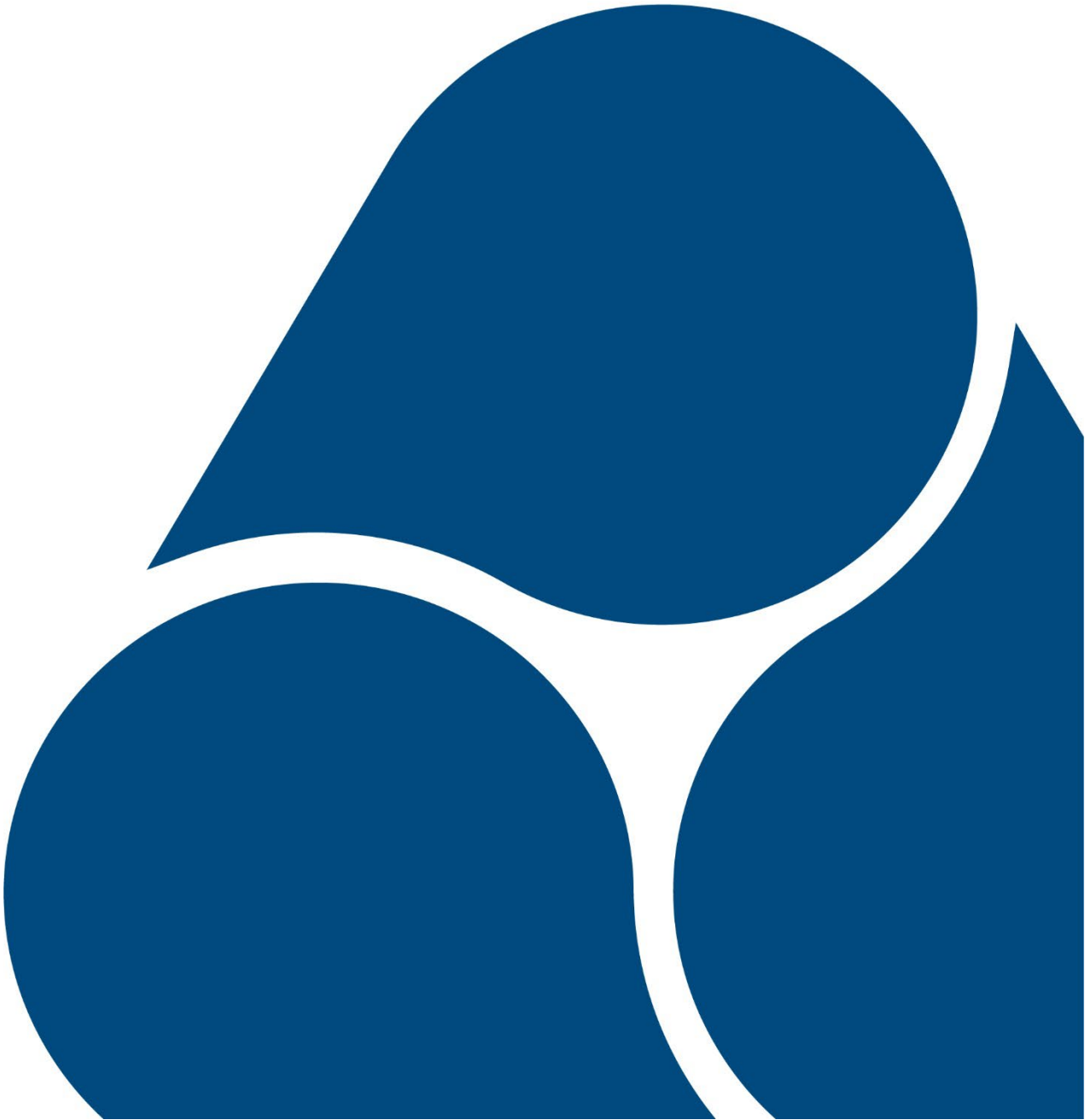
Office for Product
Safety & Standards

Safety of Smart Domestic Appliances

A review of the safety risks of time-shifting and internet connectivity

March 2023



Acknowledgements

This independent research report was produced by Mott MacDonald. The study was undertaken between September 2018 and May 2019 and updated in 2022.

The views expressed in this report are those of the authors, not necessarily those of the Office for Product Safety and Standards or the Department for Business, Energy & Industrial Strategy (nor do they reflect Government policy).

The following organisations were consulted as part of this project:

- Association of Manufacturers of Domestic Electrical Appliances (AMDEA)
- BEIS
    - Office for Product Safety and Standards
    - Energy Security, Networks & Markets
    - Science & Innovation for Climate & Energy
    - Smart Metering Implementation Programme
- Department for Digital, Culture, Media and Sport (DCMS)
- Electrical Safety First
- Electrolux
- Intertek
- London Fire Brigade (LFB)

We are grateful to all respondents for their time and insights.

Contents

Executive Summary

Context

Smart, flexible energy can help drive the transition towards a future low carbon energy system, whilst bringing significant benefits for consumers, the energy system and the wider economy. A smart system can reduce costs by up to £10bn a year by 2050, by reducing the amount of new generation and network needed to meet increased electricity demand[1].

The Government believes that harnessing the full potential of smart energy technologies, including demand-side response (DSR), is key to maximising the efficiency of the emerging energy system, and to the delivery of secure, affordable and clean energy now and in the future. The Government is working closely with Ofgem and industry to support the transition to a smarter, more flexible energy system, with the aim to establish a best-in-class regulatory framework.

DSR can help consumers save money as well as reduce system costs by enabling consumers to use more electricity when energy is plentiful and cheaper, and reduce consumption when energy is scarcer and more expensive. As set out in their joint Smart Systems and Flexibility Plan[2], the Government and Ofgem are putting in place the infrastructure, and supporting measures, to enable consumers to participate in the emerging smart energy system.

Safety of smart appliances

Smart appliances are key to the ability of domestic consumers to participate in, and enjoy the benefits of, the emerging smart energy system. In supporting this transition, the Government wants to ensure that consumers are appropriately protected.

The Government intends to set regulatory requirements for certain Energy Smart Appliances (ESAs)[3] that are suitable for flexible consumer use, to support their uptake and to guard against potential risks relating to interoperability, data privacy, grid stability and cyber security. In tandem, with Government sponsorship, the British Standards Institution has published technical standards for certain smart appliances[4], including electric vehicle (EV) chargepoints.

---

[1] BEIS (2021) Smart systems and flexibility plan. https://www.gov.uk/government/publications/transitioning-to-a-net-zero-energy-system-smart-systems-and-flexibility-plan-2021

[2] Ibid.

[3] The Government proposes to set regulatory requirements for domestic-scale ESAs with the highest flexibility potential for the energy systems and consumers. This includes private EV charge points, electric heating appliances (including heat pumps, heat batteries and storage heaters) and batteries. Other ESAs such as white goods may also be included in scope of regulation further into the future, as consumer uptake grows, and markets mature. .

[4] https://www.bsigroup.com/en-GB/about-bsi/uk-national-standards-body/about-standards/Innovation/energy-smart-appliances-programme/: these technical standards relate to cold appliances, wet appliances, heating, ventilation, air conditioning, battery storage, and EV chargepoints, and are underpinned by the same set of principles guiding regulation: interoperability, data privacy, grid stability and cyber security.

This report is therefore timely. It outlines potential safety features that smart appliances may provide, and identifies any potential safety risks related to the use of certain smart appliances, so that any necessary mitigation measures can be put in place in good time.

The cohort of appliances under consideration in this report has been limited to cookers, dishwashers, fridge/freezers,[5] tumble dryers and washing machines, which together account for about two thirds of domestic appliance fires in the UK.

Almost 15% of such domestic appliances sold in 2018[6] were equipped with internet connectivity. This might be offered to add new features or functionality, or to enable operation of the appliance to be time-shifted to take advantage of lower-priced electricity. A reduction in the price premium, and the introduction of new internet-enabled services, could result in it becoming a standard feature on even the lowest cost models.

The impact on safety of two important features that are enabled by an internet connection are considered by this report: "time shifting" (which is a form of DSR), and the downloading of software updates, as well as how any potential risks that are identified can be mitigated.

The analysis in this report shows that mitigating actions are required to avoid the potential increase in risk of fatal house fires[7] due to time-shifting. In addition to mitigating the potential risks, the analysis also identifies an opportunity to leverage the functionality that internet-enabled products can provide to further enhance the safety of those consumers that opt to use smart appliances. This report recommends how Government and industry can build on work already underway to address any such safety risks, and to ensure that there is appropriate mitigation in place before the risks outlined become realised.

It is also worth noting that, in a world where consumers replace old appliances with new smart-enabled appliances, there will be a significant improvement in standards as newer appliances must meet more stringent safety requirements. This report does not address this consumer benefit, and instead focuses on the specific impact of the smart element of these new appliances.

Time-shifting of Domestic Appliances

For many years, it has been possible to operate appliances at times when the occupants are either asleep or not at home. However, new functionality offered by smart appliances will encourage more consumers to benefit from cheaper electricity tariffs by intelligently time-shifting electrical loads away from periods of peak demand. This will help to reduce UK carbon emissions by optimising the use of lower carbon sources of electricity. It will also reduce the investment required in additional generating capacity or reinforcement of distribution networks. This report assumes that the appliances most likely to be used for DSR[8] are higher-energy-consuming devices with loads that can be shifted in time, such as washing machines, tumble dryers or dishwashers.

This report assumes that 20% of all UK washing machines, tumble dryers and dishwashers will be smart appliances by 2030, and that these will operate in smart mode,

[5] Fridge/freezer is defined as a domestic fridge, freezer or combined fridge/freezer.
[6] 14.5% of sales were recorded as having a smart connection; 71.8% had no smart connection, and 13.6% were unknown. (Source, GFK)
[7] Which? (2018) Revealed: the brands linked to the most appliance fires.
https://www.which.co.uk/news/2018/02/revealed-the-brands-linked-to-the-most-appliance-fires/
[8] Time-shifting is a specific type of DSR.

i.e. time-shifting, 80% of the time. In addition, we assume that, while rare, fires in time-shifted appliances are more likely to result in casualties and fatalities when users are not present to take action to protect themselves and their property, e.g. at night.

If mitigating measures are not adequately put in place, fires that occur while householders are asleep could develop into life-threatening incidents. Our modelling[9] has shown that, without appropriate mitigation in place, an additional 12 fires with casualties and 1.1 fatalities could occur each year from 2030 (an increase of 1.3%).[10] This is likely to overestimate the risk because we have assumed that all of the time-shifting happens to a period of the day where there is a higher risk of fatality; in reality, much time-shifting may happen at times of day when homeowners are both present and awake, e.g. late evening or early morning. Although we do not have evidence to assess the periods to which consumers will time shift, it is expected that some consumers will avoid periods when they are asleep if the appliance is loud enough to keep them awake.

This increased risk is not forecast to be realised until 20% of all UK households are time shifting smart appliances 80% of the time that they use these appliances, which is unlikely to happen much earlier than 2030, which allows sufficient time to establish mitigating measures. For example, additional safety standards could be developed and existing standards will be updated that decrease the risks of fires resulting in casualties. Additionally, smart appliances will offer opportunities to improve safety such as through condition monitoring and simplified recalls. According to our modelling, we estimate that if this risk is reduced by at least 6.5%, there would be no net increase in casualties and fatalities. This is important to consider given that work on mitigation is already underway.

Hence, our modelling has shown that smart domestic appliances pose a small increased risk to fire safety when time-shifted. There is an opportunity to offset that projected risk, and to actually *increase* safety, if the right mitigation measures are established in good time.

Faulty or Malicious software

The concept that safety can be assured in the design phase of an appliance fails to recognise that changing the software in a smart appliance is changing the design. Consequently, a design that was once very safe could be rendered unsafe by a malicious or poorly written software download.

The additional complexity that is inherent in smart appliances, and the novelty of some of their features, makes it potentially more likely that they will contain design vulnerabilities. In theory, rigorous software engineering will detect and eliminate all such problems before the software is released. In practice, proving that software is error-free is difficult, and some vulnerabilities may be present.

To reduce this risk, appliance manufacturers should ensure that they, and companies in their supply chain, adhere to consumer Internet of Things (IoT) security standards and best practice[11] to ensure that their products are properly secured against current and evolving threats. Users of smart appliances can protect themselves by following advice

[9] Based on recent LFB statistics for fatal house fires caused by faulty appliances.
[10] The assumptions supporting this result are described more fully in 5.2.
[11] Such as the DCMS Code of Practice and ETSI Technical Specification 303 645.

given by DCMS and the National Cyber Security Centre.[12] Building on this, DCMS have recently introduced a bill to regulate the security of consumer connectable products by mandating security requirements based on the top three requirements of the Code of Practice[13]. Additionally, as noted above, the Government has introduced primary legislation in the Energy Security Bill[14] which seeks enabling powers to set regulatory requirements for certain energy smart appliances, and has worked with industry to develop appropriate technical standards in tandem, with cyber security a key principle[15]. The standards (PAS 1878 and 1879) were published in 2021. The Government has also published a consultation[16] which focuses on how these primary powers would be implemented. The consultation sets out proposals to ensure consumers and electricity system are protected, and seeks views on ongoing work by government to establish system-level cyber security requirements for energy smart appliances. The proposals focus on larger domestic-scale energy smart appliances including electric vehicle charge points, batteries, and heating appliances (such as heat pumps).

While it should be stressed that there have to date been no reported incidences of malware[17] compromising the safety of an appliance, malicious software could attempt to cause damage, for example by:

- Turning on the heater in a washing machine without any water in the drum.
- Turning off a tumble dryer during the last phase of the drying cycle.
- Opening the water supply valve in a washing machine or dishwasher.
- Creating an out-of-balance load during the spin cycle of a washing machine.

More generally, switching an appliance on and off very frequently can lead to over-heating of critical components. It can also lead to degradation of components which can result in failure.

Where software is being used to control a device that could fail in a way that might lead to fire, it is therefore important that the back-up safety mechanism (such as a thermal cut-out or time-delay feature) should be implemented in hardware rather than software.

Advantages of internet connection

As outlined above, a key feature of smart appliances is the ability to enable services such as DSR. With the increase in the electrification of heat and transport, electricity demand is expected to rise, and the transition towards a net zero economy means we will need to integrate increasing volumes of intermittent renewables, making DSR ever more important

[12] NSCS (2019) Smart devices: using them safely in your home. https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home
[13] DCMS (2021) The Product Security and Telecommunications Infrastructure (PSTI) Bill – product security factsheet. https://www.gov.uk/guidance/the-product-security-and-telecommunications-infrastructure-psti-bill-product-security-factsheet
[14] BEIS (2022) Energy Security Bill. https://www.gov.uk/government/collections/energy-security-bill
[15] BSI Energy smart appliances programme. https://www.bsigroup.com/en-GB/about-bsi/uk-national-standards-body/about-standards/Innovation/energy-smart-appliances-programme/
[16] BEIS (2022) Delivering a smart and secure electricity system: the interoperability and cyber security of energy smart appliances and remote load control. https://www.gov.uk/government/consultations/delivering-a-smart-and-secure-electricity-system-the-interoperability-and-cyber-security-of-energy-smart-appliances-and-remote-load-control
[17] 'Malware' is defined as software designed to infiltrate and damage computer systems without the user's consent.

in balancing the system. Smart appliances allow consumers to provide this flexibility and realise the benefits that DSR offers.

Additionally, while internet connectivity of white goods could pose safety risks as outlined above (which can partly be mitigated by good design, installation and update practices), it also offers possibilities for innovative services that would improve product safety. These include:

- Enabling remote control and monitoring of an appliance by the user.
- Enabling proactive maintenance based on appliance condition using low cost sensors.[18]
- Alerting the user to a product recall, with automatic disabling of the appliance in the case of serious faults.
- Downloading of new software to fix faults.
- Running of an appliance in a “safe” mode while awaiting repair.
- Manufacturers could also use data from the installed base of appliances to improve the design of new products (in accordance with the data protection regulations and user agreement).

Technical Standards

Alongside the technical standards for certain smart appliances noted above, there are several other important technical standards that will impact decisions made on the design of smart appliances:

- An updated version of BS EN 60335: Household and similar electrical appliances – Safety is under development that will for the first time consider issues such as cyber-attacks or malicious software downloads.
- To gain presumption of conformity with the Radio Equipment Regulations, manufacturers normally adhere to the designated standard IEC 60730-1. However, standards are generally voluntary; a manufacturer can use other routes to demonstrate compliance with legislation.

[18] Atlas, The average cost of IoT sensors is falling. https://www.theatlas.com/charts/BJsmCFAI

1 Introduction

This report studies the safety risks associated with domestic appliances that are connected to the internet, which in 2018 represented 15% of unit sales.[19] The aim of this work is to improve the evidence base and to suggest mitigating measures to help inform policymakers and other stakeholders with an interest in this subject. Domestic appliances are a significant cause of house fires,[20] and internet connectivity could introduce new risks that would adversely impact occupant safety, if mitigation action is not taken. This report examines two important safety issues:

- For the purposes of Demand Side Response (DSR), smart appliances may operate at times when people are not nearby to take mitigating action, which could potentially make the consequences of any fire more serious.
- Downloading of faulty software or malware, either deliberately or through poor design, which could alter the operation of the appliance and compromise safety.

The report starts with an analysis of historic domestic appliance fires in order to create a baseline for fatalities and casualties against which the change due to time shifting can be compared. Existing data shows that the incidence of domestic fires correlates with grid electricity demand, indicating that most domestic fires could be associated with human activity. Using this and other assumptions, the report makes estimates of the likely potential increase in fatalities and serious injury due to time-shifting, with the analysis repeated for different assumed penetrations of smart appliances.

The report explores how new features and services might make smart appliances an increasingly popular option.

The report considers what failures might occur as a result of faulty software or malware being downloaded on to a smart appliance. While some engineering judgement has been necessary, it is apparent that the types of failure that might be expected are largely the same as with non-internet connected devices. The principal observations are that traditional appliance manufacturers should have direct access to designers with software engineering and cyber security skills, and that hardware sensors and controls should be used in critical parts of the design to reduce the vulnerability to failure due to faulty software or malware. It is of note that there have to date been no reported incidences of malware causing a domestic appliance to fail, but as this sector develops it will become even more important that manufacturers take appropriate precautions to mitigate the possible risks.

The final section of the report features a review of applicable technical standards, which shows that ongoing work is needed to keep standards up to date with advances in technology.

[19] Sales of smart large domestic appliances are increasing, with 14.5% of sales in 2018 recorded as having a smart connection. 71.8% of the remainder had no smart connection, and 13.6% were unknown. Source: GfK.

[20] Which? (2018) Revealed: the brands linked to the most appliance fires. https://www.which.co.uk/news/2018/02/revealed-the-brands-linked-to-the-most-appliance-fires/

Many of the product safety issues discussed in this report arise as a result of cyber-security issues. If cyber-security is compromised, this can lead to safety issues. While this report addresses the product safety implications, it excludes detailed consideration of wider cyber-security issues.

The scope of this report was limited to Cookers, Dishwashers, Fridge/Freezers, Tumble dryers and Washing machines, which together account for about two thirds of domestic appliance fires in the UK (See Table 1).

In this document, the term “smart appliance” refers to a networked appliance in which the majority of the internal control functions have been implemented in software running on a microcontroller.

2 Appliance safety issues

2.1 Types of appliances at risk

Government statistics show that there were an average of 17,670 domestic appliance fires per year in England between 2010 and 2016.[21] However, the definition of "domestic appliance" is very wide and includes items such as battery chargers, paint strippers, camping stoves and PC equipment.

Table 1 shows that there was an average of 11,259 fires per year in England between 2010 and 2016 associated with these large domestic appliances, representing 63.7% of appliance fires.

Table 1: Fires caused by Large Domestic Appliances

Type of Appliance	Average number of fires / year	Proportion of fires (%)	Proportion of ALL appliance fires (%)	Probability of being time-shifted
Cooker including oven	9,284	82.5%	52.5%	Very low
Tumble dryer	659	5.9%	3.7%	High
Washing machine	614	5.5%	3.5%	High
Dishwasher	362	3.2%	2.1%	High
Fridge/freezer	264	2.3%	1.5%	Low
Combination washer dryers	76	0.7%	0.4%	High
Total	**11,259**	**100%**	63.7%	

Source: Domestic Appliance Fires Dataset Guidance, Home Office, 10 May 2018, p10. DSR column: Mott MacDonald.

These statistics include fires caused by user error as well as technical faults. Data provided by the London Fire Brigade suggests that approximately 85% of fires in washing machines, tumble dryers, dishwashers, and fridge/freezers are caused by technical faults,

[21] Publishing Incident Recording System data on the fire and rescue service at an incident level: Domestic Appliance Fires Dataset Guidance, Home Office, 10 May 2018, p10. The dataset is sourced from fire and rescue services, comprising of primary dwelling fires in England where the source of ignition was a domestic appliance.

while about 15% are caused by incorrect installation or operation. The figures for cookers are very different, with around 6% of cooker fires being caused by technical faults, and 94% being caused by incorrect installation or operation.

Applying these percentages to the figures in Table 1 suggests that the average number of appliance fires in England caused by technical faults is approximately 2,235 / year. This implies that there are about 2,657 fires / year in the UK as a whole caused by technical faults.[22] However, we understand that the fire service tends to attribute fires to misuse rather than a design fault if no fatality has occurred, so the proportion of fires caused by design faults may actually be higher than the percentages given above. This view seems to be supported by estimates produced by the consumer magazine Which? that suggest an average of 3,103 fires per year in the UK caused by faulty appliances and their leads.[23]

The final column of Table 1 indicates appliances that are most suitable for shifting the demand for electricity from peak to off-peak periods when participating in DSR schemes.

Tumble dryers, washing machines and dishwashers are most likely appliances to be time-shifted because:

- They are amongst the most significant users of household energy.
- Unlike cookers, the exact time at which the appliance runs is often not critical.
- Although they are significant users of energy, current designs of domestic fridge/freezer do not have the capability to be time shifted.

While there have been no reported incidences of malware compromising the safety of an appliance to date, the growth of smart appliances that can connect to the internet or other public or private networks[24] could lead to fires being deliberately caused by hackers. In addition to the large appliances listed in Table 1, other domestic appliances that could potentially be attacked in this way include microwave ovens,[25] grills and toasters.[26]

As the costs of providing internet connectivity drop, manufacturers are likely to include this functionality in lower-cost appliances. This suggests that the findings of this project could become increasingly significant in the coming years.

[22] The population of England is assumed to represent 84.1% of the population of the UK.
[23] The consumer magazine Which? reports that there were 6,206 household fires across the UK caused by faulty appliances and leads between 1st April 2014 and 31st March 2016. This equates to an average of 3,103 fires per year. The cause of the fire is based on the professional opinion of a fire officer, but is not forensically investigated. https://www.which.co.uk/news/2018/02/revealed-the-brands-linked-to-the-most-appliance-fires/
[24] Some appliances might have a direct Internet connection (such as a WiFi link to a home router). Other appliances may be linked to a mobile phone by Bluetooth or a mobile data service, and there is at least one appliance connected by text messaging. We consider that any connection to a public network is potentially unsafe.
[25] 1,022 fires / year in England between 2010 and 2016.
[26] 1,972 fires / year in England between 2010 and 2016.

2.2 Appliance-specific safety issues

Safety issues that have been identified by investigations of failed domestic appliances are discussed below. None of these fires were caused deliberately by internet-based attacks of the sort discussed in this report, but some of them could perhaps have been triggered accidentally by a remote action. For example, if an oven has a build-up of fat deposits, then switching it on remotely could be the trigger that starts the fire. The consequences of such fires are likely to be considerably more serious if the user is not present.

All appliances are vulnerable to fires caused by poor maintenance, faulty components or improper usage. However, most of the problems listed in the following sections are specific to certain types of appliance.

2.2.1 Cookers

Most cooker-related fires are caused by user error rather than equipment failure, but this means that the user is normally available to deal with any fire as soon as it starts. Although more than half of domestic appliance fires originate at the cooker, the cooker is only responsible for 2% of fire-related fatalities.[27]

Causes of cooker fires include:

- Cooker left unattended while a meal is being cooked.
- Fat deposits in the oven's internal ducting.
- Plastic items left inside oven.
- Fault in heating element or gas burner.
- Resistive heating on spade connector.
- Electrical fault causing gas inlet pipe to arc against the appliance.
- Oven turned on by accident.

The dangers of leaving a cooker hob unattended while turned on are obvious, so this should rule out the possibility of being able to turn on a hob via an internet connection[28]. However, it appears that there is nothing in current legislation to prevent an oven from being remotely controlled, and many ovens have built-in timers that allow them to operate while unattended. Norway has passed a law that requires the installation of a cooker safety device in every new kitchen to reduce the risk of cooking fires. These intelligent devices[29] can detect a situation in which a fire is likely to start before any toxic gases have been produced.[30]

[27] Source: Fire Facts London 1, London Fire Brigade, Worksheet 3.4.
[28] Clause 22.40 of BS EN 60335-2-6 states that "Hobs shall not be controlled by a remote operation".
[29] Innohome https://innohome.com/innohome/
[30] The European Stove Guard Standard EN 50615 ("Particular requirements for devices for fire prevention and suppression for electric hobs") was published on March 6, 2015, by the European Committee for Electrotechnical Standardization.

2.2.2 Washing machines

Causes of washing machine fires include:

- High currents associated with heater elements can result in a Printed Circuit Board (PCB) failure.
- The heater control relay can become stuck in the on position.
- Wear and tear on the door switch can lead to resistive heating of the contacts.
- Damage to motors, belts, bearings or other moving parts can cause overheating as a result of friction.
- Motor windings can overheat if the drum is unable to rotate or is overloaded with clothes.
- Motor start / run capacitor failure.[31]

2.2.3 Tumble dryers

Causes of tumble dryer fires include:

- Lint/fluff from clothes coming into contact with the heating element.
- Stopping a tumble dryer by turning the power off during the last quarter of the drying sequence. Whilst a tumble dryer is running, a fan blows air over the heating element and keeps it at the desired temperature. If the power is cut, the fan will stop immediately but the heater will continue giving off heat for a while. If dry clothes remain in the drum with the door shut, then they can start to smoulder.
- Clothes contaminated with flammable solvents or oils (including organic cooking oils) may not be properly cleaned if they are washed on a low-temperature cycle, thereby leaving a source of ignition when the clothes are placed in the tumble dryer.
- Overheating in the heating element.
- High currents associated with heater elements can result in PCB failure.
- Wear and tear on the door switch can lead to resistive heating of the contacts.
- Damage to motors, belts, bearings or other moving parts can cause overheating as a result of friction.
- Motor start / run capacitor failure.

2.2.4 Dishwashers

Causes of dishwasher fires include:

[31] It is noted that the use of Variable Speed Drives can eliminate the need for motor start and run capacitors, although these devices can also introduce other problems.

- High currents associated with heater elements can result in PCB failure.
- Wear and tear on the door switch can lead to resistive heating of the contacts.
- Heating element still energised after water pump failure.
- Moisture can cause short circuits between electrical wiring.
- Motor start / run capacitor failure.

2.2.5 Fridge/freezers

Table 1 shows that fridge/freezers only cause about 1.5% of appliance fires. However, the fires that they cause tend to be more serious than for other appliances because they contain flammable refrigerant, and because they can occur when nobody is around to take mitigating action.

A small fire can spread rapidly if it encounters escaping refrigerant (e.g. isobutane) or polyurethane foam insulation. Within minutes, it may have engulfed the whole appliance and any flammable materials that happen to be nearby. If the refrigerant explodes, it can cause an increase in air pressure that can blow out windows. Failure of the motor start capacitor is reported as being the most common cause of failure.[32] These capacitors may fail due to age, damage, manufacturing defects, improper installation or incorrect repairs.

Other causes of fridge/freezer fires include:

- Blocked air vents caused by a build-up of dust or fluff.
- Overheating of defrost timers in fridge/freezers, attributed to short-circuiting as a result of water ingress.
- High currents associated with heater elements can result in PCB failure.
- Motor start / run capacitor failure.

[32] White goods and Fire Risks; Domestic Refrigeration, IFIC Forensics. https://www.cila.co.uk/cila/download-link/sig-downloads/property/333-ific-forensics-domestic-fridges-fire-risks-march-2018/file

3 Benefits of smart appliances

Smart appliances are key to enable domestic consumers to participate in, and to enjoy the benefits of, the emerging smart energy system. As connected devices, they can respond to signals (such as price) and modulate their energy consumption accordingly, and so are key to demand side response (DSR) at the domestic level. This will help consumers to save money, as well as improve the efficiency of the system.

The section shows how different stakeholders might gain a range of specific benefits from the connecting of domestic appliances to the internet.

3.1 Consumer benefits

Internet connectivity offers the user a wide variety of new features. This section summarises the most common features that are or might soon be available in domestic appliances.

3.1.1 Monitoring and control via smartphone or similar interface

The ability to monitor and operate appliances remotely via a computer, smart-phone or tablet enables the user to:

- Schedule an appliance to come on when electricity costs drop below a pre-specified threshold.
- Receive alerts on a smartphone when problems are detected (for example, the refrigerator door is open, oven left on / over-heating, dishwasher leaking, or the freezer not cold enough).
- Turn on the oven to cook a dish while travelling home from work.
- Minimise the risk to small children by locking front panel controls.
- Personalise control settings to suit individual requirements.

Monitoring and operating remotely also has the potential to assist those with limited mobility and aid those who care for vulnerable consumers.

3.1.2 Minimising downtime through proactive maintenance

Smart appliances can improve appliance reliability by offering:

- Remote diagnostics to detect problems as soon as the first symptoms appear. In some cases, this can enable the fault to be fixed proactively before the appliance breaks down.
- Alerts when maintenance is required (filter needs changing, rinse agent needs topping-up etc).
- Immediate technical support from the manufacturer’s online support centre via the mobile application.

- Automatic software updates to fix errors or improve product reliability.

3.1.3 Saving time

The user can save time by allowing their appliances to:

- Automatically re-order laundry powder or dishwasher tablets when stocks are running low.
- Schedule tasks to be performed by connected appliances.
- Programme the microwave by scanning the barcode on a packet of food.
- Respond to voice commands detected by a digital assistant (e.g. “preheat the oven”).[33]

3.1.4 Reducing energy costs

Careful selection of when appliances operate can help to reduce energy costs by:

- Shifting operation of high-energy-using appliances to times of day when energy tariffs are lower, or when rooftop solar panels are likely to be generating electricity.
- Enabling participation in DSR programmes.
- Altering room temperatures depending upon who is at home.
- Monitoring and controlling the usage of individual appliances via smartphone.

3.1.5 Improving safety

Monitoring of the home environment can provide an additional level of safety:

- Turning off the hob and alerting the user if a pan is boiling over.
- Warning the user via their smartphone if smoke is detected in the kitchen, and possibly calling the fire brigade.
- Remote monitoring of appliances used by old or vulnerable people to detect signs of abnormal behaviour. For example, detecting that the kettle has not been used in the morning.
- Informing the user directly of a product recall, or even the remote disabling of particularly dangerous appliances.
- Newly developed appliances on the market such as smart appliances will comply with the latest technical standards, as such they may be safer than their non-connected equivalents.

[33] Allowing domestic appliances to be controlled by a digital assistant (e.g. Alexa, Siri or Google Assistant) using voice commands opens up new security risks (https://www.techrepublic.com/article/smart-office-secrets-alexa-siri-and-google-assistant-could-hear-commands-the-human-ear-cant/), but they are beyond the scope of this study. Similarly, allowing domestic appliances to place orders online creates fraud risks, but they are also beyond the scope of this study.

3.2 Manufacturer benefits

Internet connectivity will enable manufacturers to enhance their products and create new, value-added services. The following sections describe some possible opportunities.

3.2.1 Product differentiation

Adding an internet connection enables an appliance manufacturer to differentiate their products by increasing the perceived value at relatively low cost. However, as noted in Section 2.1, this functionality could migrate into cheaper appliances as the costs of providing internet connectivity decline and smart features become more common.

3.2.2 Collecting consumer data

Collecting data on how a product is used, problems that arise, service needs etc, will enable domestic appliance manufacturers to improve product design and help with marketing strategy. Such activity does raise data security issues that could fall within the scope of the General Data Protection Regulation. It should be noted that one of the key principles underpinning the Government's proposed smart appliances regulation, and the related development of technical standards, is data privacy.

3.2.3 New product features

Smart appliances will enable manufacturers to provide new product features/enhancements which could be downloaded automatically or by the consumer. A similar approach is used in the smartphone market to ensure that apps are updated regularly.

3.2.4 Value-added services

A smart appliance can recognise different user preferences. Many domestic appliances already have a bewildering range of programmes and options that a user can select, so it is reasonable to assume that smart appliances would remember each user's preferred settings that were selected during device installation. Adding a network connection would be relatively inexpensive, but could then create a multitude of possibilities for value-added services.[34]

3.2.5 Proactive maintenance services

The cost and performance of sensors and condition monitoring equipment for monitoring critical parameters such as current, noise, temperature and vibration means that they are being used in an increasing variety of applications. If this technology was fitted to domestic appliances, then the manufacturer could use Artificial Intelligence (AI) to predict certain appliance failures such as a worn bearing or damaged drive belt. A proactive maintenance service could then be offered in which problems are fixed before the product becomes unusable. Such proactive call-outs are not emergencies and so can be scheduled more efficiently.

[34] The register (2015) The Internet of things is great until it blows up your house. https://www.theregister.co.uk/2015/04/17/the_internet_of_things_is_great_until_it_blows_up_your_house/

3.3 Retailer Benefits

The benefits of smart appliances for the retailer may not be quite as strong as for consumers and manufacturers, but they are still significant.

3.3.1 New product features

For most users, appliances are not particularly exciting, with many offering very similar functionality and performance. However, if the benefits of network connectivity are sufficiently compelling, then retailers might be able to encourage customers to invest in more expensive models. Internet connectivity currently attracts a significant price premium, but this is likely to fall as it becomes more common.

3.3.2 Installation services for smart appliances

The importance of clear guidance on device installation and maintenance is set out in the DCMS Code of Practice[35]. However, the process for setting-up the network connection on a smart appliance might be beyond the capability of some consumers. This means that the setting-up and maintenance of the network connection could be undertaken by retailers. As security standards for smart appliances are improved, the need for such support is likely to increase.

3.3.3 Proactive maintenance services

As noted in Section 3.2.5, retailers could undertake proactive maintenance services to reduce the frequency or severity of appliance breakdowns.

3.3.4 Multi-vendor appliance networking

In the short term, it seems likely that each appliance manufacturer will promote their own proprietary networking solution. However, not many customers buy all their appliances from a single manufacturer, and some of their appliances are likely to be older than others. To network the appliances in a heterogeneous environment of this type, common networking standards will be needed. As in other areas of networking, it is possible that appliance networking will only really take off when a viable vendor-independent standard has evolved and been adopted by the industry. At this point, it may be possible for powerful players in the retail sector to establish their own networks and offer some or all of the services listed in Section 3.3.

[35] DCMS (2018) Secure by Design Code of Practice for Consumer IoT Security https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security

4 Risks associated with smart appliances

As outlined above, smart appliances have an important role in helping support the transition towards a smarter, more flexible and more affordable energy system. Yet as with all electrical appliances, there are associated risks to be considered around product safety. This section outlines these potential risks, with later sections detailing relevant mitigation options which should be taken forward.

4.1 Categories of failure mechanism

This report distinguishes between three different categories of failure mechanism:

- **Inherent design vulnerability.** A problem that can arise at the level of an individual component or a larger sub-system, irrespective of whether it is connected to the internet.
- **Non-malicious remote action.** An action, such as a software download, that accidentally introduces a software error.
- **Malicious remote action.** An action intended to harm the appliance, such as the deliberate downloading of malicious software.

As appliances become smarter, it will potentially become more common for them to operate at times when the householder is not present. Therefore, the consequences of a failure could become more significant, if no mitigation action is taken. This issue is considered in Section 4.5.

4.2 Inherent design vulnerabilities

Any domestic appliance could contain inherent design vulnerabilities that may or may not be known to the manufacturer. These vulnerabilities are not caused by an internet connection, but the presence of an internet connection could enable attackers to exploit them for malicious purposes.

The additional complexity that is inherent in smart appliances, and the novelty of some of their features, could make it more likely that they will contain design vulnerabilities, if mitigating actions are not taken. It is possible to put cyber-security measures in place to protect connected devices in the home, however these will not completely remove the risk of a vulnerability being exploited and a household network could still be compromised by another device with less robust protection. It should be noted that one of the key principles underpinning the Government's proposed smart appliances regulation, and the related development of technical standards, relates to cyber security.

These risks must be mitigated to an acceptable level. Section 7 describes how an internet connection might assist with the management of any design vulnerabilities that do emerge in smart appliances.

4.3 Issues that arise due to non-malicious remote action

Problems in this category are typically created as a result of a defective software download that could inadvertently introduce new security weaknesses or safety problems. Although software updates do pose challenges, they are the most important way of minimising software issues, by closing cybersecurity vulnerabilities, fixing bugs, increasing stability and more.[36] Cybersecurity attacks rarely work against systems that have the most recent software updates installed.[37]

4.4 Issues that arise due to malicious remote action

Malicious remote action could be as simple as sending a stream of commands to an appliance to exploit a known vulnerability in the design. For example, constantly switching an appliance on and off might eventually cause a component to fail. Threats could also come from malicious software being installed on the appliance.

Smart appliances are typically linked back to a server[38] that is controlled by the manufacturer or a cloud service provider. Since this server will be connected to a large number of separate appliances, and will typically be used for the distribution of software updates to those appliances, it represents a very attractive target for hackers. If the server can be compromised, then it could be used to launch an attack on a large number of appliances simultaneously.

The risks associated with an attack on an individual appliance are considered in Section 6.1, while attacks on groups of appliances connected to a server are considered in Section 6.2. Section 7 lists some ways in which these risks can be mitigated, and as mentioned above, work is already underway in Government to help mitigate these risks.

4.5 Issues made worse if appliance is operating while unattended

For many years, it has been possible to operate appliances at times when the occupants are either asleep or not at home. This will usually have been done using a time switch or a radio signal from the utility provider.

However, if an appliance develops a fault while it is operating unattended, then the consequences are likely to be more severe than if people are nearby and can take mitigating action. In particular, appliance fires that occur while householders are asleep could develop into life-threatening situations before anyone becomes aware of the problem. London Fire Brigade statistics show that while more than 38% of domestic fires originate at the cooker, the cooker is only responsible for 2% of fire-related fatalities.

[36] NCSC (2019) The problems with patching. https://www.ncsc.gov.uk/blog-post/the-problems-with-patching
[37] NCSC (2017) Time to KRACK the security patches out again. https://www.ncsc.gov.uk/blog-post/time-krack-security-patches-out-again
[38] For the context of this report, the term Server refers to the IT infrastructure and includes cloud-based models.

Conversely, other Large Domestic Appliances (including fridge/freezers) are responsible for less than 5% of domestic fires but cause nearly 33% of fire-related fatalities.[39]

Figure 1 displays the grid power demand curve, showing that most domestic fires occur at peak times of electricity use when householders are likely to be using their electrical appliances. This suggests that most fires are initiated by human activity which could include misuse of the appliance, or a faulty appliance causing a fire soon after it is switched on.

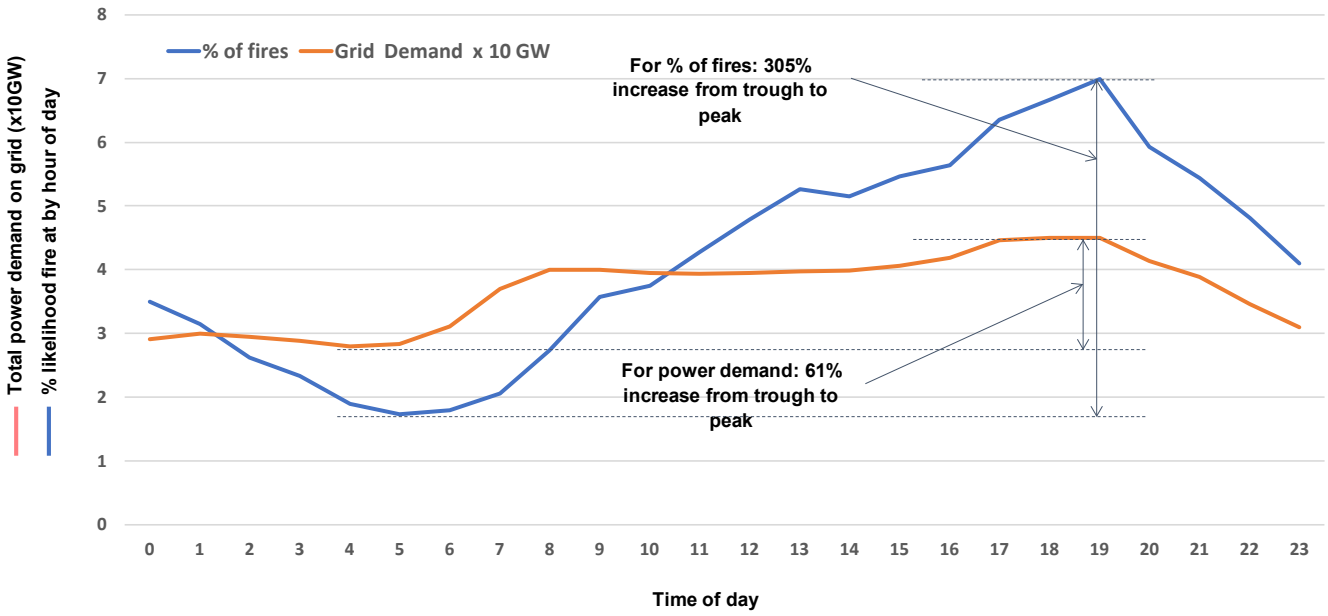


Figure 1: Grid Power demand vs % risk of domestic fires

Sources: Grid power demand from Gridwatch web site for Wednesday 31st October 2018. Fire data is from LFB - % of all primary fires by hour of day (totals to 100%).

Section 2.1 explains why washing machines, tumble dryers, washer dryer combinations and dishwashers are all likely to be suitable for time-shifting as part of a DSR scheme. Table 2 shows that these appliances are responsible for roughly half of all the domestic fires caused by appliance faults, and so the distribution of fires over a 24-hour period is also likely to be time-shifted.

Table 2: Appliance fires caused by technical faults

Appliance	% of fault-related appliance fires
Washing Machines	19%
Tumble Dryers	18%
Combination Washer Dryers	3%

[39] Source: Fire Facts, London Fire Brigade. https://data.london.gov.uk/dataset/fire-facts--fire-deaths-in-greater-london

Dishwashers	9%
Total	**49%**

Source: Electrical Safety First (ESF). Based on a total of 2,562 domestic appliance fires in 2015/16. https://www.electricalsafetyfirst.org.uk/media-centre/press-releases/2017/07/five-fires-per-day-caused-by-white-goods-in-england/

The occupier is typically incentivised to use time-shifting by offering them savings on their electricity bill. However, the simple concept of offering a cheaper electricity tariff at night and a more expensive tariff during the day is likely to become less applicable in future because:

- The power generated by non-dispatchable renewable energy sources can lead to variations in power availability, and hence price, at any time of day.
- Heat pumps are an increasingly important component of electricity demand as they replace heating based on fossil fuels.
- Charging of Electric Vehicles (EVs) at home will increase night time electricity use.
- The roll-out of smart meters will enable much more granular electricity tariffs (e.g. a different price every half hour).
- Some devices may be used to provide fast-acting response (within one second) for services to National Grid, Distribution System Operators or Aggregators. This would provide revenue for the home to offset electricity costs, but would probably only be applicable for space / water heating and air conditioning.

Figure 2 illustrates how smart appliances will be able to react to lower spot pricing for electricity as new forms of supply and demand change the grid demand curve. However, it should be noted that this has not been considered in the modelling section of this report.

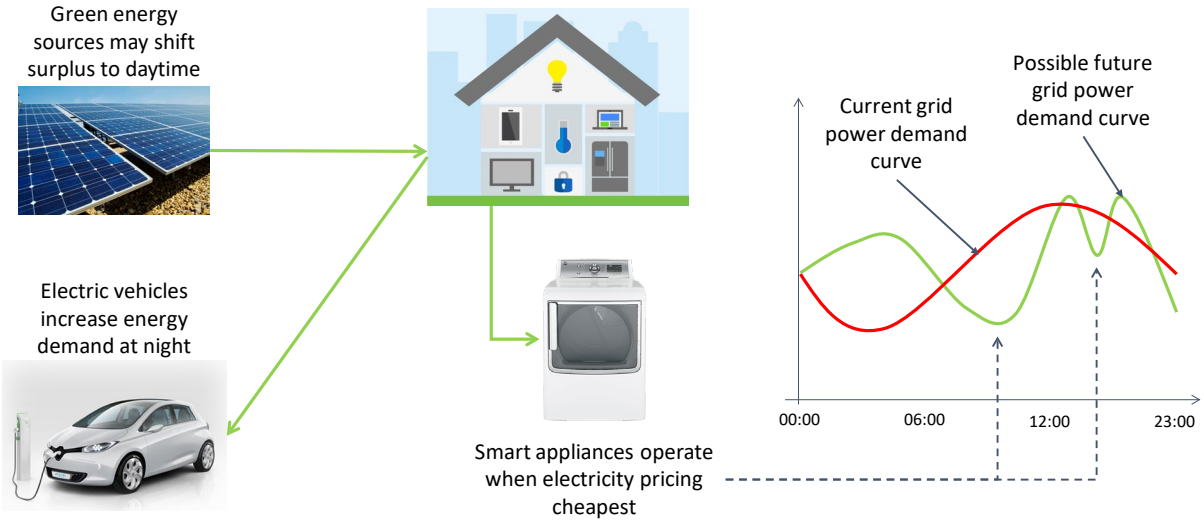


Figure 2: How new patterns of domestic energy generation could alter energy prices over the day

Source: Mott MacDonald

The purpose of this diagram is not to predict what the grid demand curve might look like in the future, but to illustrate that the operation of smart appliances may not necessarily be time-shifted to the middle of the night. Any change in the pattern of appliance use will re-distribute the incidence of appliance fires. Since time-shifted fires are more likely to occur when people are not around to deal with them, the consequences of these fires could be more serious.

5 Modelling the impact of time-shifting on appliance fires

5.1 Purpose and design of the model

In order to gain a quantitative understanding of the safety implications of time-shifting the operation of domestic appliances, a model was created to calculate how many more injuries or fatalities might result due to time-shifted, and hence unattended, fires. It should be noted that the model does NOT consider additional fires caused deliberately by internet-based attacks, or accidentally by downloading faulty software.

The design of the model is described in Appendix 1.

5.2 Modelling assumptions

Table 3 explains the assumptions used in the model:

Table 3: Modelling assumptions

	Assumption	Commentary
1	**The distribution of domestic appliance fires over a 24-hour cycle is roughly the same as the distribution of ALL Primary Fires over the same period.**	The only data identified that shows the distribution of fires over a 24-hour cycle is published by the London Fire Brigade and shows the distribution of ALL Primary Fires in London. Primary fires include the following categories: Dwelling, Other Residential, Non-Residential, Transport and Outdoor. Primary fires do NOT include: Rubbish, Open Land, Other Outdoor Structure, Derelict Building or Derelict Vehicle fires. For the period between 2010 and 2017, residential fires represented 57% of Primary Fires in London.
2	**Only washing machines, tumble dryers (including washer-dryers) and dishwashers need to be considered for time-shifting.**	Other types of domestic appliance will not be time shifted because: It is not safe (e.g. cooking hobs). The appliance does not consume enough electricity to be worth time-shifting (e.g. small appliances).

		It is very inconvenient for the user (e.g. microwave cookers). The appliance operates continuously (e.g. fridge/freezers).
3	**The current distribution of fires for washing machines, tumble dryers and dishwashers over a 24-hour cycle is roughly the same as for domestic appliances as a whole.**	The data showing the distribution of fires over a 24-hour cycle is very limited (see Assumption 1). Although the rate at which fires occur will be different for different appliances, it seems reasonable to assume that the distribution of those fires over a 24-hour cycle will be similar for most appliances other than cookers.
4	**Washing machines, tumble dryers and dishwashers will be time shifted from 4-9pm to 0-5am by DSR or some other means.**	The period 4-9pm was chosen to cover the evening peak on the electricity grid. Similarly, the period 0-5am was chosen to align with the period of lowest energy demand. This may change in the future, as discussed in Section 4.5. Hence, this assumption reflects a 'highest risk scenario', also ignoring that some consumers might not want to shift the appliance activity to night-time, e.g. due to noise disturbances or similar.
5	**20% of households will sign-up for time-shifting and use the time-shifting feature in 80% of times.**	As explained in Section 4.5, the consequences of time-shifting domestic appliances are currently very hard to predict on a year-by-year basis because there are too many variables that are poorly understood. Ultimately, the proportion of homes that will sign-up for time shifting of their dishwashers, washing machines and tumble dryers will depend on the size of the financial incentives that are offered. Although extensive modelling has been carried out on DSR, it appears that it has mostly been confined to time-shifting of domestic heating and electric vehicles rather than appliances. For these reasons, the model includes a sensitivity analysis to examine the effect of changing the proportion of homes that time-shift their appliances to 10% or

		30%.(source 2012 BEIS commissioned research: Baringa/Element Energy: Electricity System Analysis – future system benefits from selected DSR scenarios.) Consumers are unlikely to use their appliances in smart mode all the time. Instead, we have assumed that they use the time-shifting functionality 80% of the time. All these assumptions relate to the year 2030.
6	**Time-shifted washing machines, tumble dryers and dishwashers operating during the night have the same rate of Casualties / 1,000 fires as fridge/freezers.**	Assumption 6 has been used to calculate the number of additional fires with casualties that might occur as a result of time-shifting fires from times when appliances are likely to be attended to times when they are likely to be unattended. This assumption could be challenged by arguing that some fridge/freezer fires are made worse by dangers that are specific to these types of appliances, rather than because these appliances are operating while unattended. Against this, it can be pointed out that fridge/freezer fires are likely to be reasonably evenly distributed over a 24-hour cycle, and residents are only likely to be asleep for about one third of this time; in contrast, almost all time-shifted fires will occur while residents are asleep. Again, this assumption is a 'high risk assumption' and in reality, consumers are likely to shift partly to other times of the day (see assumption 4)
7	**The ratio of fatalities to injuries for appliance-related fires is roughly the same as for all fires.**	The calculation of the number of additional fatalities per year that might occur as a result of time-shifting assumes that fatalities represent a relatively constant proportion of fire casualties, and that the proportion is roughly the same for appliance-related fires as for all fires. 2017 was omitted from this calculation because it was felt

		that the ratio was unreasonably distorted by the Grenfell Tower fire.
8	**ALL fires associated with washing machines, tumble dryers and dishwashers will be time-shifted in homes that have signed-up for time-shifting.**	Data provided by the London Fire Brigade suggests that approximately 85% of fires in washing machines, tumble dryers, dishwashers and fridge/freezers are caused by technical faults, while about 15% are caused by incorrect installation or operation. However, we understand that the fire service tends to attribute fires to misuse rather than a design fault if no fatality has occurred, so the proportion of fires caused by design faults is likely to be higher than 85%. Furthermore, many of the fires caused by incorrect installation or operation (e.g. appliance too full or unsafe DIY repair) will only occur once the appliance starts operating, so would also be time-shifted.
9	**Households do not currently time-shift appliances to the night.**	Data suggests there is very limited use of washing machines, tumble dryers and washer-dryers during the night. This is not the case with dishwashers which are used a moderate amount during this period[40]. However, due to challenges with calculating the proportion of appliances that currently time-shift to the night, including variance between appliances, it is assumed that no time-shifting currently occurs. Hence, this assumption reflects a 'highest risk scenario' in terms of the percentage increase of households time-shifting appliances, as in reality a small proportion of householders will already be doing this.

[40] BEIS (2013) Household Electricity Survey: A study of domestic electrical product usage. https://www.gov.uk/government/publications/household-electricity-survey--2

5.3 Conclusions from modelling

Based on the assumptions set out above, Figure 3 shows the effect of time-shifting on the distribution of appliance fires. The solid blue line represents the current distribution of appliance fires,[41] while the dotted red line shows the distribution of appliance fires after the fires attributable to washing machines, tumble dryers, combination washer dryers and dishwashers have been time-shifted.[42]

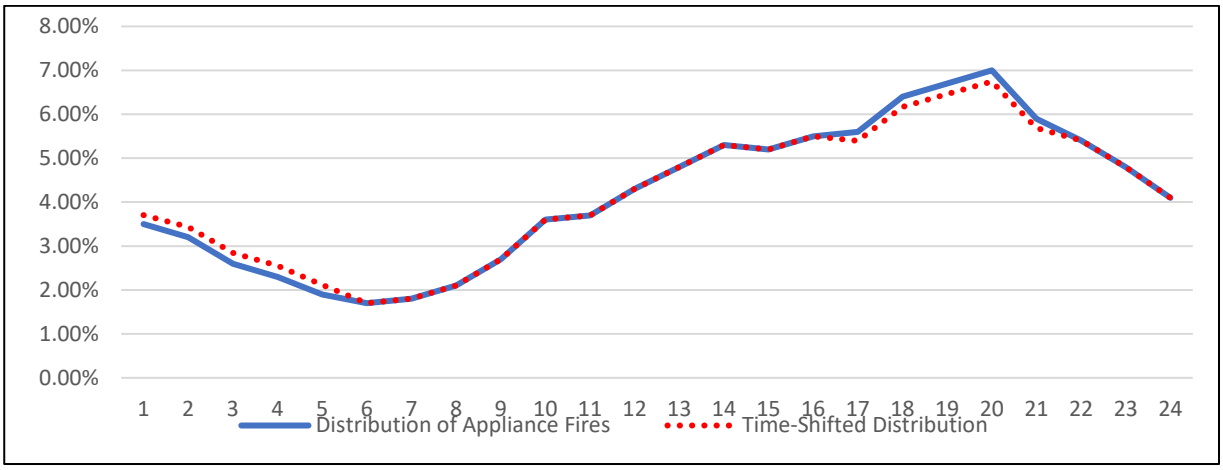


Figure 3: Probability of appliance fires by time of day. Source: Mott MacDonald

The model has produced the following estimates of the impact of time-shifting on appliance fires:

- In 2030, the model expects fires at night to increase by 6% (87 / year), caused by UK appliances time-shifting from the evening peak to the middle of the night.
- Of these time-shifted fires, an additional 1.3% fires (12 / year) are expected to result in casualties.
- This equates to an increase in fatalities of 1.3% (1.1 / year).

Assumption 5 in Table 3 above states that "20% of households will sign-up for time-shifting". Since a lot of uncertainty exists around that assumption, a sensitivity analysis was carried out to investigate the impact of changing the assumption to 30% or 10%.

Table 4: Sensitivity analysis on % of homes that time-shift appliances

% of homes that time-shift appliances	10%	20%	30%
Increase of fires at night / year (due to time-shifting)	3% (43)	6% (87)	9% (130)

[41] See Appendix 1, Table 1, Column 2
[42] See Appendix 1, Table 1, Column 6

Increase in fires with casualties / year that result from time-shifting	0.6% (6)	1.3% (12)	1.9% (17)
Increase in fatalities / year that result from time-shifting	0.6% (0.5)	1.3% (1.1)	1.9% (1.6)

Source: Mott MacDonald

As explained in Section 4.5, the number of appliances that are likely to be time-shifted by DSR or other mechanisms is currently subject to uncertainty. However, these results may provide a reasonable indication of the possible impact of time-shifting on appliance safety, if no mitigating actions are taken by the Government and industry.

6 How could an internet connection be used to attack a domestic appliance?

6.1 Attacks on individual domestic appliances

Possible mechanisms for carrying out an attack on an individual appliance include:

- Attacking an insecure home network.
- Attacking the app on a smartphone or similar device.
- Attacking the server.

A cyber-attack on an individual appliance could have obvious safety implications.[43] It could also enable the appliance to be used for cybercrime (e.g. to launch Distributed Denial of Service (DDoS) attacks or mine crypto currencies), but cybercrime implications fall outside the scope of this report.

Domestic appliances are often designed using a controller chip that has direct control over all the heaters, valves, sensors, displays etc used by the appliance. If the machine has a vulnerability, then the control of these components could be compromised[44] and used maliciously to potentially cause hazards such as overheating, flooding or the immobilisation of safety features designed to protect against fire. There is no evidence that any of these attacks have been seriously attempted to date, however, these are examples of the risk's manufacturers need to guard against.

6.2 Attacks on the servers used to monitor domestic appliances

If an appliance manufacturer or a DSR aggregator[45] is using a server to control domestic appliances in customers' homes, then it might be possible to use that server to launch an attack on a large number of appliances simultaneously.

Once an attacker has gained control of the server, then it should be possible to install malware on the smart appliances via a normal software download. As in the case of a DoS[46] botnet,[47] the appliances would continue to work normally until the malware is activated by a central command.

---

[43] The register (2017) Half-baked security: Hackers can hijack your smart Aga oven 'with a text message'. https://www.theregister.co.uk/2017/04/13/aga_oven_iot_insecurity/

[44] The register (2017) Dishwasher has directory traversal bug. https://www.theregister.com/2017/03/26/miele_joins_internetofst_hall_of_shame/

[45] An aggregator is a new type of energy service provider that controls the electricity use of a group of consumers according to signals from the grid.

[46] Distributed Denial of Service (DDoS) – where multiple devices on the Internet flood the targeted server with requests, thereby overwhelming the server's ability to respond. This tends to lead to the server 'crashing'.

[47] The online definition of Botnet is: 'a number of Internet-connected devices, each of which is running one or more bots. Botnets can be used to perform distributed denial-of-service attack, steal data, send spam, and allows the attacker to access the device and its connection." The owner can control the botnet using

The methods of attack would be similar to those described in Section 6.1. However, if the number of appliances is sufficiently large or they are concentrated in a small enough area, then it might be possible to disable or damage a number of appliances simultaneously, which may create problems for local services (e.g. maintenance and fire brigades) and the local electricity system, if mitigation action is not taken ahead of time.

As outlined in the joint Government and Ofgem Smart Systems and Flexibility Plan, work is currently underway to ensure cyber security risks similar to those summarised above are effectively identified and addressed.

6.3 Ways for users of smart appliances to protect themselves

To minimise the risk of buying products with security weaknesses, consumers should select appliances from reputable manufacturers and buy them from reputable dealers. DCMS and the National Cyber Security Centre have published guidance for consumers on the safeguarding actions that they can take.[48] These include:

- Referring to the manufacturer's documentation when setting up the device.
- Checking the default settings, for example by changing the default password if it is easily guessable.
- Managing online accounts to make them more secure, for example by turning on two-factor authentication.
- Ensuring software updates are installed promptly.
- Performing a factory reset if the device is sold or given to someone else.

Guidance is also given if the consumer suspects or becomes aware of an incident.

6.4 Ways for appliance manufacturers to protect their customers

Smart home appliances add a new dimension to the cyber risks of home networking. This is because smart appliances can be installed and operated by users with no knowledge of cyber security issues, and also because the very wide range of hardware and software found in home networks can create unforeseen cyber risks.

Cyber security for smart appliances should be based on established best practice as set out in the DCMS Secure by Design Code of Practice for Consumer IoT Security.[49] Important recommendations from this document include:

- **Easy to use.** The user should not be expected to be proficient in cyber security to operate the device.

command and control software. The word "botnet" is a combination of the words "robot" and "network". The term is usually used with a negative or malicious connotation.' The Mirai botnet was found in August 2016 and has been used in a number of high-profile Internet attacks.

[48] NCSC (2019) Smart devices: using them safely in your home. https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home

[49] DCMS (2018) Secure by design Code of Practice for Consumer IoT Security. https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

- **Clear instructions.** The instructions should be simple to understand and should recognise any differences between hardware variants or software revisions.
- **Easy to update.** Any product changes to remove vulnerabilities should be done in a secure manner.
- **Easy disposal.** Appliances should be configured such that any personal data can easily be removed from them when there is a transfer of ownership, when the consumer wishes to delete it, or when the consumer wishes to dispose of the device.

The assumption in this section is that hackers are able to exploit a security weakness or some other form of vulnerability to take control of individual appliances and/or the servers to which they are connected.

A standard for cybersecurity in the IoT has also been developed, the ETSI Technical Specification 303 645 which is discussed further in section 7. This can be used by manufacturers and other companies to test their products against to ensure they meet best practice for cybersecurity.[50]

6.4.1 Hardware-based protection

Where software is being used to control a potentially dangerous device, such as a heater or an electric motor, then the back-up (as required by IEC 60730 for Class B systems) should be implemented in hardware rather than software. For example, the heater in a washing machine could be under software control to reduce cost, but a hardware thermal cut-out would prevent malware from using the heater to start a fire. A similar approach could be used to detect and prevent other dangerous situations where the software has failed to intervene.

6.4.2 Data Security

As explained in Section 3.2.2, a smart appliance will generate large amounts of information (how the appliance is used, problems that arise, service needs etc). This may be stored alongside personal information such as name, address, telephone number and email address. It is likely that this information will eventually be used for marketing purposes, though consent is required to process personal data.

Appliance manufacturers will have to store this data securely and comply with the provisions of the General Data Protection Regulation (GDPR). Since appliances are often sold on the second-hand market, it is essential that no personal data is stored on the appliance. Furthermore, the appliance should allow the user to initiate a factory reset when disposing of the appliance.

As outlined in section 7, one of the key principles underpinning the Government's proposed smart appliance regulatory plans, and the related development of technical standards, is data privacy.

[50] ETSI Consumer IoT security. https://www.etsi.org/technologies/consumer-iot-security

6.4.3 BS EN 60335 requirements

BS EN 60335 includes several requirements that would reduce the impact of internet threats:

Table 5: BS EN 60335 requirements for remote operation of appliances

BS EN 60335 requirements	Commentary
22.40 Unless the appliance can operate continuously, automatically or remotely without giving rise to a hazard (e.g. refrigerators), appliances for remote operation shall be fitted with a switch for stopping the operation of the appliance. The actuating member of this switch shall be easily visible and accessible.	For built-in appliances, it may be difficult to disconnect the power to the appliance if it is behaving in a dangerous manner. A front panel switch could overcome this problem.
22.49 For remote operation, the duration of operation shall be set before the appliance can be started unless the appliance switches off automatically at the end of a cycle (e.g. washing machine, dishwasher) or it can operate continuously without giving rise to a hazard (e.g. refrigerator).	This means, for example, that an oven cannot be switched on remotely without first specifying how long it should be on for.
22.50 Controls incorporated in the appliance, if any, shall take priority over controls actuated by remote operation.	It might be possible for malware to disable the front panel controls.
22.51 A control on the appliance shall be manually adjusted to the setting for remote operation before the appliance can be operated in this mode. There shall be a visual indication on the appliance showing that the appliance is adjusted for remote operation.	This control prevents appliances such as washing machines from being switched-on by remote command unless the user has confirmed that it is safe to do so. However, it might be possible for malware to disable this control. There are exceptions to this requirement: “The manual setting and the visual indication of the remote mode are not necessary on appliances that can • operate continuously, or • operate automatically, or • be remotely operated

	without giving rise to a hazard". The only domestic appliance listed as an exception is a refrigerator.

Source: BS EN 60335 / Mott MacDonald

6.4.4 IT skills

Some of the IT skills likely to be required for developing smart appliances, such as software design for cyber security and the protection of personal data, require appliance manufacturers to expand their technical capability and organisational awareness. But those that still rely on externally sourced hardware and software may not have a full understanding of the level of security provided by these components. Therefore, it is important that manufacturers consider the skillset required for developing secure smart appliances.

6.5 Ways to minimise software issues occurring accidentally

The ability to download new software into an installed appliance provides a useful way for the manufacturer to introduce new features or remedy software defects. Thorough testing of software upgrades being released should detect and attempt to rectify all problems before the software is released, but this can be difficult to achieve in practice. For example:

- It is likely that microcontrollers and other devices will continue to evolve over the life of an appliance, and this may require other hardware design changes. The downloaded software must be able to determine the exact hardware configuration of each appliance, and may have to configure itself differently for different hardware revisions.
- It is likely that 3rd party software such as operating systems, device drivers and library routines will continue to evolve during the lifetime of the appliance. This can sometimes create unexpected compatibility issues.
- It may become necessary to maintain multiple variants of the software to meet the requirements of different countries or markets. A defect that appears in one software variant may or may not occur in other variants.

In practice, proving that software is error-free is notoriously difficult,[51] and bugs will still exist.

For smart devices with a significant amount of internal storage, it is possible to store two successive software downloads at the same time. This makes it relatively simple to drop back to the previous software version if the latest download proves to be faulty. However, the microcontrollers used in domestic appliances may not have enough storage to do this. It should therefore be possible for a previous software version to be downloaded if the new version proves to be faulty.

[51] Schneier (2009) Proving a Computer Program's Correctness. https://www.schneier.com/blog/archives/2009/10/proving_a_compu.html

6.6 Opportunities to improve safety

Smart appliances have several potential safety benefits:

- Enabling the delivery of proactive maintenance services, as described in sections 3.1.2 and 3.2.5.
- Advise the appliance owner that it is subject to a recall, which would help to boost the sometimes-low levels of response to recall campaigns.[52] In some circumstances it could monitor the appliance condition to enable operation until it becomes dangerous.
- Disabling of an appliance with a serious fault that is the subject of an urgent recall.

[52] Electrical Safety First (2014) Consumer Voices on Product Recall. https://www.electricalsafetyfirst.org.uk/mediafile/100205681/Product-Recall-Report-2014.pdf

7 Regulations and standards for domestic appliances

Standards, regulations and directives have a key role to play in improving product safety. Not only can they help to improve product design and construction, but they can also be relevant for product installation and operation. This section discusses some British and European standards and regulations that are directly relevant to smart appliances.

7.1 BS EN 60335: Household and similar electrical appliances – Safety

The principal objective of this standard is summarised in Part 1[53] as follows:

> *"Appliances shall be constructed so that in normal use they function safely so as to cause no danger to persons or surroundings, even in the event of carelessness that may occur in normal use."*

The standard includes a number of requirements for Remote Operation, which is defined as

> *"control of an appliance by a command that can be initiated out of sight of the appliance using means such as telecommunications, sound controls or bus systems".*

These requirements are discussed in Section 7.2 of this document.

The BS EN 60335 standard includes an Annex on Software Evaluation that describes how appliance software can be checked for compliance with the standard. The Annex requires that

> *"programmable electronic circuits requiring software" ... "shall use measures to control and avoid software-related faults in safety-related data and safety-related segments of the software".*

There are extensive requirements to detect hardware problems in the microcontroller, such as:

- Stuck bits in registers, programme counter or memory.
- Interrupts not occurring or occurring too frequently.
- Clocking problems.
- Data errors on external communication.

These requirements are derived from the IEC 60730-1 standard, which is discussed in the following section.

[53] BS EN 60335-1: 2012+A13:2017, Household and similar electrical appliances – Safety, British Standards Institution.

The Annex also includes short sections on software architecture, module design and coding, but these consist mainly of generic statements about good software design practices. For example:

- Document the software design properly.
- Break the software down into modules.
- Use structured programming techniques.
- Avoid GOTO statements in High-Level Language programs.

There is also a short section on software testing, which includes the requirement to report the tests used to validate compliance. If the software is modified in a way that might affect the operation of protective electronic circuits, then the tests must be repeated. There is no requirement for software verification by an independent tester.

Clause 24.1.7 states that

> *"If remote operation of the appliance is via a telecommunications network, the relevant standard for the telecommunications interface circuitry in the appliance is EN 41003".*

This standard has now been replaced by BS EN 62949:2017: "Particular safety requirements for equipment to be connected to information and communication technology networks". However, this standard relates to fixed telecoms network connections. Appliances are normally connected via WiFi, so the Radio Equipment Regulation is applicable. This is discussed in Section 7.4.

The comments above relate to BS EN 60335 Part 1. Part 2 of the standard includes requirements that apply to a specific type of appliance. The relevant sections are listed below:

Table 6: Relevant sections in BS EN 60335 Part 2

Appliance	Relevant Section
Dishwashers	BS EN 60335-2-5
Cookers	BS EN 60335-2-6
Washing Machines	BS EN 60335-2-7
Tumble Dryers	BS EN 60335-2-11
Refrigerators & Freezers	BS EN 60335-2-24

7.2 IEC 60730-1: Automatic electrical controls for household and similar use

The IEC 60730 safety standard defines the test and diagnostic methods that ensure the safe operation of embedded control hardware and software for household appliances. The standard divides applicable equipment into three categories:

- Class A: Equipment in this category is deemed to be safe if the software malfunctions.
- Class B: Equipment would probably be put in this category if a safety feature has been implemented in software and there is back-up protection in case the software fails.
- Class C: Equipment in this category typically presents special safety hazards (such as the potential to explode).

Home appliances such as washing machines, dishwashers, tumble dryers, refrigerators, freezers and cookers normally fall under the Class B classification. Some self-testing requirements for Class B equipment are listed in Table 7:

Table 7: Self-testing requirements for Class B systems

Microcontroller Component	Fault / Error
CPU Registers; CPU program counter	Stuck
Interrupt handling & execution	No interrupt or too-frequent interrupts
Clock	Failure or wrong frequency
Non-volatile memory (e.g. ROM)	All single-bit faults
Volatile memory (e.g. RAM)	DC fault
Internal data path	Stuck
External communications	Failure or errors
Input / Output peripheral	Failure or errors
Analogue interfaces	Failure or inaccurate

Source: IEC 60730-1, Table H.11.12.7

Manufacturers generally adhere to the designated standard IEC 60730-1 to demonstrate compliance with legislation. Microcontroller vendors have developed software libraries that have been independently certified to make it simpler for appliance manufacturers to achieve IEC 60730 compliance.

The technical tests defined in IEC 60730 are referenced extensively from BS EN 60335.

7.3 ETSI Technical Specification 303 645

ETSI EN 303 645 was published in 2020 and is designed to prevent large-scale, prevalent attacks against smart devices by establishing a security baseline for connected consumer products[54], including appliances. It sets out practical steps for IoT manufacturers and other industry stakeholders to improve the security of consumer IoT products and associated services. Implementing the standard should enable consumers to use their products securely while also protecting their privacy and safety. It will also mitigate against the threat of Distributed Denial of Service (DDoS) attacks as discussed in section 6.

There are 13 requirements in total which align with those in the DCMS Code of Practice for consumer IoT security[55]. The top three requirements are:

- No default passwords.
- Implement a vulnerability disclosure policy.
- Keep software updated.

7.4 The Radio Equipment Regulations

The Radio Equipment Regulations (RER), which implements Directive 2014/53/EU on Radio Equipment, cover any radio interfaces (including WiFi) that might be used in domestic appliances in the UK. The RER establishes a regulatory framework for radio equipment within the UK by setting essential requirements for health and safety, electromagnetic compatibility and the efficient use of the radio spectrum. It also provides the basis for future regulation in areas such as:

- Technical features to protect privacy and personal data.
- Technical features for fraud prevention,
- Interoperability.
- Access to emergency services.
- Compliance issues relating to the combination of radio equipment and software.

The RER is a ‘total safety directive’ which means that it covers all aspects of safety for the appliances in scope - not just their transmitting and receiving parts. What this means in

[54] ETSI Consumer IoT security. https://www.etsi.org/technologies/consumer-iot-security
[55] DCMS (2018) Secure by Design Code of Practice for Consumer IoT Security. https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

practice is that a washing machine without a network connection is covered by the Electrical Equipment Safety Regulations (EESR), but one with a network connection is covered by the RER. This does not really matter because the general safety requirements in RER reference those in the EESR.

The Radio Equipment Regulations do not currently require equipment manufacturers to provide information about software (including firmware) that is embedded in the equipment or used in conjunction with it, so long as the software cannot change the technical characteristics of the radio equipment (e.g. by moving it to a different frequency range or a higher output power).

7.5 Energy Smart Appliances - Publicly Available Specifications

The British Standards Institution (BSI) has implemented a standardisation programme to enable the secure placement on the market and accelerate the uptake of Energy Smart Appliances (ESA). The programme of work, sponsored by the Government, follows from the standards mapping research project carried out by BSI in 2018 at the request of the Government. BSI published a report on this work which identified key gaps in the standards landscape related to ESAs[56].

The programme published two Publicly Available Specifications (PAS 1878 and 1879) in 2021: one covering the framework for ESAs to operate in a DSR system, the other providing an ESA classification and requirements for smart functionality. The key principles underpinning this work are data privacy, cyber-security, grid-stability and interoperability[57]. Although specific requirements for safety are out of scope of this PAS, these four principles provide some related safety aspects for consumers and infrastructure.

In tandem with this work on technical standards, the Government has set out its intention to set regulatory requirements for certain smart appliances, based on the same principles listed above[58].

The Government has introduced primary legislation via the Energy Security Bill[59], which seeks enabling powers to introduce regulations for energy smart appliances (such as electric vehicle charge points and smart heat pumps) so that devices meet minimum technical requirements for cyber security, interoperability, data privacy and grid stability. These powers will also allow Government to mandate that electric heating appliances and EV chargepoints must have smart functionality, prohibiting the sale of non-smart devices in Great Britain.

[56] BSI Smart Appliances & EV Chargepoints Standards Landscape Mapping Review. https://www.bsigroup.com/en-GB/smart-appliances-flexible-energy/
[57] BSI ESA Programme Brochure. Available at: https://www.bsigroup.com/en-GB/smart-appliances-flexible-energy/
[58] BEIS (2018) Proposals regarding setting standards for smart appliances. https://www.gov.uk/government/consultations/proposals-regarding-setting-standards-for-smart-appliances
[59] BEIS (2022) Energy Security Bill. https://www.gov.uk/government/collections/energy-security-bill

The Government has also published a consultation[60] which focuses on how these primary powers would be implemented. The consultation sets out proposals to ensure consumers and electricity system are protected, and seeks views on ongoing work by government to establish system-level cyber security requirements for energy smart appliances, and develop a competitive market for energy smart appliances and DSR.

7.6 Commentary on standards and regulations

Standards are key to improving appliance safety, but it appears that technology developments in smart appliances are running well ahead of standardisation efforts. BS EN 60335 Clause 19.1 states that:

> *"Electronic circuits shall be designed and applied so that a fault condition will not render the appliance unsafe with regard to electric shock, fire hazard, mechanical hazard or dangerous malfunction."*

Whilst this is fine for simple appliances, it fails to recognise that changing the software in a smart appliance is changing the design. Consequently, a design that was once perfectly safe could be rendered unsafe by a malicious or poorly written software download.

The current draft of 60335[61] does not consider issues such as cyber-attacks or malicious software downloads, and there is no mention of personal data security issues. It is understood that a new draft of 60335 will address software and remote control issues in more detail.

To address the security issues with connected consumer products, including appliances, DCMS have recently introduced the Product Security and Telecommunications Infrastructure Bill (PSTI)[62]. This bill aims to protect consumer connectable devices from cyber-attacks. The security requirements, to be set out in regulations, are based on the top three requirements from the Code of Practice for consumer IoT security and the ETSI EN 303 645 standard. These are: ban default passwords, require products to have a vulnerability disclosure policy and require transparency about the length of time for which the product will receive important security updates.

Additionally, the Radio Equipment Directive, which will have a direct impact on appliances in Northern Ireland and likely influence the GB market to some extent, increased the scope of the RED to include more elements of cyber security in 2021[63]. However, the RED does not cover servers and the other IT infrastructure that is likely to be connected to a wireless

[60] BEIS (2022) Delivering a smart and secure electricity system: the interoperability and cyber security of energy smart appliances and remote load control. https://www.gov.uk/government/consultations/delivering-a-smart-and-secure-electricity-system-the-interoperability-and-cyber-security-of-energy-smart-appliances-and-remote-load-control

[61] BS EN 60335-1:2012 + A13:2017, incorporating corrigenda October 2013, January 2014 and October 2014.

[62] DCMS (2021) The Product Security and Telecommunications Infrastructure (PSTI) Bill – product security factsheet. https://www.gov.uk/guidance/the-product-security-and-telecommunications-infrastructure-psti-bill-product-security-factsheet

[63] European Commission (2021) Commission strengthens cybersecurity of wireless devices and products. https://ec.europa.eu/growth/news/commission-strengthens-cybersecurity-wireless-devices-and-products-2021-10-29_en

interface, so any security requirements in the RED would only be able to address part of the problem.

Indeed, it can be argued that a network interface specification is exactly the wrong place to put cyber security requirements. This is because the normal assumption within distributed IT systems is that the network is unreliable and insecure, so overall responsibility for maintaining security and data integrity lies with the applications that are transmitting data over the network rather than the network itself. Whilst the Radio Equipment Directive may seek to improve link-level security by adding (say) a layer of encryption, the ultimate responsibility for the integrity of the data used by the appliance in its operation should remain with the appliance manufacturers.

The development of a new standard can take over seven years from inception to implementation, and so it is assumed that standards will continue to develop well behind the technology. However, as outlined in the above section, two Publicly Available Specifications (PAS 1878 and 1879) related to Energy Smart Appliances and Demand Side Response were recently published in 2021.

To gain presumption of conformity with the Radio Equipment Regulations, manufacturers normally adhere to the designated standard IEC 60730-1. However, standards are generally voluntary; a manufacturer can use other routes to demonstrate compliance with legislation.

8 Conclusions

Although the attractions of internet connectivity might seem modest at present, a reduction in the price premium and the offering of new internet-enabled services could result in it becoming a standard feature on even the lowest cost models. The ability to have remote control of a device is perhaps the most obvious benefit, but internet connection would also enable proactive maintenance and simplify product recalls. More broadly, as this report has highlighted, smart appliances can help support the transition towards a smarter, more flexible, cleaner and more affordable energy system for consumers.

However, domestic appliances are a significant cause of house fires. The analysis in this report found that internet connectivity could potentially lead to a small increase in the number of fatal house fires due to time-shifting, if mitigating action is not taken.

Fires in time-shifted appliances are more likely to occur when users are not present to take mitigating action, and fires that occur while householders are asleep could develop into life-threatening incidents. Based on recent LFB statistics for fatal house fires caused by faulty appliances, and assuming that 20% of all UK households have taken up each of the smart appliances considered, and that they use them in smart mode (e.g. time shifting) 80% of the time, and assuming that load is always shifted to the night when consumers are asleep (the highest risk), modelling has shown that an additional 12 fires with casualties and 1.1 fatalities could occur each year (an increase of 1.3%). We estimate that this risk could be mitigated by additional safety standards, and other measures, that decrease the risks of fires resulting in casualties by at least 6.5%, in which case this projected increase in casualties and fatalities would not be expected to occur. Moreover, further mitigation measures would create a net benefit in terms of safety for consumers that use smart appliances. As noted above, the increased unmitigated risk of fatalities is not reached until 20% of all UK households are time shifting certain domestic smart appliances 80% of the time, which is unlikely to happen before 2030, and allows sufficient time to establish such mitigating measures, more so given that work on mitigation is already underway.

In addition, the traditional idea that appliance safety can be assured in the design phase fails to recognise that changing the software in a smart appliance after purchase is changing the design. Consequently, a design that was once very safe could be rendered unsafe by a malicious or poorly-written software download. Where software is being used to control a device that could fail in a way that might lead to fire, it is important that the back-up safety mechanism should be implemented in hardware rather than software.

To reduce the risk of appliance failure through a malicious or poorly-written software download, appliance manufacturers should ensure that they, and companies on their supply chain, adhere to consumer Internet of Things (IoT) security standards and best practice to ensure that their products are properly secured against current and evolving threats. Users of smart appliances can help to protect themselves by following advice given by DCMS and the National Cyber Security Centre.

The development of appropriate standards, and consideration of regulatory options, will also help ensure the safety risks raised in this report are properly mitigated. A watching

brief should be kept on BS EN 60335, PAS 1878/1879, EN 303 645 and The Product Security and Telecommunications Infrastructure (PSTI) Bill, which will influence software (including firmware) design for appliances.

Lastly, while the focus of this report is on the safety hazards due to the internet connection of smart appliances, it should be stressed that there have to date been no reported incidents of fires due to internet connection. In addition, the ability to offer proactive maintenance services and simplify product recall could help to reduce incidents. It is recommended that technical standards specify that smart appliances have specific safety features such as condition monitoring and proactive maintenance.

9 Appendices

9.1 Modelling the impact of time-shifting

9.1.1 Structure of model

Table 8 in the model uses Assumptions 1 – 5 (see Section 5.2) to calculate the time-shifted distribution of washing machine, tumble dryer, combination washer dryer and dishwasher fires.

Table 8: Model data

Hour of Day	Distribution of Appliance Fires	Distribution for WM, TD, DW	Time-Shifted Distribution for WM, TD, DW	Distribution of Appliance Fires excluding WM, TD, DW	Time-Shifted Distribution
0	3.5%	0.5%	**0.7%**	3.0%	3.7%
1	3.2%	0.5%	**0.7%**	2.7%	3.4%
2	2.6%	0.4%	**0.6%**	2.2%	2.8%
3	2.3%	0.3%	**0.6%**	2.0%	2.6%
4	1.9%	0.3%	**0.5%**	1.6%	2.1%
5	1.7%	0.3%	0.3%	1.4%	1.7%
6	1.8%	0.3%	0.3%	1.5%	1.8%
7	2.1%	0.3%	0.3%	1.8%	2.1%
8	2.7%	0.4%	0.4%	2.3%	2.7%
9	3.6%	0.5%	0.5%	3.1%	3.6%
10	3.7%	0.6%	0.6%	3.1%	3.7%
11	4.3%	0.7%	0.7%	3.6%	4.3%
12	4.8%	0.7%	0.7%	4.1%	4.8%
13	5.3%	0.8%	0.8%	4.5%	5.3%
14	5.2%	0.8%	0.8%	4.4%	5.2%
15	5.5%	0.8%	0.8%	4.7%	5.5%

16	5.6%	0.9%	**0.6%**	4.7%	5.4%
17	6.4%	1.0%	**0.7%**	5.4%	6.2%
18	6.7%	1.0%	**0.8%**	5.7%	6.5%
19	7.0%	1.1%	**0.8%**	5.9%	6.7%
20	5.9%	0.9%	**0.7%**	5.0%	5.7%
21	5.4%	0.8%	0.8%	4.6%	5.4%
22	4.8%	0.7%	0.7%	4.1%	4.8%
23	4.1%	0.6%	0.6%	3.5%	4.1%
Checks	100.1%	15.2%	15.2%	84.9%	100.1%

Source: Fire Facts London 1, Worksheet 2.9

Column 1 shows the hour of the day at which fires occurred.

Column 2 shows the proportion of Primary Fires that occur during each hour of a 24-hour cycle. Using Assumption 1, this gives the daily distribution of appliance fires.

Column 3 shows the proportion of appliance fires that are attributable to washing machines, tumble dryers, washer-dryer combos and dishwashers during each hour of a 24-hour cycle. This calculation is based on Assumptions 3 and 4, and the proportion is derived from Table 10 in the model (see below).

Column 4 shows the time-shifted distribution for appliance fires that are attributable to washing machines, tumble dryers, washer-dryer combos and dishwashers during each hour of a 24-hour cycle. This calculation is based on Assumptions 4 and 5, and the changes are shown in bold text in the table above. 20% of the fires in each hourly period between 4pm and 9pm have been shifted by 8 hours, in 80% of cases, for example, 20% of 80% of all fires occurring between 6pm and 7pm have been time-shifted to 2am-3am.

Column 5 shows the daily distribution of appliance fires excluding the fires attributable to washing machines, tumble dryers, washer-dryer combos and dishwashers.

Column 6 shows the daily distribution of appliance fires after the fires attributable to washing machines, tumble dryers, washer-dryer combos and dishwashers have been time-shifted.

Table 9 in the model uses Assumption 7 to calculate the ratio of fatalities to casualties for appliance-related fires.

Table 9: Model data

Year	Fatalities	Injuries	Fatalities as % of Casualties for all fires
2010	59	1239	4.5%

2011	55	1227	4.3%
2012	42	1153	3.5%
2013	49	1054	4.4%
2014	29	972	2.9%
2015	33	984	3.2%
2016	46	889	4.9%
Sum	**313**	**7518**	4.0%

Source: Fire Facts London 1, Worksheet 1.2

Table 10 in the model calculates the breakdown of fires across the types of appliance that fall within the scope of this project. The washing machine category also includes the data for spin dryers.

Table 5: Model data

Domestic Appliances Considered by this Project		Number of Fires 2010-2016	Average Number of Fires / Year	% of Fires	% of ALL Appliance Fires
Cooker incl.oven		64,986	9,284	82.5%	52.5%
Tumber dryer		4,615	659	5.9%	3.7%
Washing machine		4,296	614	5.5%	3.5%
Dishwasher		2,536	362	3.2%	2.1%
Fridge/freezer		1,850	264	2.3%	1.5%
Washer/Dryer combi		530	76	0.7%	0.4%
Total		78,813	11,259	100.0%	63.7%

Source: Domestic Appliance Fires Dataset Guidance, Home Office, 10 May 2018, p10.

9.1.2 Summary of Assumptions and Results

The calculation of the principal results for the model is shown below.

Note, within the report we have referenced the percentage increase in fatalities due to an increase of fires at night-time. This is seen as more robust than the estimated absolute additional fatality number, as the model calculates those based on past casualty and fatality data. Since appliances are getting safer over time, fires and hence casualties / fatalities are decreasing over time. We have modelled smart appliance uptake by 2030, the overall number of appliance fires should have decreased by then compared to the assumptions in this model. Hence the absolute figures in Table 11 overestimate the additional fatalities in 2030. However, the increase in casualties / fatalities in percentage is still correct and hence more accurate to use than the absolute figure displayed below.

Table 6: Calculation of principal results

Parameter	Assumptions, with results for 3 levels of DSR sign-up			Source
	Low	Mid	High	
Number of appliance fires / year in UK (all domestic appliance types)		17,670		Domestic Appliance Fires Dataset Guidance, Home Office, 10 May 2018, p10.
Number of appliance fires / year in UK (appliances listed in Table 1)		11,259		Domestic Appliance Fires Dataset Guidance, Home Office, 10 May 2018, p10.
% fires / year in WM, TD & DW between 4pm - 9pm:		4.8%		
Percentage of WM, TD & DW signed-up for time-shifting	10%	20%	30%	MM estimate (Assumption 5), based on Baringa/Element Energy (2012): Electricity System Analysis – future system benefits from selected DSR scenarios
Percentage of times that WM, TD & DW are used in smart mode	80%	80%	80%	MM estimate (Assumption 5), based on Baringa/Element Energy (2012): Electricity System Analysis – future system benefits from selected DSR scenarios
Additional fires / year at night-time due to time-shifting	**43**	**87**	**130**	

% Increase in fires / year at night time due to time shifting %	**3%**	**6%**	**9%**	
UK fires with casualties / 1k fires for WM, TD & DW:		61		UK Government Fire Statistics analysed by London Fire Brigade.
UK fires with casualties / 1k fires for time-shifted WM, TD & DW:		194		Source: UK Government Fire Statistics analysed by London Fire Brigade.
Additional UK fires with casualties / year due to fires shifted to night-time:	**6**	**12**	**17**	
Fatalities as % of casualties for appliance-related fires		4.0%		Fire Facts London 1, Worksheet 1.2
Additional UK fires with fatalities / year due to fires shifted to night-time:	0.2	0.5	0.7	
Average number of fatalities for UK fatal appliance fires		2.3		UK Government Fire Statistics, FIRE0602, Worksheet: Data Fire-Related Fatalities.
Additional UK fatalities / year due to fires shifted to night-time:	**0.5**	**1.1**	**1.6**	
Increase in UK fatalities and fires with casualties / year in %	**0.6%**	**1.3%**	**1.9%**	

Source: Mott MacDonald

Since the figure of 20% used in Assumption 5 is subject to uncertainty, a sensitivity analysis was carried out to investigate the impact of changing the assumption to 30% or 10%.

Contact us if you have any enquiries about this publication, including requests for alternative formats, at: OPSS.enquiries@beis.gov.uk

Office for Product Safety and Standards

Department for Business, Energy and Industrial Strategy
4th Floor, Cannon House, 18 The Priory Queensway, Birmingham B4 6BS
https://www.gov.uk/government/organisations/office-for-product-safety-and-standards