Assessment of the ‘remote ON/OFF control’ switch functionality in the context of cyber-security and the BAT evaluation

ECOS

12th March 2015

http://ecostandard.org

1.1. Introduction

Regarding the recent BAT stakeholder forum meeting 2015-03-05 and the currently proposed "Metrics and Assessment Methodology" draft report ECOS would like to provide the following assessment and comments, which are intended to clarify the questions we raised regarding the evaluation of the cyber security implications of the common minimum functionality ‘g’:

> *‘Allow remote on/off control of the supply and/or flow or power limitation’*

To preface our comments we would like to point out what our working assumptions are based on the following assessments:

I. Assuming that the smart meter is a passive participant of the electric grid, smart meters can pose a risk of loss of revenue or privacy, depending on the data collection characteristics and underlying communication systems. These damages can be resolved by normal political processes or legal procedures and do not pose an imminent risk to critical European infrastructure.

II. With the implementation of the common minimum functionality ‘g’ (remote on/off switch), smart meters are no longer just meters but now an active participant of the electric grid. The Smart Meter now has potential characteristics of a power generator or a power demand (depending on the actual power flow at each point in time). As such, in ECOS’ view, the smart meter must obey the same grid code rules as any other active device on the electric grid and not risk security of supply.

III. As soon as the smart meter is an active device on the electric grid, or as soon as it becomes a communications hub in the smart grid infrastructure, it must meet the same cyber security standards as all other active devices of the smart grid, such as generators or substations.

From recent geopolitical events and reports regarding the state of global cyber-security, it is clear that the electric grid of the European Union is a highly critical infrastructure, which needs to be protected against highly skilled organised criminals and foreign state actors. Therefore:

IV. Cyber security decisions must be made on the basis of the principles of forward looking caution and unbiased risk assessments. This includes a *systemic* analysis of the security by design principle.

Therefore, as an organization representing environmental and social concerns, ECOS insists that the highest level of security by design, when it comes to technology which has the potential to disrupt the critical European infrastructure. Counter-arguments suggestion that those threats are unlikely, because

- attackers would have to break the law
- attackers would have to be highly skilled

are not acceptable for us as a ‘solution’ to the risks posed by the ‘remote ON/OFF switch’ functionality.

1.2. The scale of the risks of the ON-OFF switch

Smart metering is implemented, for cost-benefit reasons, in bulk with typically one product per roll out. So systemic "features" (bugs) are available at a large scale after the roll out.

Smart metering roll-outs will be, in some countries, specifically targeted at distributed generation and at the goal of managing (cutting off) that distributed generation when needed. One example would be Germany, where already today 1.4 million PV installations, with a combined peak power of 22 GW, are connected to the low voltage grid. In the following decade(s) this number could rise beyond 50 GW.

Any national incident of 10 GW, or more, must be considered to be highly critical to the stability of the European grid.

So, for example, switching 50% of all German low voltage level PV would be enough to trigger such a cross border incident on the production side of the balance equation. With the European grid reaching a typical power consumption of ca. 300 GW, and assuming that ca. 100 GW would be under the control of smart meters with "ON-OFF" functionality at the low voltage level, then a coordinated cyber-attack on 10% of that demand side of the system could also result in a critical incident.

In that context it must also be stressed that shutting down 10 GW of consumption or production offline via a smart meter has a far more dramatic impact than switching off 10 GW of traditional power plants via a cyber-attack. Shutting down 10 GW of large power plants would most likely reduce the power in a gradual fashion over a couple of minutes, due to the high generator inertia created by its rotating masses. Moreover, the number of affected devices would be limited in number and have trained technicians on site.

Shutting down 10 GW via smart meters in a mass coordinated way can happen in less than one second, or even as quickly as 100 milliseconds. There is no inertia involved and each disconnection relay can easily handle the disconnection of its entire load. There would be no gradual reduction in energy but instead a hard cut-of, which could trigger secondary reactions (e.g. from protection devices at higher grid levels) that are difficult to predict. Due to the distributed nature and the large number of affected devices, applying a ‘fix’ to the smart metering system (region) that was attacked in such a way would most likely represent a huge challenge.

Only ‘synchronized bulk switching’ events pose a real danger. A bulk event requires synchronization of individual events. In the context of smart meters this, however, is almost trivial, as smart metering system typically support information broadcasting at the communication level and secondly, and perhaps more importantly, by design they must maintain a very precise time information (for tariff switching etc.).

1.3. Analysis of possible techniques

The following is a short overview of the techniques which ECOS has encountered and analysed in the context of the ‘remote ON/OFF switch’ and cyber-security threats outlined above.

1.3.1. Insufficient techniques

A1: Unsecure ‘remote ON/OFF switch’ command transmission

This technique would be in effect if the underlying communication infrastructure could be considered unsecure from the cyber-security point of view. Recent observations published on European Smart Meter roll-outs indicate that this is a realistic possibility.

A2: Secure "ON-OFF switch" command transmission

A robust encryption communication system can ensure that the command, which was broadcasted by the DSO, reaches (only) the intended target and that the command remains in its original form.

According to the discussion during the second BAT stakeholder forum this technique (secure communication channel) would be considered sufficient, even for the remote ON/OFF switch functionality.

Recent reports on numerous and sophisticated attacks on communication and computer systems, which have previously been considered ‘secure’, lead us to the conclusion that there remains a considerable risk that current secure communication could become unsecure during the long life time of a smart metering system (10 to 20 years). Typical attacks could focus on encryption systems which can be provoked to "leak" secrets (e.g. attacks on elliptic curve cryptography) or the highly efficient theft of internal databases holding the crypto keys, such as the recent Gemalto attack.

Moreover, as discussed during the first BAT stakeholder forum, a secure communication channel does not prevent incorrect commands from being correctly transmitted, as it would still result in incorrect actions. Such an attack would typically be triggered from within a trusted zone or communication network. Examples of high security computer networks which have been penetrated at central places in the recent past are plentiful, such as ‘Stuxnet’, ‘Flame’ and, ‘Shamoon’, among others.

Therefore a cyber-attack could be successful, if the attackers can inject an ON-OFF switch command into the regular system. The addition of secure communication cannot prevent such an attack, which is why ECOS does not consider this technique to be secure by design.

A3: Validation logic for the ‘remote ON/OFF switch’ command in the DSO backend

A technique, which was mentioned in the papers of the Smart Metering Coordination Group, to address the risks of A2 is to apply sanity checks for ON/OFF commands within the DSOs backend system. A documented implementation from the Netherlands tries to limit the number of switch commands for a given time period, so as to reduce the risk of bulk events.

Such a technique can prevent unintended bulk switch events, such as those triggered by DSOs employees (users of the backend system) or by a programming error in the backend software, if such programming error happens in the layers above the validation logic.

However, such a technique is not sufficient because it is implemented at a central location in software, which can be modified. History documents countless attacks on highly protected backend systems.

To draw a parallel to regular cryptography, this technique could be considered the 'MD5-password hash', which arguably is better than using plaintext passwords. However, given the large risk and the existing and well documented cyber-attacks of today, just being better is not good enough. This is why ECOS is unwilling to accept A3 as a solution to the problem.

1.3.2. Best available techniques

B1: No remote ON/OFF switch

Not including the remote ON/OFF switch is the best approach to solving the cyber security implications that arise from that functionality; however, this obviously would remove that feature from the list of the ten minimum functionalities.

If there is no disconnection relay, then it is possible to technically guarantee that the smart meter will never have a negative impact on grid stability.

In addition, the removal of the disconnection relay should significantly reduce the cost of a smart meter. Due to the high currents, that the relay has to disconnect under load, the relay must be robust and high quality. It significantly adds to the size of the meter, the weight and to the cost.

The technique of not having such a switch is clearly available on the market.

B2: Switching commands are validated against the grid code

The second most effective technique would be the validation of the remote ON/OFF switch command against the current state and the resulting impact on the electric grid.

From the European point of view, only a check against the status of the grids frequency is required. The smart meter must ensure that no generation is disconnected below a critical frequency and that no demand is disconnected above a critical frequency.

As the Smart Meter's switching activity is a binary operation (connected or not), similar grid code rules must be applied, as for (micro) cogeneration power plants. Furthermore, it is necessary that responses to the grids state are delayed by a random time factor, which must be large enough to prevent coordinated events. However, for this approach to really be considered as 'hardened against cyber-attacks', the responsible code must be outside the reach of what an upgradeable firmware can modify.

In the context of the BAT analysis it would also require a validation of the smart meters random number generation function(s) as they are critical for the random delay.

We are not aware of any real smart meter roll out which so far has implemented this technique.

However, we consider this technique to be available, because:

- there are multiple and inexpensive ways to solve the "out of firmware upgrade reach" issue
- robust random number generators are well documented
- required grid codes are well documented and established
- the implementation of the necessary grid state check should be possible in around ten lines of source code
- there are ways to implement the features at no additional cost to the product

1.4. Conclusion

Common minimum functionality ‘g’, the "remote ON/OFF switch", is the only metering functionality which poses a substantial risk to the security of supply.

According to our analysis there are two techniques (B1 and B2), which, in the context of cyber security, ECOS would consider safe and classify as security by design.