ENA Smart Metering Security & Privacy Control Points

For: Energy Networks Association

May 2010

Engage Consulting Limited

Document Ref: ENA-CR009-002 -1.1

Restriction: ENA authorised parties

www.engage-consulting.co.uk

Executive Summary

Use Case Control Points

The network operators' smart meter functionality requirements will enable them to collect the data to fulfil their business processes thereby enabling the implementation of Smart Grids in Great Britain. The uses of the data have been detailed in a series of Use Cases that include a basic flow of steps to describe the interaction between the actors (such as the network operator) and the smart metering system. Each of the individual steps can be deemed to be a control point where security and privacy issues and risks can be assessed. This assessment has been completed for each of the Use Cases produced for the electricity and gas network operators and is discussed in this paper.

Data Ownership

The most critical issue that requires Government confirmation is in the area of identifying who will own the smart metering data. If the consumer owns the data then the network operator will require customer permission to access the smart metering information required to make a smart grid a reality. If not all customers provide that consent then the effectiveness of network operator planning, network management, balancing, and safety activities will be impaired, not to mention the impact this would have on the assumptions underpinning the cost benefit analysis case for smart metering in GB.

Data Security and Privacy

Assuming that the network operators are able to access all the data they have specified at the required level of granularity, then that data must remain confidential and secure. Access to smart metering data must be via robust authentication processes that ensure that the party attempting to gain access is who they say they are. Once that access is achieved then robust authorisation processes must ensure that the party can only access the data and meter functionality that their role entitles them to.

Data that is extracted from the smart metering systems must be encrypted in such a way that only the intended recipient can decrypt and discern useful information from it.

Most of the network operator uses of smart metering data require knowledge of the location of the meter (or group of meters) in relation to where they connect to the LV network. Typically the network operator only needs this data in an aggregated format to understand the impact on their network and it should be provided at the appropriate level. The privacy concern related to specific properties is that the information could be used to determine the habits and behaviour of the occupant of the property the meter is connected to, and hence may fall into the hands of unauthorised parties enabling them to use the data to discern patterns in behaviour of the occupant. The inclusion of rigorous and robust security and privacy measures at the outset should resolve this issue.

Unauthorised Access

Some of the actions a network operator may take through a smart meter to manage their network will have significant impact on the end user, in the most extreme cases leaving them without power or gas. It is therefore essential that rigorous and robust authentication and authorisation processes are used to ensure that unauthorised parties cannot gain access to the smart meters to initiate any of these functions as an accident or a deliberate attempt at disruption.

Observations & Recommendation

It is essential that the security and privacy aspects of any smart metering system and smart grid are given appropriate consideration early in the design process so that the required privacy arrangements and security protocols are "baked in" to the system. This will then minimise the risk of security or privacy breaches occurring once the smart metering system is in place, so avoiding a major negative impact on the public's view of smart meters and grids and avoiding the considerable extra cost of trying to retrofit additional security and privacy measures into an existing system.

This report contains detail of the Risk Assessment undertaken for the Network Businesses based on their set of Use Cases illustrating the key aspects of their businesses requirements for smart metering to deliver a smart grid. This material should be used with detail from other key stakeholders e.g. Retailers, to help DECC/Ofgem E-Serve develop a complete list of High Level Privacy and Security Requirements that can be used to develop a balanced Privacy and Security architecture to deliver the roll-out of smart meters within GB that will also support the development of a Smart Grid.

Document Control

Authorities

Version	Issue Date	Author	Comments
0.1	9th April 2010	Craig Handford & James Boraston	Use Case control points
0.2	12th April 2010	James Boraston	Report first draft
0.3	15th April 2010	James Boraston	Update with comments and include Dutch smart experience in appendix
0.4	22nd April 2010	Tom Hainey	Review and minor update prior to issuing to ENA members for review
0.5	27th April 2010	James Boraston	Incorporate ENA member comments
1.0	29th April 2010	James Boraston / Tom Hainey	Issue to ENA Members
1.1	12th May 2010	Tom Hainey	Minor update to Executive Summary
Version	**Issue Date**	**Reviewer**	**Comments**
0.2	14th April 2010	Tom Hainey	Review of first draft
1.0	29th April 2010	Tom Hainey	Review after ENA Members comments incorporated
1.1	12th May 2010	Tom Hainey	Minor update to Executive Summary
Version	**Issue Date**	**Authorisation**	**Comments**

Related Documents

Reference 1	ENA Smart Metering Project Initiation Document (ENA-CR004-001-1.0)
Reference 2	ENA Smart Metering System Use Cases (ENA-CR007-002-1.1)
Reference 3	DECC – "Towards a smarter future: Government response to the Consultation on Electricity and Gas Metering".
Reference 4	High Level Smart Metering and Smart Grid Security Considerations (ENA-CR009-001-0.4)

Distribution

Recipient 1 - Alan Claxton (ENA)
Recipient 2 - ENA Members

Table of Contents

1 Introduction

Since their production of an initial set of ENA Requirements for Smart Metering which formed part of their response to the DECC consultation on smart metering, the ENA and its member companies have recognised the importance of further developing their original functional specification in order to fully support the objectives of the ENSG Smart Grid Vision and Route map, and in recognition of the importance that DECC has placed on the development of Smart Grids. In order to achieve this objective, ENA has commissioned Engage Consulting Limited (Engage) to undertake a project (PID – Reference 1) to address 4 key areas of work as follows:

- **Workstream 1 – ENA Smart Metering System Requirements:** Update and enhance key network requirements needed to support current network businesses and the future needs of Smart Grids;
- **Workstream 2 - Development of Appropriate Use Cases:** To fully articulate the key aspects of the ENA requirements it is intended that specific Use Cases will be developed for critical areas related to energy network businesses and smart grids;
- **Workstream 3 – Performance Standards & Communication Requirements:** This workstream will develop appropriate scenarios for each Use Case and undertake a data traffic analysis to assess the impact this will have on the smart metering communications infrastructure; and
- **Workstream 4 - Privacy & Security Considerations:** This activity will provide an overview of the scope, principles and concepts that need to be considered when developing a secure smart metering system solution to take account of the Energy Networks additional requirements.

This report represents the final output of Workstream 4.

1.1 Background

The Government's response to the DECC smart metering consultation process (Reference 3) included a number of statements emphasising the importance of developing a smart grid in Great Britain and of ensuring that network businesses were able to contribute by specifying the functional requirements of a smart metering system that would be required to support that objective.

It is therefore imperative that the correct level of factual and detailed information is fed into Ofgem E-Serve's Phase 1 work. This will ensure that in developing the smart meter functionality and communications infrastructure requirements, full account can be taken of the short, medium and long term needs of network operators such that the key functionalities can be incorporated in an appropriate manner and within the relevant timescales.

1.2 Purpose

Purpose of this report is to:

- Identify the security and privacy issues and risks from the basic steps in the electricity use case flows;

- Identify the security and privacy issues and risks from the basic steps in the gas use case flows; and
- Highlight the key security and privacy issues and risks

1.3 Scope

This project is focused on ensuring that the requirements of energy networks – in respect of the short, medium and longer term functionality required of smart metering, and associated communication infrastructure - are clearly defined and aligned with work being undertaken by the DECC/Ofgem E-Serve Smart Metering Implementation Project. This particular report details some specific security and privacy issues and risks that may arise from the ENA members smart metering functionality requirements.

1.4 Copyright and Disclaimer

The copyright and other intellectual property rights in this document are vested in ENA. Engage Consulting Limited has an unlimited licence to use any techniques or know-how developed by it under this Agreement on its future work.

No representation, warranty or guarantee is made that the information in this document is accurate or complete. While care is taken in the collection and provision of this information, Engage Consulting Limited shall not be liable for any errors, omissions, misstatements or mistakes in any information or damages resulting from the use of this information or action taken in reliance on it.

2 Use Case Security & Privacy Control Points Review

The detail of the ENA members Smart Metering requirements have been described in the electricity and gas Use Cases documented in the ENA Smart Metering System Use Cases (ENA-CR007-002-1.1) product from Workstream 2 of this project. Each Use Case includes steps from a basic (everything goes as expected) and alternative flow (problems are encountered) that detail the interaction between an actor (or actors) and the Smart Metering System. Each of the basic steps within a Use Case is a control point where the flow could cease or deviate if a problem arises. For the purposes of this analysis we have analysed the security and privacy issues and risks applicable at each of those control points and suggested some potential solutions.

The full set of Use Case steps and identified issues and risks are included in Appendix A for electricity and Appendix B for gas.

This section provides an overview of the findings from the analysis.

2.1 Key Findings

The same security control point issues and risks were identified for both gas and electricity Use Cases. This section will therefore not differentiate between the two fuels.

At a high level the security control point issues and risks identified fall into two categories:

- Data issues; and
- Authentication and authorisation issues.

2.2 Data issues

There is the potential for a wide variety of issues with the Smart Metering data that network operators may wish to use. The data incorporates measurement data (power flow, voltages, etc.), meter standing data and messages (control, configuration, alarms, etc.) These issues include security and privacy and are summarised in Table 1 below including an indication of the priority of the issue / risk.

Table 1 – Summary of data issues identified from analysing the electricity and gas use cases

Issue / Risk	Recommendation	Priority
Customer has not given consent for data to be taken	Develop robust consenting process presumably run by Suppliers as they have the customer relationship	H
Incorrect configuration of validation rules	Defined and robust rules must be specified in the early design of systems	H
Data corrupted in transit	Develop robust validation rules	H
Incorrect / non compliant data is received / sent	Develop robust validation rules	H

Issue / Risk	Recommendation	Priority
Received data isn't stored securely	DNO's and Smart Metering System need to have secure and robust management of data	H
Data no longer available / deleted / overwritten	Data needs to be secure and confidential	M
Data not received in time	Smart Meters are correctly configured and updated	M
Data lost	Communication channels are secure allowing retrieval of "lost" data through back-ups	M
Incorrect configuration for time period	Develop robust authentication rules	M
Data loaded into incorrect system	DNO's and Smart Metering System need to have secure and robust management of data	M
Incorrect data collected	Clear and robust configuration rules required Develop robust validation rules	M
Storage limits exceeded	Appropriate measured data storage requirements at the DNOs and Smart Metering System	L

2.2.1 Data ownership

The question of which party owns the data that the smart meter measures, records and stores is one that has not been resolved as yet. This is however an issue with massive implications to the Great Britain cost benefit analysis case for Smart Grids and Smart Metering.

In a recent on-line smart metering discussion[1], a representative from Consumer Focus (the statutory watchdog for UK consumers, including energy), stated that from "their perspective consumers have the right to own their own data and choose how it is used. In practice this means that all the data collected by the meter should be kept within the home meter."

If this view is adopted by Ofgem E-Serve and the Government, then network operators will require the consent of the consumer before they can extract the data from the smart meters that they will need to fulfil their business processes captured in the use cases.

An argument could be made that some of the data items the network operators require, such as voltage, are measuring the quality of the delivered energy and as such is more the networks' data than the consumers.

Other data items such as meter standing data, e.g. the Calorific Value, and command or configuration messages from network operators, could also be argued to not belong to the customer.

[1] Zoe McLeod, Consumer Focus, 5th March 2010. http://www.utilityweek.co.uk/news/uk/electricity/online-smart-metering-discussi.php

2.2.2 Privacy

Most of the network operator's uses of the smart metering data require them to know where the meter is located in relation to the network. For some, though not all of the smart meter measured parameters, this locational information could allow parties to determine the habits of the occupants of the property, and hence by analysing the data derive private information about them. Times of occupancy, use of specific equipment, and other information could be derived that would be of use for marketing purposes or even for criminals.

Any data stored in the meter, transmitted through the communication network, or stored within network operator systems, must be held securely, with robust authentication and authorisation rules ensuring access to the meter and data only by authorised parties, and encrypted when in transit ensuring that should the data be intercepted by an unauthorised party they cannot use it.

If a unique method of identifying the location of the meter, similar to a computer IP address, is adopted then data could be securely stored within network operator systems using a reference key to determine the location. This would then ensure that should the data be accessed by unauthorised parties it would be useless without the reference key.

2.2.3 Data integrity

Integrity is the assurance that any data received are exactly as sent by an authorised entity – i.e. they contain no modification, insertion or deletion.

Network Operators need to be sure that the data they receive from smart meters is from the meter they expect it to be from, and that it has not been tampered with, or become corrupt in transit.

To ensure this the data must be securely stored within the meter, must be encrypted on exit, and pass through robust validation processes to ensure that it is the same on receipt as it was when it left the meter. The Smart Meter must include validation of the data before it is able to be sent. Validation must then also occur at the recipient before the data is accepted.

2.3 Authentication and Authorisation issues

The practise of authentication establishes that parties attempting to access the meter, network and data are in fact who they say they are. Authorisation then defines what a party is allowed to do once they have been authenticated.

There were several authentication and authorisation issues identified within the electricity and gas Use Case steps, which are summarised in the following table with an assessment of the priority of the issue / risk.

Table 2 – Summary of authentication and authorisation issues identified from analysing the electricity and gas use cases

Issue / Risk	Recommendation	Priority
Data intercepted by unauthorised recipient	Develop robust authorisation and encryption rules Access to data must be encrypted	H

Data sent by unauthorised party	Develop robust authentication rules	H
Data sent to the wrong recipient	Develop robust authorisation and encryption rules	H
Unauthorised party configures Smart Metering System to stop recording data	Access to configure the meter must be via robust authentication and authorisation rules	H
Unauthorised access to customer data	Develop robust consenting process presumably run by Suppliers as they have the customer relationship	H
Incorrect configuration of validation rules	Defined and robust rules must be specified in the early design of systems	H
Data obtained for the wrong customer	Develop robust authorisation and encryption rules	H
Incorrect configuration for time period	Develop robust authentication rules	M
Data sent to wrong IHD	Develop robust authorisation and encryption rules	L

2.3.1 Unauthorised access to the meter

It is essential that only fully authenticated and authorised parties are able to access the smart meters. The authentication rules must ensure that a party trying to access the meter is who they say they are, and then once that access has been granted, the authorisation rules must restrict access to only the functionality and associated data that this party is entitled and authorised to see.

This is particularly critical considering the functionality that network operators wish to have included in smart meters.

There are forms of direct intervention with the smart meter systems that a network operator has proposed, such as:

- **Maximum power threshold** – this sets an upper limit to the power that can be consumed at premises to enable more properties to remain on supply during system constraint or fault. Consumption over the specified level will result in a warning message followed by disconnection if energy use remains high. The assumption here is that the householder will have agreed to these actions being undertaken by the network operator under emergency conditions;
- **Direct control of appliances -** Smart Metering System to communicate with Energy Management System's within the premises to determine when appliances draw load. The assumption here is that the householder will have agreed to these actions being undertaken by the network operator;
- **Direct control of micro-generation** – Smart Metering System to communicate with micro-generation installed at premises to reduce generation when network conditions require it. Again consent is assumed to have been given by the householder in advance; and
- **Auto-disconnection / Auto-isolation** – the Smart Meters will be configured to detect conditions that may present a safety risk to the consumer or attached equipment, such as extremes in voltage or dangerous gas conditions, that will initiate auto-disconnection/isolation

from the network. This is linked to health and safety and overrides any privacy issues.

If a malicious unauthorised party was able to access this functionality it could have major consequences such as consumers being left without power. Any successful attacks such as these would severely damage the customer view, and acceptance, of smart metering and smart grids and so must be robustly guarded against.

There are other forms of interaction with the smart meter systems, such as the network operators sending messages to the meter and/or the In Home Display, e.g.:

- Notifying customers of planned outages;
- Notifying customers of network emergencies;
- Updating stored Calorific Values (potentially); and
- Updating the meter with tariff details.

If unauthorised parties were able to hack into the system to send messages disrupting these uses it would have less of an extreme impact than the previous examples, but would still badly damage customer confidence in smart metering and smart grids.

A further nuisance impact of unauthorised access to the meter, that would be unlikely to be noticeable to the customer, would be an unauthorised party changing the configuration settings within the meter, e.g. changing the frequency of reads, validation rules, etc.

2.3.2 Unauthorised access to data

Robust authorisation rules must ensure that parties authenticated as having permission to access the smart metering system can only access the functionality, and data, they are authorised to use or see. To satisfy confidentiality requirements there must be robust encryption methods that ensure that only authorised parties in possession of the relevant encryption key will be able to decrypt any data obtained from the smart metering system.

There must be similarly tight security measures employed to protect smart metering data stored within network operator systems to ensure that confidentiality requirements are met.

3 Observations & Recommendations

3.1 Observations

The issues of security and privacy for smart metering systems and smart grids are becoming a key area of focus in many countries. For example:

- The publication of the draft 'Smart Grid Cyber Security Strategy and Requirements' by the U.S. National Institute of Standards and Technology (NIST) focused mainly on the Security of smart grids and was criticised by privacy organisations regarding its approach to privacy when initially published. The updated draft issued in February 2010 has included additional detail regarding privacy provided by their Privacy Sub-group who conducted a privacy impact assessment (PIA) for the consumer-to-utility portion of the Smart Grid. Appendix C provides a brief summary of the key tasks that NIST indicate should be part of any Smart Grid Cyber Security Strategy.
- The Dutch experience of getting to the point of seeking approval from their Senate for a mandated roll-out of smart meters which was to capture 15 minute data, only to see it rejected due to Consumer groups lobbying that what they proposed broke Article 8 of the European Convention on Human Rights. This has resulted in extensive work in the Netherlands to ensure Privacy concerns are dealt with and seen to be at the heart of whatever proposal regarding smart meters they take forward. Brief details of this are provided in Appendix D for reference.

For those countries that have already implemented smart metering roll-outs in Europe (e.g. Sweden and Italy) it is unclear how much emphasis was given to security and privacy issues in their overall system design. Only time will tell if they got the balance right between the Utility requirements for data and end-to-end system security and overall privacy of personal data. Any problems will potentially be expensive to rectify.

With GB just about to move into the design stage of their smart metering / smart grid solution it is imperative that the dual aspects of end-to-end system security and the privacy of personal data are given appropriate consideration in the system design phase. This is an area where any time and cost of developing these aspects appropriately should be considered as a necessary cost of doing business, with any cost to deliver this being considered as 'ring-fenced' and protected from any attempts to reduce it to control an overall project budget. Once installation occurs, and processes go live the cost of addressing exposed security or privacy risks will be many times any cost savings made in not addressing these concerns during the design phase.

3.2 Recommendations

It is essential that the security and privacy aspects of any smart metering system and smart grid are given appropriate consideration early in the design process so that the required privacy arrangements and security protocols are "baked in" to the system. This will then minimise the risk of security or privacy breaches occurring once the smart metering system is in place, so avoiding a major negative impact on the public's view of smart meters and grids and avoiding the considerable extra cost of trying to retrofit security and privacy measures into an existing system.

This report contains detail of the Risk Assessment undertaken for the Network Businesses based on their set of Use Cases illustrating the key aspects of their businesses requirements for smart metering to deliver a smart grid. This material should be used with detail from other key stakeholders e.g. Retailers, to help DECC/Ofgem E-Serve develop a complete list of High Level Privacy and Security Requirements that can be used to develop a balanced Privacy and Security architecture to deliver the roll-out smart meters within GB that will also support the development of a Smart Grid.

Appendix A - Electricity Use Case Security Control Points

1. Approach

Based on the final list of Use Cases it is intended that the Basic Steps that are shown for each Use Case will be reviewed to identify for each step any Security & Privacy Issues / Risks and identify any appropriate recommendations to address them.

It should be noted that due to the structure of the Use Case documents created there will be repetition in the basic steps between several Use Cases. All of the Use Case basic steps have been included here for completeness.

2. Security & Privacy Review

The security control points below majors on the security issues, but also covers key privacy areas related to consumer data that might be an issue and need to be dealt with.

3.3 Assessment of Network Performance

3.3.1 01 - Monitor Power Flows and Voltage Levels to Identify Thermal Capacity and Statutory Voltage Headroom

Scenario 1 – Data is sent periodically from the Smart Metering System

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Smart Metering System determines that the DNO configured time period that has been set to send data has been reached and sends the half-hourly data to the Distribution Network Operator	• Incorrect configuration for time period • Data sent to the wrong recipient • Data intercepted by unauthorised recipient • Data corrupted in transit	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Develop robust validation rules
2	The Distribution Network Operator receives the data and loads it into its system to use in monitoring power flows and voltage levels	• Incorrect / non compliant data is received • Data no longer available / deleted / overwritten	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and to be confidential • Data transfer rules required
3	The Smart Metering System continues to	• Data intercepted by unauthorised recipient	• Develop robust authentication rules

	make available data to the DNO at the predetermined interval until the DNO configures it to stop	• Incorrect data received • Data loaded into incorrect system • Received data isn't stored securely • Unauthorised party configures Smart Metering System to stop recording data	• Develop robust authorisation and encryption rules • Develop robust access and use rules • Access to data must be encrypted • Access to configure the meter must be via robust authentication and authorisation rules • Data needs to be secure and confidential • DNO's and Smart Metering System need to have secure and robust management of data
	Alternative Flows		
	At Basic Flow step 2		
2a 1	The Distribution Network Operator does not receive the data	• Data sent to wrong recipient • Data intercepted by unauthorised recipient	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Develop robust access and use rules • Data transfer rules required
2a 2	The Distribution Network Operator checks and takes steps to ensure that the Smart Metering System has been configured correctly and is working properly	• Data not received in time • Data lost • Smart Metering System accessed and configured by unauthorised party	• DNO's and Smart Metering System need to have secure and robust management of data • Develop robust consenting process presumably run by Suppliers as they have customer relationship • Access to configure Smart Metering System via robust authentication and authorisation rules
2a 3	Go back to Basic Flow step 1	• See Step 1	

Scenario 2 – DNO requests data

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Distribution Network Operator sends a message to the Smart Metering System requesting the stored half-hourly power flow (including that of any collected generation data) and voltage data	• Unauthorised access to customer data • Customer has not given consent for data to be taken • Request sent to the wrong recipient • Request intercepted by unauthorised recipient • Request sent to wrong group of meters	• Develop robust consenting process presumably run by Suppliers as they have customer relationship • Develop robust authentication rules • Develop robust authorisation and encryption rules
2	The Smart Metering System receives the message and validates it	• Request sent to the wrong recipient • Request sent by unauthorised party • Request sent to wrong group of meters	• Develop robust authentication rules • Develop robust authorisation and encryption rules
3	The Smart Metering System retrieves the stored half-hourly power flow (including that of any generation data), and voltage data	• Incorrect / non compliant data is retrieved • Data no longer available / deleted / overwritten	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and confidential • Data transfer rules required
4	The Smart Metering System sends the data to the Distribution Network Operator	• Data intercepted by unauthorised recipient • Data sent to incorrect recipient • Data corrupted in transit	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Develop robust validation rules
5	The Distribution Network Operator receives the data and loads it into its system to use in monitoring power flows and voltage levels	• Incorrect data received • Data loaded into incorrect system • Received data isn't stored securely • Data sent by unauthorised party	• Develop robust access and use rules • Access to data must be encrypted • Data needs to be secure and confidential • DNO's and Smart Metering System need to have secure and robust management of data
Alternative Flows			

	At Basic Flow step 2		
2a 1	The Smart Metering System rejects the message as invalid	• Incorrect data sent / received • Incorrect validation rules	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required
2a2	The Smart Metering System sends notification to the Distribution Network Operator detailing error type along with date/time stamp	• Notification not sent	• Data transfer rules required with system 'handshakes'
2a 3	The Distribution Network Operator receives the message and takes the required steps to resolve the error	• Unsure how to correct data • Insufficient information sent to resolve the error i.e. error unclear	• Data transfer rules required
2a 3	Once error is resolved go back to Basic Flow step 1	• See Step 1	
	At Basic Flow step 3		
3a1	The Smart Metering System does not have any measured data stored	• Incorrect / non compliant data being requested • Data no longer available / deleted / overwritten • Customer has not given consent to data to be taken	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required • Develop robust consenting process presumably run by Suppliers as they have customer relationship
3a 2	The Smart Metering System sends a no data found message to the Distribution Network Operator	• Error not sent / sent incorrectly	• Data transfer rules required
3a 3	The Distribution Network Operator checks and takes steps to ensure that the Smart Metering System has been configured correctly	• Incorrectly configured • Incorrect data being requested	• Data transfer rules required • Develop robust consenting process presumably run by suppliers as they have customer relationship

	and is working properly		
3a4	End flow		
	At Basic Flow step 5		
5a 1	The Distribution Network Operator does not receive the data from the Smart Metering System	- Incorrect / non compliant data being sent - Unable to process data - No data received for DNO purposes	- Data transfer rules required - Develop robust consenting process presumably run by suppliers as they have customer relationship - Develop robust access rules
5a 2	The Distribution Network Operator checks and takes steps to ensure that the Smart Metering System has been configured correctly and is working properly	- Incorrectly configured - Incorrect data being requested	- Data transfer rules required - Develop robust consenting process presumably run by suppliers as they have customer relationship
5a 3	Go back to Basic Flow step 1	- See Step 1	

3.3.2 02 - Determine Network Impact of Proposed New Demand / Generation Connections

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Distribution Network Operator sends a message to the Smart Metering System requesting the stored half-hourly power flow and voltage data (and micro-generation data where available)	- Unauthorised access to customer data - Customer has not given consent for data to be taken - Request sent to the wrong recipient - Request intercepted by unauthorised recipient - Request sent to wrong group of meters	- Develop robust consenting process presumably run by Suppliers as they have customer relationship - Develop robust authentication rules - Develop robust authorisation and encryption rules
2	The Smart Metering System receives the message and validates it	- Request sent to the wrong recipient - Request sent by unauthorised party - Request sent to wrong	- Develop robust authentication rules - Develop robust authorisation and encryption rules

		group of meters	
3	The Smart Metering System retrieves the stored half-hourly power flow and voltage data	• Incorrect / non compliant data is retrieved • Data no longer available / deleted / overwritten	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and confidential • Data transfer rules required
4	The Smart Metering System sends the data to the Distribution Network Operator	• Data intercepted by unauthorised recipient • Incorrect data sent • Data sent to incorrect recipient • Data corrupted in transit	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Develop robust access and use rules • Develop robust validation rules • Access to data must be encrypted • Data needs to be secure and confidential • DNO's and Smart Metering System need to have secure and robust management of data
5	The Distribution Network Operator receives the data and loads it into its system / procedure for determining network capacity	• Data intercepted by unauthorised recipient • Incorrect data received • Data loaded into incorrect system • Received data isn't stored securely • Data sent by unauthorised party	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Develop robust access and use rules • Access to data must be encrypted • Data needs to be secure and confidential • DNO's and Smart Metering System need to have secure and robust management of data
Alternative Flows			
	At Basic Flow Step 5		
5a 1	The Distribution Network Operator does not receive the data	• Data no longer available / deleted / overwritten • Customer has not given consent for data to be taken	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and confidential • Data transfer rules required • Develop robust consenting process presumably run by Suppliers as they have customer relationship

5a 2	The Distribution Network Operator checks and takes steps to ensure that the Smart Metering System has been configured correctly and is working properly	• Incorrectly configured • Incorrect data being requested • Configuration changed by unauthorised party	• Data transfer rules required • Develop robust consenting process presumably run by Suppliers as they have customer relationship • Access to configure Smart Metering System via robust authentication and authorisation rules
5a 3	Go back to Basic Flow step 1	• See step 1	

3.3.3 03 - Determine Network Impact of Proposed Increases in Demand / Generation at Existing Connection Points

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Distribution Network Operator sends a message to the Smart Metering System requesting the stored half-hourly power flow and voltage data (and micro-generation data where available)	• Unauthorised access to customer data • Customer has not given consent for data to be taken • Request sent to the wrong recipient • Request intercepted by unauthorised recipient • Request sent to wrong group of meters	• Develop robust consenting process presumably run by suppliers as they have customer relationship • Develop robust authentication rules • Develop robust authorisation and encryption rules
2	The Smart Metering System receives the message and validates it	• Request sent to wrong recipient • Request intercepted by unauthorised recipient • Request sent to wrong group of meters	• Develop robust authentication rules • Develop robust authorisation and encryption rules
3	The Smart Metering System retrieves the stored half-hourly power flow and voltage data	• Incorrect / non compliant data is received • Data no longer available / deleted / overwritten	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required
4	The Smart Metering System sends the data to the Distribution Network Operator	• Data intercepted by unauthorised recipient • Incorrect data sent • Data sent to incorrect recipient	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Develop robust access and

		• Data corrupted in transit	use rules • Access to data must be encrypted • Data needs to be secure and be confidential • DNO's and Smart Metering System need to have secure and robust management of data
5	The Distribution Network Operator receives the data and loads it into its system / procedure for determining network capacity	• Data intercepted by unauthorised recipient • Incorrect data received • Data loaded into incorrect system • Received data isn't stored securely • Data sent by unauthorised party •	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Develop robust access and use rules • Access to data must be encrypted • Data needs to be secure and be confidential • DNO's and Smart Metering System need to have secure and robust management of data
Alternative Flows			
	At Basic Flow Step 5		
5a 1	The Distribution Network Operator does not receive the data	• Incorrect / non compliant data being requested • Data no longer available / deleted / overwritten • Customer has not given consent for data to be taken	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required • Develop robust consenting process presumably run by Suppliers as they have customer relationship
5a 2	The Distribution Network Operator checks and takes steps to ensure that the Smart Metering System has been configured correctly and is working properly	• Incorrectly configured • Incorrect data being requested • Meter configured by unauthorised party	• Data transfer rules required • Develop robust consenting process presumably run by Suppliers as they have customer relationship • Access to configure Smart Metering System via robust authentication and authorisation rules
5a 3	Go back to Basic Flow step 1		

3.3.4 04 – Monitor Demand and Generation Profiles for Network Load Forecasting

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	At the defined interval the Smart Metering System collects the data and sends it to the Distribution Network Operator	• Incorrect configuration for time period • Data sent to the incorrect recipient • Data intercepted by unauthorised recipient • Incorrect data sent • Data corrupted in transit	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Develop robust validation rules • Access to data must be encrypted • Data needs to be secure and confidential • DNO's and Smart Metering System need to have secure and robust management of data
2	The Distribution Network Operator receives the data and loads it into their systems	• Incorrect / non compliant data is retrieved • Data no longer available / deleted / overwritten • Data corrupted in transit • Data loaded into incorrect system • Received data isn't stored securely • Data sent by unauthorised party	• Develop robust access and use rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required • DNO's and Smart Metering System need to have secure and robust management of data
Alternative Flows			
	At Basic Flow step 2		
2a 1	The Distribution Network Operator does not receive the data from the Smart Metering System	• Incorrect / non compliant data being requested • Data no longer available / deleted / overwritten • Customer has not given consent for data to be taken • Data corrupted in transit	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required • Develop robust consenting process presumably run by Suppliers as they have customer relationship
2a 2	The Distribution Network Operator checks and takes steps to ensure the Smart Metering System is	• Incorrectly configured • Configured by unauthorised party	• Data transfer rules required • Access to configure Smart Metering System via robust authentication and authorisation rules

	configured correctly and had data to send		
2a 3	The Distribution Network Operator requests the Smart Metering System resends the data	• Incorrect data being requested • Request intercepted by unauthorised party	• Develop robust authentication rules • Develop robust authorisation and encryption rules
2a 4	The Smart Metering System resends the data	• Data intercepted by unauthorised recipient • Data sent to wrong recipient • Incorrect data sent • Data corrupted in transit	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Access to data must be encrypted • Data needs to be secure and confidential • DNO's and Smart Metering System need to have secure and robust management of data
2a 5	Back to Basic Flow step 2	• See step 2	

3.3.5 05 – Determine Latent Demand due to Embedded Generation

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	At the defined interval the Smart Metering System sends the data to the Distribution Network Operator	• Incorrect configuration for time period • Data sent to the incorrect recipient • Data intercepted by unauthorised recipient • Incorrect data sent • Data corrupted in transit	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Develop robust validation rules • Access to data must be encrypted • Data needs to be secure and confidential • DNO's and Smart Metering System need to have secure and robust management of data
2	The Distribution Network Operator receives the data and loads it into their	• Incorrect / non compliant data is received • Data no longer available / deleted / overwritten • Data loaded into incorrect	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and be confidential

	systems	system • Data corrupted in transit	• Data transfer rules required • DNO's and Smart Metering System need to have secure and robust management of data
Alternative Flows			
	At Basic Flow step 2		
2a 1	The Distribution Network Operator does not receive the data from the Smart Metering System	• Information sent to wrong recipient • Non compliant data received • Data no longer available / deleted / overwritten • Customer has not given consent for data to be taken	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Data transfer rules required • DNO's and Smart Metering System need to have secure and robust management of data • Access to data must be encrypted • Data needs to be secure and be confidential • Develop robust consenting process presumably run by Suppliers as they have customer relationship
2a 2	The Distribution Network Operator checks and takes steps to ensure the Smart Metering System is configured correctly and had data to send	• Incorrectly configured • Unable to communicate with metering system • Configured by unauthorised party	• Data transfer rules required • Develop robust authentication rules • Develop robust authorisation and encryption rules • Access to configure Smart Metering System via robust authentication and authorisation rules
2a 3	The Distribution Network Operator requests the Smart Metering System resends the data	• Request sent to the wrong recipient • Request intercepted by unauthorised recipient • Request sent to wrong group of meters	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Data transfer rules required
2a 4	The Smart Metering System resends the data	• Incorrect data collected • Data corrupted in transit • Data sent to wrong recipient • Data intercepted by unauthorised party	• Develop robust access rules • Develop robust authentication rules • Develop robust authorisation and encryption rules • Data transfer rules required • Access to data must be encrypted • Data needs to be secure and confidential

2a 5	Back to Basic Flow step 2	• See step 2	

3.3.6 06 – Identify Voltage Quality Issues

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Smart Metering System accumulates time and date stamped voltage quality events	• Unauthorised access to customer data • Customer has not given consent for data to be taken • Incorrect data received • Data isn't stored securely in the meter	• Develop robust authentication and authorisation process • Develop robust consenting process presumably run by Suppliers as they have customer relationship • Develop robust access and use rules • Access to data must be encrypted • Data needs to be secure and be confidential • DNO's and Smart Metering System need to have secure and robust management of data
2	The Smart Metering System stores the recorded events for a period of three months (after which time the meter continues to record events but overwrites the most historic events)	• Unauthorised access to customer data • Customer has not given consent for data to be taken • Data isn't stored securely in the meter • Wrong data overwritten	• Develop robust authentication and authorisation process • Develop robust consenting process presumably run by Suppliers as they have customer relationship • Develop robust access and use rules • Access to data must be encrypted • Data needs to be secure and confidential • DNO's and Smart Metering System need to have secure and robust management of data
3	The Distribution Network Operator receives the information from the Smart Metering System at the	• Incorrect / non compliant data is retrieved • Data no longer available / deleted / overwritten • Data corrupted in transit • Data sent from	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required

	intervals required	unauthorised party	• Develop robust validation rules
4	The information is analysed to determine if further follow-up investigation is required.	• Internal Process	

3.4 Actively Manage Network / System Balancing

3.4.1 07 - Collect Data for Active Management and System Balancing

Security Control Points			
Control Point No	**Activity**	**Issues / Risks**	**Recommendations**
Basic Flow			
1	The Smart Metering System measures real and reactive power flow and voltage data	• Incorrectly configured • Unauthorised access to customer data • Customer has not given consent to data to be taken	• Clear and robust configuration rules required • DNO's and Smart Metering System need to have secure and robust management of data • Develop robust consenting process presumably run by Suppliers as they have customer relationship
2	The Smart Metering System sends the data to the Distribution Network Operator	• Data sent to the incorrect recipient • Data intercepted by unauthorised party • Incorrect data sent	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Data transfer rules required • Access to data must be encrypted • Data needs to be secure and confidential
3	The Distribution Network Operator receives the data and loads it into its system along with data from sensors within networks and other information to identify whether actions are needed or actions that have been carried out have been successful.	• Incorrect / non compliant data is received • Data no longer available / deleted / overwritten • Data corrupted in transit • Data loaded into incorrect system • Received data isn't stored securely • Data sent by unauthorised party	• Develop robust access rules • Develop robust validation rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required • DNO's and Smart Metering System need to have secure and robust management of data
Alternative Flows			

	At Basic Flow step 2:		
2a 1	The Smart Metering System fails to send the message	• Incorrect request being made • Information sent to wrong recipient	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Data transfer rules required • DNO's and Smart Metering System need to have secure and robust management of data
2a 2	The Distribution Network Operator's systems identify the missing data, the Distribution Network Operator, investigates the cause of the failure and may reconfigure the meter	• Incorrectly configured • Wrong meter re-configured	• Data transfer rules required • DNO's and Smart Metering System need to have secure and robust management of data
2a 3	The use case returns to Basic Flow step 1.	• See step 1	

3.4.2 08 - Active Management of Network Voltage

3.4.2.1 Scenario 1 – Operation of **(Distribution Use of System)** Time of Use Tariff

Security Control Points			
Control Point No	**Activity**	**Issues / Risks**	**Recommendations**
Basic Flow			
1	The Smart Metering System accumulates readings for registers according to the Time of Use tariff	• Unauthorised access to customer data • Customer has not given consent to data to be taken • Incorrectly configured • Storage limits exceeded • Incorrect data collected	• Develop robust consenting process presumably run by Suppliers as they have customer relationship • Clear and robust configuration rules required • DNO's and Smart Metering System need to have secure and robust management of data • Appropriate measured data storage requirements at the DNO's and Smart Metering System

2	The Smart Metering System periodically (according to the schedule) provides readings for the registers associated with the Time of Use tariff to the Distribution Network Operator	• Incorrect data collected • Incorrectly configured • Incorrect configuration for time period	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Data transfer rules required
3	The Distribution Network Operator receives the readings and loads them into their system	• Incorrect / non compliant data is retrieved • Data no longer available / deleted / overwritten • Data sent from unauthorised party • Received data isn't stored securely • Data loaded into incorrect system • Data corrupted in transit	• Develop robust access rules • Develop robust validation rules • Access to data must be encrypted • Data needs to be secure and confidential • Data transfer rules required • DNO's and Smart Metering System need to have secure and robust management of data

Scenario 2 – Operation of (Distribution Use of System) Real Time Pricing

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Distribution Network Operator periodically sends prices to the Smart Metering System	• Incorrect data collected • Incorrectly configured schedule • Data sent to wrong meter/group of meters • Data sent by unauthorised party	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Data transfer rules required
2	The Smart Metering System validates the prices and forwards them to the In Home Display (or other display device)	• Incorrect configuration of validation rules • IHD rejects / doesn't receive the data	• Defined and robust rules must be specified in the early design of systems • Data transfer rules required
3	The Consumer uses the information on their In Home Display to influence their	• Data sent to wrong IHD	• Develop robust authentication rules • Develop robust authorisation and encryption rules

	consumption behaviour either directly or via an Energy Management System		
4	The Smart Metering System periodically sends consumption readings to the Distribution Network Operator	• Unauthorised access to customer data • Customer has not given consent to data to be taken • Incorrect data sent • Data sent to the wrong recipient • Data intercepted by unauthorised party	• Develop robust consenting process presumably run by Suppliers as they have customer relationship • Develop robust authentication rules • Develop robust authorisation and encryption rules • Data transfer rules required
5	The Distribution Network Operator receives the consumption readings and loads them into their system	• Incorrect / non compliant data is retrieved • Data no longer available / deleted / overwritten • Data sent by unauthorised party • Data corrupted in transit	• Develop robust access rules • Develop robust validation • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required

Scenario 3 – Power Sharing by Maximum Power Thresholds

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Smart Metering System recognises that power consumption has reached the threshold configured in the meter	• Incorrect configuration at the meter • Meter configured by unauthorised party	• Defined and robust rules must be specified in the early design of systems • Access to configure the meter must be via robust authentication and authorisation processes
2	The Smart Metering System sends a message to the In Home Display advising of excessive power use and warning the supply will be interrupted unless consumption is reduced	• Incorrect configuration of validation rules • IHD rejects / doesn't receive the data • Message intercepted / blocked by unauthorised party	• Defined and robust rules must be specified in the early design of systems • Data transfer rules required
3	The In Home display receives and displays	• Data sent to wrong IHD • Data intercepted by others	• Develop robust authentication rules • Develop robust authorisation

	the message		and encryption rules
4	The Consumer notes the message and turns off some appliances	• The consumer ignores the message • Message sent to the wrong consumer • Message intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
5	The Smart Metering System recognises that power consumption has dropped below the threshold configured in the meter	• Unauthorised access to customer data • Customer has not given consent to data to be taken • Data obtained for the wrong customer • Data intercepted by others	• Develop robust consenting process presumably run by Suppliers as they have customer relationship • Develop robust authentication rules • Develop robust authorisation and encryption rules
6	The Smart Metering System sends a command to the In Home Display to replace the previous message with one stating consumption has reduced below threshold	• Data sent to wrong IHD • Data intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
7	The Consumer notes the message and acknowledges it at the In Home Display	• The consumer ignores the message • Message sent to the wrong consumer • Message intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
Alternative Flows			
	At Basic Flow step 4:		
4a 1	The Consumer does not turn off some appliances	• Internal / Customer Process	
4a 2	After a predetermined time the Smart Metering System cuts supply and logs the event	• Message intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
4a 3	The Smart Metering System sends a message to the In Home Display stating supply has been interrupted due to	• Data sent to wrong IHD • Data intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules

	excessive power use		
4a 4	The Consumer notes the message and acknowledges it at the In Home Display	• The consumer ignores the message • Message sent to the wrong consumer • Message intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
4a 5	The Consumer turns off some appliances	• Internal / Customer Process	
4a 6	The Consumer restarts supply with an action at the meter (such as pressing a button)	• Internal / Customer Process	
4a 7	The Smart Metering System restarts supply and logs the event	• Internal process	

Scenario 4 – Direct Control by DNO's of Appliances or Micro-generation

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Distribution Network Operator sends a message to the Smart Metering System of an event requiring greater or less demand or greater or less generation for a known duration	• Incorrect data collected • Incorrectly configured • Message sent to wrong recipient • Message intercepted by others • Message sent by unauthorised party	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Data transfer rules required
2	The Smart Metering System validates the message	• Incorrect configuration of validation rules • Smart Metering System rejects / doesn't receive the data	• Defined and robust rules must be specified in the early design of systems • Data transfer rules required
3	The Smart Metering System acknowledges to the Distribution Network Operator that the event has been received	• Data sent to wrong meter • Data intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
4	The Smart Metering	• Data sent to wrong system	• Develop robust

	System forwards the message to the Energy Management System which co-ordinates the change to demand event	• Data intercepted by others	authentication rules • Develop robust authorisation and encryption rules
5	The Energy Management System recognises the end of the change to demand event and allows consumption or generation to return to unfettered use.	• Incorrect configuration	• Defined and robust rules must be specified in the early design of systems • Data transfer rules required

3.4.3 09 - Perform Active Management of Network Power Flow

Scenario 1 – Operation of Time of Use Tariff

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Smart Metering System accumulates readings for registers according to the Time of Use tariff	• Unauthorised access to customer data • Customer has not given consent for data to be taken • Incorrectly configured • Storage limits exceeded • Incorrect data collected	• Develop robust consenting process presumably run by Suppliers as they have customer relationship • Clear and robust configuration rules required • DNO's and Smart Metering System need to have secure and robust management of data • Appropriate measured data storage requirements at the DNO's and Smart Metering System
2	The Smart Metering System periodically (according to the schedule) provides readings for the registers associated with the Time of Use tariff to the Network Operator	• Incorrect data collected • Incorrectly configured • Incorrect configuration for time period	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Data transfer rules required
3	The Network Operator receives the readings	• Incorrect / non compliant data is retrieved	• Develop robust access rules • Access to data must be

	and loads them into their system	- Data no longer available / deleted / overwritten - Data sent from unauthorised party - Received data isn't stored securely - Data loaded into incorrect system - Data corrupted in transit	encrypted - Data needs to be secure and be confidential - Data transfer rules required - DNO's and Smart Metering System need to have secure and robust management of data

Scenario 2 – Operation of Real Time Pricing

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Network Operator periodically sends prices to the Smart Metering System	- Incorrect data collected - Incorrectly configured schedule - Data sent to wrong meter/group of meters - Data sent by unauthorised party -	- Develop robust authentication rules - Develop robust authorisation and encryption rules - Data transfer rules required
2	The Smart Metering System validates the prices and forwards them to the In Home Display (or other display device)	- Incorrect configuration of validation rules - IHD rejects / doesn't receive the data	- Defined and robust rules must be specified in the early design of systems - Data transfer rules required
3	The Consumer uses the information on their In Home Display to influence their consumption behaviour either directly or via an Energy Management System	- Data sent to wrong IHD	- Develop robust authentication rules - Develop robust authorisation and encryption rules
4	The Smart Metering System periodically sends consumption readings to the Network Operator	- Unauthorised access to customer data - Customer has not given consent to data to be taken - Incorrect data sent - Data sent to the wrong recipient - Data intercepted by unauthorised party	- Develop robust consenting process presumably run by Suppliers as they have customer relationship - Develop robust authentication rules - Develop robust authorisation and encryption rules - Data transfer rules required

5	The Network Operator receives the consumption readings and loads them into their system	• Incorrect / non compliant data is retrieved • Data no longer available / deleted / overwritten • Data sent by unauthorised party • Data corrupted in transit	• Develop robust access rules • Develop robust validation • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required

Scenario 3 – Power Sharing by Maximum Power Thresholds

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Smart Metering System recognises that power consumption has reached the threshold configured in the meter	• Incorrect configuration at the meter • Meter configured by unauthorised party	• Defined and robust rules must be specified in the early design of systems • Access to configure the meter must be via robust authentication and authorisation processes
2	The Smart Metering System sends a message to the In Home Display advising of excessive power use and warning the supply will be interrupted unless consumption is reduced	• Incorrect configuration of validation rules • IHD rejects / doesn't receive the data • Message intercepted / blocked by unauthorised party	• Defined and robust rules must be specified in the early design of systems • Data transfer rules required
3	The In Home display receives and displays the message	• Data sent to wrong IHD • Data intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
4	The Consumer notes the message and turns off some appliances	• The consumer ignores the message • Message sent to the wrong consumer • Message intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
5	The Smart Metering System recognises that power consumption has dropped below the threshold configured in the meter	• Unauthorised access to customer data • Customer has not given consent for data to be taken • Data obtained for the wrong customer	• Develop robust consenting process presumably run by Suppliers as they have customer relationship • Develop robust authentication rules • Develop robust authorisation

		• Data intercepted by others	and encryption rules
6	The Smart Metering System sends a command to the In Home Display to replace the previous message with one stating consumption has reduced below threshold	• Data sent to wrong IHD • Data intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
7	The Consumer notes the message and acknowledges it at the In Home Display	• The consumer ignores the message • Message sent to the wrong consumer • Message intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
Alternative Flows			
	At Basic Flow step 4:		
4a 1	The Consumer does not turn off some appliances	• Internal / Customer Process	
4a 2	After a predetermined time the Smart Metering System cuts supply and logs the event	• Message intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
4a 3	The Smart Metering System sends a message to the In Home Display stating supply has been interrupted due to excessive power use	• Data sent to wrong IHD • Data intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
4a 4	The Consumer notes the message and acknowledges it at the In Home Display	• The consumer ignores the message • Message sent to the wrong consumer • Message intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
4a 5	The Consumer turns off some appliances	• Internal / Customer Process	
4a 6	The Consumer restarts supply with an action at the meter (such as	• Internal / Customer Process	

	pressing a button)		
4a 7	The Smart Metering System restarts supply and logs the event	• Internal process	

Scenario 4 – Direct Control of Appliances or Micro-generation

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Network Operator sends a message to the Smart Metering System of an event requiring greater or less demand or greater or less generation for a known duration	• Incorrect data collected • Incorrectly configured • Message sent to wrong recipient • Message intercepted by others • Message sent by unauthorised party	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Data transfer rules required
2	The Smart Metering System validates the message	• Incorrect configuration of validation rules • Smart Metering System rejects / doesn't receive the data	• Defined and robust rules must be specified in the early design of systems • Data transfer rules required
3	The Smart Metering System acknowledges to the Network Operator that the event has been received	• Data sent to wrong meter • Data intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
4	The Smart Metering System forwards the message to the Energy Management System which co-ordinates the change to demand event	• Data sent to wrong system • Data intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
5	The Energy Management System recognises the end of the change to demand event and allows consumption or generation to return to unfettered use.	• Incorrect configuration	• Defined and robust rules must be specified in the early design of systems • Data transfer rules required

3.4.4 10 - Perform System Balancing

Scenario 1 – Operation of Time of Use Tariff

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Smart Metering System accumulates readings for registers according to the Time of Use tariff	• Unauthorised access to customer data • Customer has not given consent to data to be taken • Incorrectly configured • Storage limits exceeded • Incorrect data collected	• Develop robust consenting process presumably run by Suppliers as they have customer relationship • Clear and robust configuration rules required • DNO's and Smart Metering System need to have secure and robust management of data • Appropriate measured data storage requirements at the DNO's and Smart Metering System
2	The Smart Metering System periodically (according to the schedule) provides readings for the registers associated with the Time of Use tariff to the Network Operator	• Incorrect data collected • Incorrectly configured schedule • Incorrect configuration for time period	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Data transfer rules required
3	The Network Operator receives the readings and loads them into their system	• Incorrect / non compliant data is retrieved • Data no longer available / deleted / overwritten • Data sent from unauthorised party • Received data isn't stored securely • Data loaded into incorrect system • Data corrupted in transit	• Develop robust access rules • Develop robust validation rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required • DNO's and Smart Metering System need to have secure and robust management of data

Scenario 2 – Operation of Real Time Pricing

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Network Operator periodically sends prices to the Smart Metering System	• Incorrect data collected • Incorrectly configured schedule • Data sent to wrong meter/group of meters • Data sent by unauthorised party	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Data transfer rules required
2	The Smart Metering System validates the prices and forwards them to the In Home Display (or other display device)	• Incorrect configuration of validation rules • IHD rejects / doesn't receive the data	• Defined and robust rules must be specified in the early design of systems • Data transfer rules required
3	The Consumer uses the information on their In Home Display to influence their consumption behaviour either directly or via an Energy Management System	• Data sent to wrong IHD	• Develop robust authentication rules • Develop robust authorisation and encryption rules
4	The Smart Metering System periodically sends consumption readings to the Network Operator	• Unauthorised access to customer data • Customer has not given consent to data to be taken • Incorrect data sent • Data sent to the wrong recipient	• Develop robust consenting process presumably run by Suppliers as they have customer relationship • Develop robust authentication rules • Develop robust authorisation and encryption rules • Data transfer rules required
5	The Network Operator receives the consumption readings and loads them into their system	• Incorrect / non compliant data is retrieved • Data no longer available / deleted / overwritten • Data sent by unauthorised party • Data corrupted in transit	• Develop robust access rules • Develop robust validation • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required

Scenario 3 – Power Sharing by Maximum Power Thresholds

Security Control Points			
Control Point No	**Activity**	**Issues / Risks**	**Recommendations**
Basic Flow			
1	The Smart Metering System recognises that power consumption has reached the threshold configured in the meter	• Incorrect configuration at the meter • Meter configured by unauthorised party	• Defined and robust rules must be specified in the early design of systems • Access to configure the meter must be via robust authentication and authorisation processes
2	The Smart Metering System sends a message to the In Home Display advising of excessive power use and warning the supply will be interrupted unless consumption is reduced	• Incorrect configuration of validation rules • IHD rejects / doesn't receive the data • Message intercepted / blocked by unauthorised party	• Defined and robust rules must be specified in the early design of systems • Data transfer rules required
3	The In Home display receives and displays the message	• Data sent to wrong IHD • Data intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
4	The Consumer notes the message and turns off some appliances	• The consumer ignores the message • Message sent to the wrong consumer • Message intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
5	The Smart Metering System recognises that power consumption has dropped below the threshold configured in the meter	• Unauthorised access to customer data • Customer has not given consent to data to be taken • Data obtained for the wrong customer • Data intercepted by others	• Develop robust consenting process presumably run by Suppliers as they have customer relationship • Develop robust authentication rules • Develop robust authorisation and encryption rules
6	The Smart Metering System sends a command to the In Home Display to replace the previous message with one stating consumption	• Data sent to wrong IHD • Data intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules

	has reduced below threshold		
7	The Consumer notes the message and acknowledges it at the In Home Display	• The consumer ignores the message • Message sent to the wrong consumer • Message intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
Alternative Flows			
	At Basic Flow step 4:		
4a 1	The Consumer does not turn off some appliances	• Internal / Customer Process	
4a 2	After a predetermined time the Smart Metering System cuts supply and logs the event	• Message intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
4a 3	The Smart Metering System sends a message to the In Home Display stating supply has been interrupted due to excessive power use	• Data sent to wrong IHD • Data intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
4a 4	The Consumer notes the message and acknowledges it at the In Home Display	• The consumer ignores the message • Message sent to the wrong consumer • Message intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
4a 5	The Consumer turns off some appliances	• Internal / Customer Process	
4a 6	The Consumer restarts supply with an action at the meter (such as pressing a button)	• Internal / Customer Process	
4a 7	The Smart Metering System restarts supply and logs the event	• Internal process	

Scenario 4 – Direct Control of Appliance or Micro-generation

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Network Operator sends a message to the Smart Metering System of an event requiring greater or less demand or greater or less generation for a known duration	• Incorrect data collected • Incorrectly configured • Message sent to wrong recipient • Message intercepted by others • Message sent by unauthorised party	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Data transfer rules required
2	The Smart Metering System validates the message	• Incorrect configuration of validation rules • Smart Metering System rejects / doesn't receive the data	• Defined and robust rules must be specified in the early design of systems • Data transfer rules required
3	The Smart Metering System acknowledges to the Network Operator that the event has been received	• Data sent to wrong meter • Data intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
4	The Smart Metering System forwards the message to the Energy Management System which co-ordinates the change to demand event	• Data sent to wrong system • Data intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
5	The Energy Management System recognises the end of the change to demand event and allows consumption or generation to return to unfettered use.	• Incorrect configuration	• Defined and robust rules must be specified in the early design of systems • Data transfer rules required

3.4.5 11 - Check Effectiveness of Active Network Management / System Balancing Measures

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Smart Metering System measures power flow and voltage data	• Unauthorised access to customer data • Customer has not given consent for data to be taken • Incorrect configuration for time period	• Develop robust authentication and authorisation process • Develop robust consenting process presumably run by Suppliers as they have customer relationship • Develop robust access and use rules • Access to data must be encrypted • Data needs to be secure and be confidential • DNO's and Smart Metering System need to have secure and robust management of data
2	The Smart Metering System sends the data to the Network Operator	• Data sent to the wrong recipient • Data intercepted by unauthorised recipient	• Develop robust authentication rules • Develop robust authorisation and encryption rules
3	The Network Operator receives the data and loads it into its system to analyse the effectiveness of load management mechanisms.	• Incorrect / non compliant data is retrieved • Data no longer available / deleted / overwritten • Data corrupted in transit • Data sent by unauthorised party	• Develop robust access rules • Develop robust validation rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required
Alternative Flows			
	At Basic Flow step 2:		
2a 1	The Smart Metering System fails to send the message	• No data stored • Incorrect configuration	• Secure data storage arrangements required • Develop robust configuration rules
2a 2	The Network Operator's systems identify the missing data, the Network Operator, investigates the cause of the	• Wrong meter re-configured	• Data transfer rules required • DNO's and Smart Metering System need to have secure and robust management of data

	failure and may reconfigure the meter		
2a 3	The flow returns to step 1.	• See Step 1	

3.5 Actively Manage Network – Planned & Unplanned Outages

3.5.1 12 – Notify Customer of Planned Outage

Scenario 1 – Consumer notification of planned / emergency outage

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Distribution Network Operator sends an instruction to the Smart Metering System to display notification of planned / emergency outage message for the Consumer	• Data sent to the wrong recipient • Data intercepted by unauthorised recipient • Data sent by unauthorised party	• Develop robust authentication rules • Develop robust authorisation and encryption rules
2	The Smart Metering System validates the request	• Incorrect configuration of validation rules • Smart Metering System rejects / doesn't receive the data	• Defined and robust rules must be specified in the early design of systems • Data transfer rules required
3	The Smart Metering System forwards the message to an In Home Display (or alternative display device)	• Data sent to wrong IHD • Data intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
4	The message is displayed until the Consumer acknowledges it, or it expires	• The consumer ignores the message • Message sent to the wrong consumer • Message intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
5	The Smart Metering System sends a delivery receipt and message displayed	• Data sent to wrong recipient • Data intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules

	message to the Distribution Network Operator		
Alternative Flows			
	At Basic Flow step 2		
2a 1	The Smart Metering System deems the request invalid	• Incorrect data sent / received • Incorrect validation rules	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and confidential • Data transfer rules required
2a 2	The Smart Metering System sends notification to the Distribution Network Operator detailing error type along with date/time stamp	• Notification not sent	• Data transfer rules required with system 'handshakes'
2a 3	The Distribution Network Operator takes the required steps to resolve the error	• Unsure how to correct data • Insufficient information sent to resolve the error i.e. error unclear	• Data transfer rules required
2a 4	Once the error is resolved back to Basic Flow step 1	• See Step 1	
Alternative Flows			
	At Basic Flow step 5		
5a 1	The Distribution Network Operator does not receive the delivery receipt message from the Smart Metering System	• Incorrect / non compliant data being sent • Unable to process data • No data received for purposes • Data corrupted in transit	• Data transfer rules required • Develop robust access rules
5a 2	The Distribution Network Operator is aware that a failure has occurred	• Internal process	
5a 3	The Distribution Network Operator arranges for a card notifying of the planned outage to be	• Internal process	

	delivered to the Consumer's address		

Scenario 2 – Consumer Notified that Outage is Over

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Distribution Network Operator sends an instruction to the Smart Metering System to display notification that the planned / emergency outage is over message for the Consumer. This could include a reminder to reset clocks / check trips, etc.	• Data sent to the wrong recipient • Data intercepted by unauthorised recipient • Data sent by unauthorised party	• Develop robust authentication rules • Develop robust authorisation and encryption rules
2	The Smart Metering System validates the request	• Incorrect configuration of validation rules • Smart Metering System rejects / doesn't receive the data	• Defined and robust rules must be specified in the early design of systems • Data transfer rules required
3	The Smart Metering System forwards the message to an In Home Display (or alternative display device)	• Data sent to wrong IHD • Data intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
4	The message is displayed until the Consumer acknowledges it, or it expires	• The consumer ignores the message • Message sent to the wrong consumer • Message intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules
5	The Smart Metering System sends a delivery receipt and message displayed message to the Distribution Network	• Data sent to wrong recipient • Data intercepted by others	• Develop robust authentication rules • Develop robust authorisation and encryption rules

	Operator		
Alternative Flows			
	At Basic Flow step 2		
2a 1	The Smart Metering System deems the request invalid	• Incorrect data sent / received • Incorrect validation rules	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required
2a 2	The Smart Metering System sends notification to the Distribution Network Operator detailing error type along with date/time stamp	• Notification not sent	• Data transfer rules required with system 'handshakes'
2a 3	The Distribution Network Operator takes the required steps to resolve the error	• Unsure how to correct data • Insufficient information sent to resolve the error i.e. error unclear	• Data transfer rules required
2a 4	Once the error is resolved back to Basic Flow step 1	• See Step 1	
Alternative Flows			
	At Basic Flow step 5		
5a 1	The Distribution Network Operator does not receive the delivery receipt message from the Smart Metering System	• Incorrect / non compliant data being sent • Unable to process data • No data received for purposes • Data corrupted in transit	• Data transfer rules required • Develop robust access rules
5a 2	The Distribution Network Operator is aware that a failure has occurred	• Internal process	
5a 3	The Distribution Network Operator arranges for an alternative contact method to be used to notify the Consumer that the planned /	• Internal process	

	emergency outage is over		

3.5.2 13 - Query Meter Energisation Status to Determine Outage Source and Location

Scenario 1 - False Outage Report

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	Consumer telephones Distribution Network Operator informing them that they are experiencing a power outage	• Internal process	
2	The Distribution Network Operator identifies the relevant meter(s) and sends an energisation status request message to the Smart Metering System	• Incorrect / non compliant data being sent • Unable to process data • No data received for purposes	• Data transfer rules required • Develop robust access rules
3	The Smart Metering System receives and validates the message	• Incorrect configuration of validation rules • Smart Metering System rejects / doesn't receive the data	• Defined and robust rules must be specified in the early design of systems • Data transfer rules required
4	The Smart Metering System checks the power supply from the network and finds it is supplied	• Internal process	
5	The Smart Metering System sends a date and time stamped network power available message to the Distribution Network Operator	• Incorrect / non compliant data being sent • Data corrupted in transit • Data intercepted by unauthorised party • Data sent to incorrect recipient	• Data transfer rules required • Develop robust validation process
6	The Distribution Network Operator requests the status	• Incorrect / non compliant data	• Data transfer rules required • Develop robust access rules

	of the contact / or switch that may be used under a Supplier's contract to control supply	being sent	
7	The Smart Metering System reports the status of the switch	• Incorrectly reported information	• Data transfer rules required • Develop robust access rules • Develop robust authentication rules • Develop robust authorisation and encryption rules
8	The Distribution Network Operator receives the message and explains to the customer the nature of the supply problem – the network operator may offer advice that the customer would need to contact the Supplier or an electrical contractor.	• Internal process	
Alternative Flows			
	At Basic Flow step 3		
3a 1	The Smart Metering System rejects the message as invalid	• Incorrect data sent / received • Incorrect validation rules	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required
3a 2	The Smart Metering System sends notification to the Distribution Network Operator detailing error type along with date/time stamp	• Notification not sent	• Data transfer rules required with system 'handshakes'
Alternative Flows			
	At Basic Flow step 5		
5a 1	The Distribution Network Operator does not receive the message	• Incorrect / non compliant data being sent • Unable to process data • No data received for purpose	• Data transfer rules required • Develop robust access rules
5a 2	The Distribution Network Operator takes the lack of response to indicate a network outage or a	• Internal process	

	communications outage and initiates their restoration process or investigates the integrity of the communications system.		

Scenario 2 – Confirmed Network Outage

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Distribution Network Operator knows / identifies which meter(s) are to be queried	• Internal process	
2	The Distribution Network Operator sends an energisation status query message to the Smart Metering System	• Incorrect / non compliant data being sent • Data sent to the wrong Metering System • Data intercepted by others	• Data transfer rules required • Develop robust authentication rules • Develop robust authorisation and encryption rules
3	The Smart Metering System is not receiving power from the network so the communications system is not in operation	• Internal process	
4	The Distribution Network Operator receives no confirmation that the message has been received by the Smart Metering System	• Incorrect / non compliant data being sent • Unable to process data • No data received for purposes	• Data transfer rules required • Develop robust access rules
5	After a defined period of time (based on the normal time a response is received in scenario 1 above) the Distribution Network Operator deduces that the Smart Metering System is either experiencing a network outage or a communications failure	• Internal process	

6	The Distribution Network Operator queries the energisation status of further Smart Metering Systems to determine the extent of the network outages/communications failures	• Incorrect / non compliant data being sent • Data sent to the wrong Metering System • Data intercepted by others	• Data transfer rules required • Develop robust authentication rules • Develop robust authorisation and encryption rules
7	The Distribution Network Operator instigates their network fault management procedures	• Internal process	

3.5.3 14 - Send Alarm to DNO during Network Outage

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Smart Metering System detects a loss of power from the network and sends a date and time stamped outage alarm to the Distribution Network Operator	• Data sent to the wrong recipient • Data intercepted by unauthorised recipient • Incorrect detection	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Data transfer rules required
2	The Distribution Network Operator receives the message	• DNO rejects / doesn't receive the data • Data corrupted in transit	• Defined and robust rules must be specified in the early design of systems • Data transfer rules required • Develop robust authentication rules • Develop robust validation rules
3	The flow is repeated by other meters in the outage affected area	• Data sent to the wrong recipient • Data intercepted by unauthorised recipient	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Data transfer rules required
Alternative Flows			
	At Basic Flow step 1		
1a 1	A Smart Metering System is unable to	• Data sent to the wrong recipient	• Develop robust authentication rules

	send the outage alarm message, e.g. due to insufficient battery power remaining – however it is assumed that at least one Smart Metering System in the affected area will succeed in sending the outage message, or a Consumer will ring the Distribution Network Operator to notify of the outage	• Data intercepted by unauthorised recipient • Incorrect detection	• Develop robust authorisation and encryption rules • Data transfer rules required
1a 2	The flow is continued by other meters in the outage affected area	• Data sent to the wrong recipient • Data intercepted by unauthorised recipient	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Data transfer rules required
Alternative Flows			
	At alternative flow step 1a1		
1a 1a	Distribution Network Operator receives neither an outage alarm nor a telephone call from a Consumer informing them of an outage	• Internal process	
1a 1b	Through monitoring their network Distribution Network Operator detects conditions suggesting an outage has occurred	• Internal process	
1a 1c	Go to Use Case 13		

3.5.4 15 – Verify Restoration of Supplies after Outage

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Smart Metering System detects restoration of power	• Internal process	

	supplied from the network		
2	The Smart Metering System sends a date and time stamped power restored message to the Distribution Network Operator	• Data sent to the wrong recipient • Data intercepted by unauthorised recipient	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Data transfer rules required
3	The Distribution Network Operator receives the message	• DNO rejects / doesn't receive the data • Data corrupted in transit	• Defined and robust rules must be specified in the early design of systems • Data transfer rules required • Develop robust authentication rules
Alternative Flows			
	At Basic Flow step 1		
1a 1	Although power has been restored to the premises due to an internal fault the Smart Metering System fails to detect this	• Internal process	
1a 2	The Distribution Network Operator will receive power restored messages from Smart Metering Systems connected to the part of the network affected by the fault	• Data sent to the wrong recipient • Data intercepted by unauthorised recipient	• Develop robust authentication rules • Develop robust authorisation and encryption rules • Data transfer rules required
1a 3	The Distribution Network Operator will send an operative to the site to determine whether power has been restored or whether the meter is faulty. The Operative will deal with any network fault if the smart metering system is not faulty.	• On visit Engineer finds that meter is ok	
1a 4	On identifying that the Smart Metering System is faulty the Distribution Network Operator will initiate their faulty meter	• Internal Process	

	detected procedure		
Alternative Flows			
	At Basic Flow step 3		
3a 1	The Distribution Network Operator does not receive the message	• Incorrect / non compliant data being sent • Unable to process data • No data received for purposes	• Data transfer rules required • Develop robust access rules
3a 2	The Distribution Network Operator is aware a failure has occurred	• Ensure that any customer data is confidential	• Data needs to be secure and be confidential
3a 3	Go to alternative flow step 1a3 above	• See step 1a 3	

3.5.5 16 – Regulatory Reporting of Outages

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Distribution Network Operator sends a message to the Smart Metering System requesting stored outage information	• Unauthorised access to customer data • Customer has not given consent for data to be taken • Incorrect data received • Data loaded into incorrect system • Data isn’t stored securely	• Develop robust authentication and authorisation process • Develop robust consenting process presumably run by Suppliers as they have customer relationship • Develop robust access and use rules • Access to data must be encrypted • Data needs to be secure and be confidential • DNO’s and Smart Metering System need to have secure and robust management of data
2	The Smart Metering System receives the message and validates it	• Incorrect / non compliant data being requested • Data no longer available / deleted / overwritten • Unauthorised access to customer data • Validation / authentication failure • Customer has not given	• Develop robust access rules • Develop robust authentication and authorisation process • Data transfer rules required • Develop robust consenting process presumably run by Suppliers as they have customer relationship

		consent for data to be taken	
3	The Smart Metering System extracts the required information from internal storage, packages it, and sends it to the Distribution Network Operator	• Incorrect configuration for time period • Request sent to the wrong recipient • Request intercepted by unauthorised recipient • Request sent to wrong group of meters	• Develop robust authentication rules • Develop robust authorisation and encryption rules
4	The Distribution Network Operator receives the information and loads it into its systems	• Incorrect / non compliant data is retrieved • Data no longer available / deleted / overwritten • Data corrupted in transit	• Develop robust access rules • Develop robust validation process • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required
5	The Distribution Network Operator analyses the information and compares it to its own outage records to build a complete picture of outage incidents and periods of supply interruption	• Internal Process	
Alternative Flows			
	At Basic Flow step 2		
2a 1	The Smart Metering System rejects the message as invalid	• Incorrect data sent / received • Incorrect validation rules	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required
2a 2	The Smart Metering System sends notification to the Distribution Network Operator detailing error type along with date/time stamp	• Notification not sent	• Data transfer rules required with system 'handshakes'
2a 3	The Distribution Network Operator receives the message and takes the required steps to resolve the error	• Unsure how to correct data • Insufficient information sent to resolve the error i.e. error unclear	• Data transfer rules required

2a 4	Once error is resolved go back to Basic Flow step 1	• See step 1	
Alternative Flows			
	At Basic Flow step 3		
3a 1	The Smart Metering System does not have any of the requested information stored	• Incorrect / non compliant data is retrieved • Data no longer available / deleted / overwritten	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and confidential • Data transfer rules required
3a 2	The Smart Metering System sends a message to the Distribution Network Operator stating “no records found” (or similar)	• Incorrect / non compliant data is retrieved	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required
3a3	Distribution Network Operator receives the message and loads it into its systems	• Data from unauthorised party • Data corrupted in transit	• Develop robust authentication and authorisation processes • Develop robust validation rules
3a 4	End of flow		
Alternative Flows			
	At Basic Flow step 4		
4a 1	The Distribution Network Operator does not receive the information from the Smart Metering System	• Incorrect / non compliant data being sent • Unable to process data • No data received for purposes	• Data transfer rules required • Develop robust access rules
4a 2	The Distribution Network Operator performs a communication test with the Smart Metering System	• Internal Process	
4a 3	The communication test fails indicating a problem with the Smart Metering System	• Internal Process	
4a 4	The Distribution Network Operator informs the Smart Metering System owner of the fault with the Smart Metering	• Unauthorised access to customer data • Customer has not given consent to data to be taken	• Develop robust authentication and authorisation process • Develop robust consenting process presumably run by

	System	- Incorrect data received - Data loaded into incorrect system - Received data isn't stored securely	Suppliers as they have customer relationship - Develop robust access and use rules - Access to data must be encrypted - Data needs to be secure and be confidential - DNO's and Smart Metering System need to have secure and robust management of data
4a 5	End of flow		

3.5.6 17 –Restore and Maintain Supply during Outages

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	Power is restored to the Smart Metering System	- Internal Process	
2	The Smart Metering System sends a date and time stamped power restored message to the Distribution Network Operator	- Incorrect configuration for time period - Message sent to the wrong recipient - Message intercepted by unauthorised recipient	- Develop robust authentication rules - Develop robust authorisation and encryption rules
3	The Distribution Network Operator receives the message and sends a message to the Smart Metering System activating the maximum power consumption threshold	- Unauthorised access to customer data - Customer has not given consent to data to be taken - Request sent to the wrong recipient - Request intercepted by unauthorised recipient - Request sent to wrong group of meters	- Develop robust consenting process presumably run by Suppliers as they have customer relationship - Develop robust authentication rules - Develop robust authorisation and encryption rules
4	The Smart Metering System receives the message and validates it	- Incorrect validation process - Request sent to the wrong recipient - Request intercepted by unauthorised recipient	- Develop robust authentication rules - Develop robust authorisation and encryption rules
5	The Smart Metering System activates the	- Message sent to the wrong recipient	- Develop robust authentication rules

	maximum power consumption threshold and sends a confirmation response to the Distribution Network Operator	• Message intercepted by unauthorised recipient	• Develop robust authorisation and encryption rules
	Alternative Flow		
	At Basic Flow step 3		
3a 1	The Distribution Network Operator does not receive the power restored message	• No data sent • Unable to process data • Incorrect / non compliant data is received	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required
3a 2	The Distribution Network Operator checks that the Smart Metering System is configured and working correctly, and that communications are working	• Internal Process	
3a 3	The Distribution Network Operator is aware that power has been restored so sends a message to the Smart Metering System activating the maximum power consumption threshold	• Unauthorised access to customer data • Customer has not given consent to data to be taken • Request sent to the wrong recipient • Request intercepted by unauthorised recipient • Request sent to wrong group of meters	• Develop robust consenting process presumably run by Suppliers as they have customer relationship • Develop robust authentication rules • Develop robust authorisation and encryption rules
3a 4	Back to Basic Flow step 4	• See step 4	
	Alternative Flow		
	At Basic Flow step 4:		
4a 1	The Smart Metering System deems the request invalid	• Incorrect data sent / received • Incorrect validation rules	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required
4a 2	The Smart Metering System sends notification to the Distribution Network	• Notification not sent	• Data transfer rules required with system 'handshakes'

	Operator detailing error type along with date/time stamp		
4a 3	The Distribution Network Operator takes the required steps to resolve the error	• Unsure how to correct data • Insufficient information sent to resolve the error i.e. error unclear	• Data transfer rules required
4a 4	Back to Basic Flow step 3	• See step 3	
	Alternative Flow		
	At Basic Flow step 5:		
5a 1	The Distribution Network Operator does not receive the confirmation response	• No data sent • Unable to process data • Incorrect / non compliant data is received	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and confidential • Data transfer rules required
5a 2	The Distribution Network Operator checks that the Smart Metering System is configured and working correctly, and that communications are working	• Internal Process	
5a 3	The Distribution Network Operator sends a message to the Smart Metering System checking whether the maximum power consumption threshold has been activated	• Unauthorised access to customer data • Customer has not given consent to data to be taken • Request sent to the wrong recipient • Request intercepted by unauthorised recipient • Request sent to wrong group of meters	• Develop robust consenting process presumably run by Suppliers as they have customer relationship • Develop robust authentication rules • Develop robust authorisation and encryption rules
5a 4	End of flow		

3.6 Safety

3.6.1 18 – Manage Meter Safety Alarm

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	Interference Responsible Entity changes conditions at the Smart Metering System to render it unsafe and requiring Distribution Network Operator intervention	• Internal / Customer Process	
2	The Smart Metering System detects the change in condition and sends a date and time stamped alarm to the Distribution Network Operator	• Data not sent • Message sent to the wrong recipient • Message intercepted by unauthorised recipient • Message sent to wrong DNO	• Develop robust authentication rules • Develop robust authorisation and encryption rules
3	The Distribution Network Operator receives the alarm and analyses the content	• DNO rejects / doesn't receive the data	• Defined and robust rules must be specified in the early design of systems • Data transfer rules required • Develop robust authentication rules
4	The Distribution Network Operator dispatches a crew to investigate the conditions at the meter	• Internal Process	
5	If the Distribution Network Operator deems the conditions to be dangerous enough they will send a message to the Smart Metering System supply switch to remotely disconnect the meter until an on-site investigation has been undertaken by skilled DNO staff	• Message sent to the wrong recipient • Message intercepted by unauthorised recipient	• Develop robust authentication and authorisation process • Develop robust access and use rules
6	The Smart Metering System receives the	• Incorrect / non compliant data being sent	• Develop robust access rules • Develop robust

	disconnect message and validates it	• Data no longer available / deleted / overwritten • Validation / authentication failure	authentication and authorisation process • Data transfer rules required
7	The Smart Metering System activates the supply switch and sends a date and time stamped confirmation message to the Distribution Network Operator	• Incorrect data received • Data loaded into incorrect system • Received data isn't stored securely	• Develop robust authentication and authorisation process • Develop robust access and use rules • Access to data must be encrypted • Data needs to be secure and confidential • DNO's and Smart Metering System need to have secure and robust management of data
8	The Distribution Network Operator receives the message and updates their system in case an outage query is received	• Incorrect / non compliant data is retrieved	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and confidential • Data transfer rules required
Alternative Flows			
	At Basic Flow step 2		
2a 1	The Smart Metering System fails to detect the change in conditions	• No data sent • Unable to process data • Incorrect / non compliant data is received	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required
2a 2	The Distribution Network Operator is unaware of the change in conditions at the meter	• No Data Action	
2a 3	The change in conditions is detected during the next routine meter inspection	• Internal Process	
2a 4	The Supplier informs the DNO of any DNO required intervention	• Unauthorised access to customer data • Customer has not given consent to data to be taken • Incorrect data received • Data loaded into incorrect system • Received data isn't stored	• Develop robust authentication and authorisation process • Develop robust consenting process presumably run by Suppliers as they have customer relationship • Develop robust access and use rules

		securely	- Access to data must be encrypted - Data needs to be secure and be confidential - DNO's and Smart Metering System need to have secure and robust management of data
2a 5	Flow ends		
Alternative Flows			
	At Basic Flow step 3		
3a 1	The Distribution Network Operator fails to receive the alarm from the Smart Metering System	- No data sent - Unable to process data - Incorrect / non compliant data is received	- Develop robust access rules - Access to data must be encrypted - Data needs to be secure and be confidential - Data transfer rules required
3a 2	Go to alternative flow step 2 above	- See step 2	
Alternative Flows			
	At Basic Flow step 6		
6a 1	The Smart Metering System rejects the message as invalid	- Incorrect data sent / received - Incorrect validation rules	- Develop robust access rules - Access to data must be encrypted - Data needs to be secure and confidential - Data transfer rules required
6a 2	The Smart Metering System sends notification to the Distribution Network Operator detailing error type along with date/time stamp	- Notification not sent	- Data transfer rules required with system 'handshakes'
6a 3	The Distribution Network Operator receives the message and takes the required steps to resolve the error	- Unsure how to correct data - Insufficient information sent to resolve the error i.e. error unclear	- Data transfer rules required
6a 4	Once error is resolved go back to Basic Flow step 5	- See step 5	
Alternative Flows			
	At Basic Flow step 8		
8a 1	The Distribution Network Operator does not	- No data sent - Unable to process data	- Develop robust access rules - Access to data must be

	receive confirmation of the supply switch activating to cut-off supply	- Incorrect / non compliant data is received	encrypted - Data needs to be secure and be confidential - Data transfer rules required
8a 2	The Distribution Network Operator informs the dispatched crew that the Smart Metering System may not have been disconnected so to test on arrival	- Internal Process	
8a 3	Flow ends		

3.6.2 19 – Manage Extreme Voltage at Meter

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Smart Metering System detects a voltage level outside its configured tolerance levels	- Internal Process	
2	The Smart Metering System sends a date and time stamped extreme voltage level alarm detailing the voltage level detected to the Distribution Network Operator	- Data not sent - Message sent to the wrong recipient - Message intercepted by unauthorised recipient - Message sent to wrong DNO	- Develop robust authentication rules - Develop robust authorisation and encryption rules
3	(Optionally) the Smart Metering System auto-disconnects itself from the network supply of electricity sending confirmation of disconnection to the Distribution Network Operator	- Data not sent - Data sent to the wrong recipient - Data intercepted by unauthorised recipient - Data sent to wrong DNO	- Develop robust authentication rules - Develop robust authorisation and encryption rules
4	The Distribution Network Operator receives the extreme voltage level	- DNO rejects / doesn't receive the data	- Defined and robust rules must be specified in the early design of systems - Data transfer rules required

	alarm and uses the information to determine the corrective action to be taken to resolve the extreme voltage level		• Develop robust authentication rules
5	The Distribution Network Operator receives the confirmation of disconnection due to extreme voltage detected and loads it into its systems to use for any outage queries	• Internal Process	
Alternative Flows			
	At Basic Flow step 1		
1a 1	The Smart Metering System fails to detect the extreme voltage level	• No data sent • Unable to process data • Incorrect / non compliant data is received	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and confidential • Data transfer rules required
1a 2	The extreme voltage level impairs equipment within/attached to the premises	• Internal Process	
1a 3	The Consumer contacts the Distribution Network Operator to complain	• Internal Process	
1a 4	The Distribution Network Operator investigates the cause of the extreme voltage and compensates the Consumer (where appropriate)	• Internal Process	
1a 5	End of flow		
	Alternative Flow		
	At Basic Flow step 2		
2a1	The Smart Metering System fails to send the extreme voltage alarm	• Unable to process data • Incorrect / non compliant data is sent	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and be confidential

			• Data transfer rules required
2a2	The distribution Network Operator receives the confirmation of auto-disconnection due to extreme voltage but no alarm	• DNO rejects / doesn't receive the data	• Defined and robust rules must be specified in the early design of systems • Data transfer rules required • Develop robust authentication rules
2a3	The Distribution Network Operator dispatches a crew to investigate the conditions on site and determine the corrective action required	• Internal Process	
2a4	End of flow		
	Alternative Flow		
	At Basic Flow step 3		
3a 1	The Smart Metering System fails to auto-disconnect	• No data sent • Unable to process data • Incorrect / non compliant data is received	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and confidential • Data transfer rules required
3a 2	The Smart Metering System sends a date and time stamped extreme voltage level alarm detailing the voltage level detected to the Distribution Network Operator	• Data not sent • Data sent to the wrong recipient • Data intercepted by unauthorised recipient • Data sent to wrong DNO	• Develop robust authentication rules • Develop robust authorisation and encryption rules
3a 3	The Distribution Network Operator receives the extreme voltage alarm but no confirmation of auto-disconnection	• DNO rejects / doesn't receive the data	• Defined and robust rules must be specified in the early design of systems • Data transfer rules required • Develop robust authentication rules
3a 4	The Distribution Network Operator uses the information from the voltage alarm to determine the corrective action required to resolve the extreme voltage level	• Internal Process	
3a 5	End of flow		

Alternative Flow			
	At Basic Flow step 2 & 3		
2b 1 or 3b 1	The Smart Metering System fails to auto-disconnect or send the extreme voltage alarm	• Configuration error	
2b 2 or 3b 2	Go to step 2a1 of the first alternative flow	• See step 2a 1	

3.7 Support Network Activities

3.7.1 20 – Configure Smart Metering System

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Distribution Network Operator sends a message to configure the Smart Metering System to perform (or cease performing) a set functionality according to supplied parameters	• Unauthorised access to customer data • Customer has not given consent to data to be taken • Request sent to the wrong recipient • Request intercepted by unauthorised recipient • Request sent to wrong group of meters	• Develop robust consenting process presumably run by Suppliers as they have customer relationship • Develop robust authentication rules • Develop robust authorisation and encryption rules
2	The Smart Metering System receives the message and validates it	• Incorrect / non compliant data being requested • Data no longer available / deleted / overwritten • Unauthorised access to customer data • Validation / authentication failure • Customer has not given consent to data to be taken	• Develop robust access rules • Develop robust authentication and authorisation process • Data transfer rules required • Develop robust consenting process presumably run by Suppliers as they have customer relationship
3	The Smart Metering System activates the requested functionality and sends a date and time stamped confirmation response to the Distribution Network	• Data intercepted by unauthorised recipient • Data sent to incorrect party	• Develop robust authentication rules • Develop robust authorisation and encryption rules

	Operator		
4	The Distribution Network Operator receives the confirmation response	• Incorrect data received • Data loaded into incorrect system • Received data isn't stored securely • Data corrupted in transit	• Develop robust access and use rules • Access to data must be encrypted • Data needs to be secure and confidential • DNO's and Smart Metering System need to have secure and robust management of data
	Alternative Flow		
	At Basic Flow step 3		
3a 1	The Smart Metering System rejects the message as invalid	• Incorrect data sent / received • Incorrect validation rules	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and confidential • Data transfer rules required
3a 2	The Smart Metering System sends a date and time stamped notification to the Distribution Network Operator detailing the error type	• Notification not sent	• Data transfer rules required with system 'handshakes'
3a 3	The Distribution Network Operator receives the message and takes the required steps to resolve the error	• Unsure how to correct data • Insufficient information sent to resolve the error i.e. error unclear	• Data transfer rules required
3a 4	Once error is resolved go back to Basic Flow step 1	• See step 1	
	Alternative Flow		
	At Basic Flow step 4		
4a 1	The Distribution Network Operator does not receive a confirmation response	• No data sent • Unable to process data • Incorrect / non compliant data is received	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and confidential • Data transfer rules required
4a 2	The Distribution Network Operator checks the current configuration of the Smart Metering	• Internal Process	

	System and takes steps to ensure that it is working properly		
4a 3	Back to Basic Flow step 1	- See step 1	

Appendix B - Gas Use Case Security Control Points

1. Approach

Based on the final list of Use Cases it is intended that the Basic Steps that are shown for each Use Case will be reviewed to identify for each step any Security & Privacy Issues / Risks and identify any appropriate recommendations to address them.

2. Security & Privacy Review

The security control points below majors on the security issues, but also covers key privacy areas related to consumer data that might be an issue and need to be dealt with.

3.1 01 - Gather Information for Planning

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Smart Metering System sends the recorded gas demand data to the Gas Distribution Network Operator	• Unauthorised access to customer data • Customer has not given consent for data to be taken • Incorrect data received • Data loaded into incorrect system • Received data isn't stored securely	• Develop robust authentication and authorisation process • Develop robust consenting process presumably run by Suppliers as they have customer relationship • Develop robust access and use rules • Access to data must be encrypted • Data needs to be secure and confidential • DNO's and Smart Metering System need to have secure and robust management of data
2	The Gas Distribution Network Operator receives the data and loads it into their system	• Incorrect / non compliant data is retrieved • Data no longer available / deleted / overwritten • Data corrupted in transit	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required • Develop robust validation rules
Alternative Flows			
	At Basic Flow step 2		
2a 1	The Gas Distribution Network Operator does not receive the correct data or it is	• Data sent to wrong recipient • Data intercepted by unauthorised recipient	• Develop robust authentication rules • Develop robust authorisation and encryption rules

	corrupt.	- Data configured incorrectly - Data corrupted in transit	- Develop robust access and use rules - Data transfer rules required - Develop robust validation rules
2a 2	Back to Basic Flow step 1	- See step 1	

3.2 02 - Configure Gas Smart Metering System

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Gas Distribution Network Operator sends a message to configure the Smart Metering System to perform (or cease performing) a set functionality according to supplied parameters	- Unauthorised access to customer data - Customer has not given consent for data to be taken - Incorrect data sent - Data loaded into incorrect metering system - Received data isn't stored securely - Message sent from unauthorised party	- Develop robust authentication and authorisation process - Develop robust consenting process presumably run by Suppliers as they have customer relationship - Develop robust access and use rules - Access to data must be encrypted - Data needs to be secure and be confidential - DNO's and Smart Metering System need to have secure and robust management of data
2	The Smart Metering System receives the message and validates it	- Incorrect / non compliant data is retrieved	- Develop robust access rules - Access to data must be encrypted - Data needs to be secure and confidential - Data transfer rules required
3	The Smart Metering System activates/updates the requested functionality and sends a date and time stamped confirmation response to the Gas Distribution Network Operator	- Incorrect / non compliant data is sent - Data intercepted by others	- Develop robust access rules - Access to data must be encrypted - Data needs to be secure and confidential - Data transfer rules required

4	The Gas Distribution Network Operator receives the confirmation response	• Incorrect / non compliant data is received • Data intercepted by others	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and confidential • Data transfer rules required
Alternative Flows			
	At Basic Flow step 3		
3a 1	The Smart Metering System rejects the message as invalid	• Incorrect data sent / received • Incorrect validation rules	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and confidential • Data transfer rules required
3a 2	The Smart Metering System sends a date and time stamped notification to the Distribution Network Operator detailing the error type	• Data not sent • Unsure how to correct data • Insufficient information sent to resolve the error i.e. error unclear	• Data transfer rules required with system 'handshakes'
3a 3	The Distribution Network Operator receives the message and takes the required steps to resolve the error	• Data not received • Unsure how to correct data • Insufficient information sent to resolve the error i.e. error unclear	• Data transfer rules required with system 'handshakes'
3a 4	Once error is resolved go back to Basic Flow step 1	• See step 1	
Alternative Flows			
	At Basic Flow step 4		
4a 1	The Distribution Network Operator does not receive a confirmation response	• Incorrect / non compliant data being sent • Unable to process data • No data received for DNO purposes	• Data transfer rules required • Develop robust access rules
4a 2	The Distribution Network Operator checks the current configuration of the Smart Metering System and takes steps to ensure that it is working properly	• Internal Process	
4a 3	Back to Basic Flow	• See step 1	

	step 1		

3.3 03 – Disable Supply of Gas by GDN

Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Gas Distribution Network sends a message to the Smart Metering System to operate the valve	• Message sent to wrong metering system • Message sent from unauthorised party • Message intercepted by unauthorised party	• Develop robust authentication and authorisation process • Develop robust access and use rules
2	The Smart Metering System receives the message and validates it	• Incorrect / non compliant data is retrieved	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and confidential • Data transfer rules required
3	The Smart Metering System activates the gas valve and sends a confirmation response message to the Gas Distribution Network Operator	• Incorrect / non compliant data is sent • Data intercepted by others	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and confidential • Data transfer rules required
4	The Gas Distribution Network Operator receives the confirmation response that the gas valve has operated	• Incorrect / non compliant data is received • Data intercepted by others	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and confidential • Data transfer rules required
5	On completion of works, a Competent Person would open gas valve on site following necessary safety checks and soundness testing.	• Internal Process	
Alternative Flows			
	At Basic Flow step 2		
2a 1	The Smart Metering System rejects the	• Incorrect data sent / received	• Develop robust access rules • Access to data must be

	message as invalid	• Incorrect validation rules	encrypted • Data needs to be secure and confidential • Data transfer rules required
2a 2	The Smart Metering System sends notification to the Gas Distribution Network Operator detailing the error type along with a date/time stamp	• Notification not sent • Unsure how to correct data • Insufficient information sent to resolve the error i.e. error unclear	• Data transfer rules required with system 'handshakes'
2a 3	The Gas Distribution Network Operator resolves the issue and goes back to Basic Flow step 1	• See step 1	
Alternative Flows			
	At Basic Flow step 4		
4a 1	The Gas Distribution Network Operator does not receive the confirmation response	• Incorrect / non compliant data being sent • Unable to process data • No data received for DNO purposes	• Data transfer rules required • Develop robust access rules
4a 2	The Gas Distribution Network Operator ensures that the Smart Metering System is configured and working correctly	• Internal Process	
4a 3	The Gas Distribution Network Operator remotely checks the status of the gas valve	• Metering system incorrectly configured • Incorrect data being sent	• Data transfer rules required • Develop robust validation rules
4a 4	Go back to Basic Flow step 4	• See step 4	

3.4 04 - Display Messages from GDN

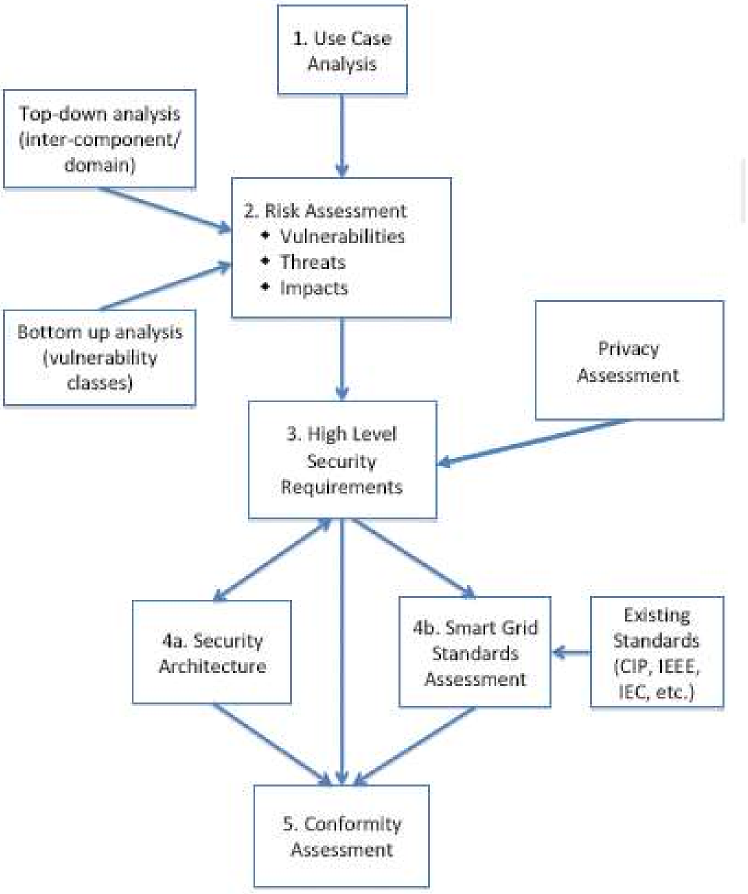
Security Control Points			
Control Point No	Activity	Issues / Risks	Recommendations
Basic Flow			
1	The Gas Distribution Network Operator sends a message to the Smart Metering System	• Unauthorised access to customer data • Customer has not given consent to data to be taken • Incorrect data sent • Data loaded into incorrect metering system • Received data isn't stored securely • Message sent by unauthorised party • Message intercepted by unauthorised party	• Develop robust authentication and authorisation process • Develop robust consenting process presumably run by Suppliers as they have customer relationship • Develop robust access and use rules • Access to data must be encrypted • Data needs to be secure and be confidential • DNO's and Smart Metering System need to have secure and robust management of data
2	The Smart Metering System receives the message, validates it and displays it	• Incorrect / non compliant data is retrieved	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required
3	The Smart Metering System sends a message displayed confirmation to the Gas Distribution Network Operator	• Incorrect / non compliant data is sent • Data intercepted by others	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required
4	The Gas Distribution Network Operator can send updates to the message.	• Unauthorised access to customer data • Customer has not given consent to data to be taken • Incorrect data sent • Data loaded into incorrect metering system • Received data isn't stored securely	• Develop robust authentication and authorisation process • Develop robust consenting process presumably run by Suppliers as they have customer relationship • Develop robust access and use rules • Access to data must be encrypted • Data needs to be secure and be confidential

			• DNO's and Smart Metering System need to have secure and robust management of data
5	The Gas Distribution Network Operator sends a message to update the message, i.e. clear message or send situation resolved message.	• Unauthorised access to customer data • Customer has not given consent to data to be taken • Incorrect data sent • Data loaded into incorrect metering system • Received data isn't stored securely	• Develop robust authentication and authorisation process • Develop robust consenting process presumably run by suppliers as they have customer relationship • Develop robust access and use rules • Access to data must be encrypted • Data needs to be secure and be confidential • DNO's and Smart Metering System need to have secure and robust management of data
Alternative Flows			
	At Basic Flow step 2		
2a 1	The Smart Metering System rejects the message as invalid	• Incorrect data sent / received • Incorrect validation rules	• Develop robust access rules • Access to data must be encrypted • Data needs to be secure and be confidential • Data transfer rules required
2a 2	The Smart Metering System sends notification to the Gas Distribution Network Operator detailing the error type along with a date/time stamp	• Notification not sent • Unsure how to correct data • Insufficient information sent to resolve the error i.e. error unclear	• Data transfer rules required with system 'handshakes'
2a 3	The Gas Distribution Network Operator resolves the issue and goes back to Basic Flow step 1	• See step 1	

Appendix C - U.S. NIST 'Smart Grid Cyber Security Strategy and Requirements'

Figure C.1 below illustrates the tasks that NIST are following as part of the development of a Smart Grid Cyber Security Strategy.

Figure C.1 – Tasks in the Smart Grid Cyber Security Strategy


1. Use Case Analysis
Top-down analysis (inter-component/ domain)
2. Risk Assessment
◆ Vulnerabilities
◆ Threats
◆ Impacts
Bottom up analysis (vulnerability classes)
Privacy Assessment
3. High Level Security Requirements
4a. Security Architecture
4b. Smart Grid Standards Assessment
Existing Standards (CIP, IEEE, IEC, etc.)
5. Conformity Assessment

The tasks shown in Figure C.1 are as follows:

Task 1 – Selection of Use Cases with Cyber Security Considerations: NIST selected Use Cases from several existing sources e.g. IntelliGrid, Electric Power Research Institute (EPRI) and Southern California Edison (SCE) and used these Use Cases to provide a common framework for performing the risk assessment, developing the security architecture and selecting and tailoring the security requirements.

Task 2 – Performance of a risk assessment: This risk assessment involved identifying vulnerabilities, impacts and threats undertaken from a high-level overall functionality perspective. The output of this will be the basis for the selection of security requirements and the identification of security requirements gaps.

The **bottom-up analysis** focused on well understood problems that need to be addressed such as authenticating and authorising users, key management for meters, and intrusion detection. This also considered interdependencies between smart grid domains / systems when considering the impacts of a cyber or physical security incident. An incident in one infrastructure can cascade to failures in other domains / systems.

The **top-down analysis** developed logical interface diagrams for the six functional priority areas that were the focus of the initial draft of this paper (NISTIR 7628) of

- Electric Transportation
- Electric Storage
- Wide area situational awareness
- Demand Response
- Advanced Metering Infrastructure
- Distribution Grid Management

Task 3 – Specification of high level security requirements: NIST made use of standards in existence that were directly relevant to a Smart Grid and information applicable to Control Systems to help develop their cyber security requirements.

Privacy Impact Assessment: because the evolving Smart Grid presents potential privacy risks, a privacy impact assessment was performed. Several general privacy principles were used to assess the Smart Grid and findings and recommendations developed. The results will be used in the identification and tailoring of security requirements.

Task 4a - Development of a security architecture: As specified in Task 2 above, the first phase in this task is to assess and revise the six functional priority areas. This functional architecture identifies logical communication interfaces between actors. This detail will be used in the next phase of work where the smart grid conceptual reference model and this functional architecture will be used in developing a single Smart Grid security architecture. The Smart Grid security architecture will overlay the security requirements on this architecture. The objective is to ensure that cyber security is addressed as a critical cross-cutting requirement of the Smart Grid.

Task 4b – Assessment of Smart Grid Standards: Standards identified as relevant to the Smart Grid will be assessed to determine if the security requirements are addressed. In this process, security requirements gaps will be identified and recommendations will be made on how to address these gaps. Also, conflicting standards and standards with security requirements not consistent with the security requirements included in NISTIR 7628 will be identified with appropriate recommendations made.

Task 5 – Conformity Assessment: The final task is to develop a conformity assessment programme for security requirements. This programme will be coordinated with the activities defined by the testing and certification standing committee of the Smart Grid Interoperability Panel. This task is due to begin in the Spring of 2010.

Appendix D- A Dutch lesson in privacy and security

In 2008 the Dutch government published a law proposal mandating the roll out of smart meters within the Netherlands. Consumer Group initiated analysis indicated that the mandated roll-out contravened Article 8 of the European Convention on Human Rights - "right to respect for private and family life" and that the requirement for all consumers to provide 15 minute readings was not in accordance with the Dutch Data Protection Law. Based on this the Dutch Senate in 2009 voted against the proposed law requiring it to be reworked so that the consumer's privacy formed its foundation.

Article 8 ECHR: Right to Respect for Private and Family Life[2]

1. Everyone has the right to respect for his private and family life, his home and his correspondence
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 8 is a qualified right which means that an interference with the right can be justified in certain circumstances. The circumstances are given in point 2 above. While Smart Metering and the Smart Grid could be argued to be for 'the economic well-being of the country', whether mandating the roll out of smart meters for all domestic consumers is 'necessary in a democratic society' is open to debate. It will be necessary to prove that the collection of smart metering data that interferes with Article 8 is proportionate and no more than is necessary. The legal recommendation is that if there is an alternative, less intrusive, way of achieving the same aim then the alternative measure should be used. Ofgem E-Serve and DECC will need to be able to meet any such challenge from consumer groups, or other parties for GB.

Privacy Violations

The privacy violations the proposed Dutch smart metering law was believed to invoke were:

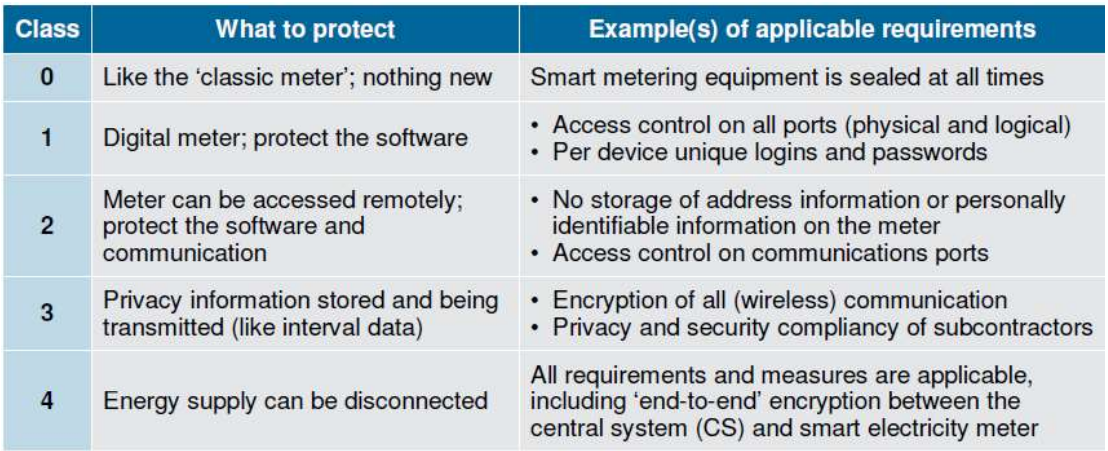
- Limitation of freedom of choice (consumers right to refuse the smart meter)
- Smart Meter data processing allows insight into:
  - Customer behaviours
  - Occupancy levels
  - Use and life-cycle of technical appliances
- Data storage:
  - Vulnerable to commercial interest
  - Vulnerable to criminal interest
  - Vulnerable to police interest
- Restriction in primary necessity of life – the supply of energy

[2] http://www.yourrights.org.uk/yourrights/the-human-rights-act/the-convention-rights/article-8-right-to-respect-for-private-and-family-life.html

Security measures

After the 2008 proposal was rejected significant work on smart metering privacy and security was undertaken. This has led to the adoption of various smart metering security measures, some of which are summarised in the following table:

Figure 1 - Dutch smart metering security suggestions[3]



Class	What to protect	Example(s) of applicable requirements
0	Like the 'classic meter'; nothing new	Smart metering equipment is sealed at all times
1	Digital meter; protect the software	• Access control on all ports (physical and logical) • Per device unique logins and passwords
2	Meter can be accessed remotely; protect the software and communication	• No storage of address information or personally identifiable information on the meter • Access control on communications ports
3	Privacy information stored and being transmitted (like interval data)	• Encryption of all (wireless) communication • Privacy and security compliancy of subcontractors
4	Energy supply can be disconnected	All requirements and measures are applicable, including 'end-to-end' encryption between the central system (CS) and smart electricity meter

A further suggestion is the application of end-to-end encryption between islands of trust. For example the smart meter could be an island that can securely send information to another island of trust, such as a data concentrator, using encryption keys. The data concentrator can then securely send information to the end recipient, another island of trust, using different encryption keys.

The critical lesson learnt from the Dutch smart metering roll out is that the later privacy and security is considered, the more expensive it will be to incorporate into the design of the solution.

[3] From netbeheer nederland presentation, "Practical lessons on developing privacy and security requirements for smart metering in the Netherlands", April 12th 2010 by Boas Bierings.