SUCCESS

Deliverable 5.8 V1.0

Data Management Plan for Trials, V2

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 700416.

Project Name	SUCCESS
Contractual Delivery Date:	April 30, 2018
Actual Delivery Date:	April 30, 2018
Contributors:	ESB, ASM, ECRO, ELCT
Workpackage:	WP5
Security:	CO
Nature:	R
Version:	1.0
Total number of pages:	13

Abstract:

This deliverable sets out version 2 of the data management plan for the SUCCESS trials. It describes the data management procedures to be used to manage personal data at individual trial sites and at the pan-European level.

Keyword list:
SUCCESS Project, data management, personal data

Disclaimer:
All information provided reflects the status of the SUCCESS project at the time of writing and may be subject to change.

Executive Summary

This deliverable updates the status regarding the generation of data by the three SUCCESS trials as originally reported in Deliverable 5.7.

As there has been no change in the trial plans, and the data generated is the same as planned, the text of the original deliverable remains fully valid, and apart from editorial changes, remains unchanged.

The objective of this deliverable is to identify the data to be generated in the three SUCCESS trials, in Ireland, Italy and Romania. To analyse this data and to determine whether it identifies or makes a natural person identifiable and resulting in the data being classified as personal, and in which case whether data protection law would be applicable.

The conclusion of this analysis is as follows:

1. For the Irish Trial, no data generated can be used to identify a natural person, and hence data protection law is not applicable to the handling of trial data.
2. For the Italian Trial, since attacks will be simulated, no personal data will be handled and therefore data protection law is not applicable to the handling of trial data.
3. For the Romanian Trial, no data generated can be used to identify a natural person, and hence data protection law is not applicable to the handling of trial data.

Authors

Partner	Name	e-mail
RWTH	Padraic McKeever	PMcKeever@eonerc.rwth-aachen.de
ESB	John Howard	john.howard2@esb.ie
ASM	Francesca Santori	francesca.santori@asmterni.it
CER	Mihai Sanduleac	mihai.sanduleac@crenerg.org

Table of Contents

1. Introduction 5
   1.1 Sope of this deliverable 5
   1.2 How to read this document 5
2. Data Management for the Irish Trial 6
   2.1 Introduction to the Irish Trial 6
   2.2 Data generation in the Irish Trial 6
   2.3 Analysis of data 6
   2.4 Irish Trial conclusion 6
3. Data Management for the Italian Trial 7
   3.1 Introduction to the Italian Trial 7
   3.2 Data generation in Italian Trial. 7
   3.3 Analysis of data 7
   3.4 Italian Trial conclusion 7
4. Data Management for the Romanian Trial 9
   4.1 Introduction to the Romanian Trial 9
   4.2 Data generation in Romanian Trial 9
   4.3 Analysis of data 9
   4.4 Romanian Trial conclusion 9
5. Conclusion 10
6. References 11
7. List of SUCCESS Abbreviations 12

1. Introduction

1.1 Sope of this deliverable

The objective of this deliverable is to identify the data to be generated in the three SUCCESS trials, in Ireland, Italy, and Romania, and to analyse this data and determine whether it identifies or makes a natural person identifiable. If so, the data would be classified as personal data. We whether data protection law would be applicable.

While the NORM devices can generate a wide range of different data for input to the CI-SOC, as specified in Annex A of Deliverable 3.7, only a limited subset of this data will be used in the trials, the relevant data is noted below in the description for each trial site.

1.2 How to read this document

This document provides information on the data generated by the SUCCESS trial sites and an analysis of the data protection implications.

- Section 2 covers the Irish Trial
- Section 3 covers the Italian Trial
- Section 4 covers the Romanian Trial.
- Sections 5 and 6 provide references and conclusions.

General descriptions of the SUCCESS solution and components deployed at the trial sites can be found in Deliverable 2.4.

2. Data Management for the Irish Trial

2.1 Introduction to the Irish Trial

The objective of the Irish Trial is to deploy a NORM device incorporated into an electric vehicle charging unit, in order to manage the security of the unit, to detect and to counter cyberattacks.

The function and architecture of the trial is described in Section 2.1 of Deliverable 5.1.

2.2 Data generation in the Irish Trial

In the Irish Trial data is generated by the Wally smart meter [1]. The main data elements generated are the following:

- Current measurements
- Voltage measurements
- Frequency measurements

These elements are collected from the meter every second. The following information can be derived from basic measurements:

- Energy usage
- Power quality

The equipment used in the trial will be owned by the ESB. Data generated during the trial will be under the control of the ESB.

The trial configuration will not monitor the identity of a vehicle connected to the charger or the identity of the user, as this is not required for the project.

Other data such as the availability of electric vehicle to grid power is not considered in this project but is being assessed in other projects such as Reserve[1].

2.3 Analysis of data

As the trial site is not open to the public and access to the EV charging station is restricted to ESB staff, no form of access control or cost based charging is used, hence no data on which vehicle or which users is connected to the charge point is collected. Hence, the only information provided to SUCCESS components are the direct measurement elements mentioned above and the two derived elements.

These seven elements do not contain any personal data, as there is no identification of the car or the user of the car that is connected to the charge point.

Thus, there is no issue with the use of the above information elements, in their storage, manipulation, and transmission, either within the Irish jurisdiction or abroad.

2.4 Irish Trial conclusion

As no personal data is being generated by the Wally or NORM devices in the Irish trial, no special precautions are required to handle data in the trial. However, it is possible that in a commercial deployment some personal data might be generated. Such data should be handled by the system in a correct manner using the Privacy-Preserving Information Security Architecture, being developed in Workpackage 3 (see Deliverables 3.2 and 3.3. for a description of the architecture).

[1] This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 727481

3. Data Management for the Italian Trial

3.1 Introduction to the Italian Trial

The objective of the Italian Trial is to deploy five NORM devices incorporated into different block of energy (BoE) units, namely electric vehicle charging station, photovoltaic arrays, batteries and blocks of buildings, in order to manage the security of ancillary services and demand response systems, and to detect and counter cyberattacks. ASM TERNI is the owner of the BoE units used during the trial as well as of the data currently generated by each unit.

The function and architecture of the trial is described in Section 2.3 of Deliverable 5.1.

3.2 Data generation in Italian Trial.

In the Italian Trial, data is generated by the Wally smart meter [1]. The main data elements generated are the following:

- Current measurements
- Voltage measurements
- Frequency measurements
- Power factor
- Harmonics measurements
- Flicker measurements

These elements are collected from the meter every second. The following information is derived from basic measurements:

- Energy usage
- Active Power
- Reactive Power
- Power quality

Since the trial configuration will be put offline, data will be generated only under request. However, historical data concerning each BoE units could be provided by ASM TERNI to SUCCESS partners under signing a data management agreement.

It is worth pointing out that demand response and ancillary services strategies are currently under study by Nobel Grid - *New Cost Efficient Business Models for Flexible Smart Grids* (GA n. 646184) [2] and ELSA *Energy Local Storage Advanced system* (GA n. 646125) [3] H2020 projects in terms of technical performance and socio-economic sustainability.

3.3 Analysis of data

As the trial site is not open to the public and under control of ASM TERNI, no form of access control or charging is used. Moreover, since attacks will be simulated, hence no personal data will be managed by the SUCCESS project for this trial.

However, in case of analysis of historical data provided by ASM TERNI to the SUCCESS consortium for the purposes of SUCCESS, ASM TERNI shall require a consent for data processing (collection, storage, manipulation, access and transmission) and will inform the involved data subjects through a general information according to Article 14(5) lett. b of the GDPR, even following the examples contained in Annex II of Deliverable 2.1. In that case the data controller is ASM and not SUCCESS, which does not determine means and purposes of the data processing, but may just receive specific data.

3.4 Italian Trial conclusion

As no personal data is being generated by the NORM device in the Italian trial, no special precautions are required to handle data generated during the trial.

However, it is possible that in a commercial deployment some personal data may be generated. Such data should be handled by the system in a correct manner using the Privacy-Preserving Information Security Architecture, being developed in the document D3.2 and D 3.3.

The transfer of historical data to other partners may require a data management agreement.

4. Data Management for the Romanian Trial

4.1 Introduction to the Romanian Trial

The objective of the Romanian Trial is to deploy up to seven NORM devices incorporated into different Energy Exchange Points (EExP) units, named PVPP, WPP, SS-secondary substation (MV/LV) and PS-primary substation, with responsibility for detecting and countering cyberattacks.

The function and architecture of the trial is described in Section 2.2 in Deliverable 5.1.

4.2 Data generation in Romanian Trial

In the Romanian Trial data is generated by the A1800 or SL7000 local smart meter [4,5] and by the low-cost PMU developed in the project. The main data elements generated by the cumulated equipment are the following:

- Time of measurements
- Voltage measurements
- Frequency measurements
- Phase of voltage measurements

These elements are collected from each five to ten seconds for the smart meters and each second for the low-cost PMU.

4.3 Analysis of data

As the trial site is not open to the public and under control of Electrica, no form of access control is used. Moreover, since attacks will be simulated, no personal data will be managed by the SUCCESS project.

However, in case of analysis of historical data provided by Electrica to the SUCCESS consortium for the purposes of SUCCESS, Electrica shall require a consent for data processing (collection, storage, manipulation, access and transmission) and will inform the involved data subjects through a general information according to Article 14(5) lett. b of the GDPR, even following the examples contained in Annex II of Deliverable 2.1.

4.4 Romanian Trial conclusion

As no personal data is being generated by the NORM devices in the Romanian Trial, no special precautions are required to handle data generated during the trial. However, it is possible that in a commercial deployment some personal data may be generated. Such data should be handled by the system in a correct manner using the Privacy-Preserving Information Security Architecture, being developed in WP 3, as described in Deliverable 3.2.

5. Conclusion

No personal data issues have been identified in the current SUCCESS trial configurations, and hence no additional measures are required for the secure handling, storage, transmission or processing of the generated data.

While it is not planned to change the architecture of the trial over the course of the project, if changes are made, the data management implications will be re-assessed to ensure that any generation of data identifying an individual is flagged, and appropriate protection measures are put in place.

In some cases, the transfer of historical data to another SUCCESS partner may require a data management agreement be put in place and specific measures (asking for the consent and informing the data subject following the form contained in Deliverable 2.1) shall be put in place.

6. References

[1] Wally A3 Energy and Power Quality Meter. User Manual, TeamWare, 1st Edition November 2011.

[2] H2020 Nobel Grid project, www.nobelgrid.eu (accessed on 24.04.2017)

[3] H2020 ELSA project, http://elsa-h2020.eu/ (accessed on 24.04.2017)

[4] Brochure Elster A1800 ALPHA meter, 2010, https://www.elstersolutions.com/assets/products/products_elster_files/DS42-1003F.pdf (accessed 25.04.2017)

[5] Brochure Itron SL7000 meter, https://www.itron.com/eu/-/media/itron/integration/brochure/acesl7000el00191fr0615.pdf (accessed 24.04.2017)

7. List of SUCCESS Abbreviations

3GPP	3rd Generation Partnership Project (standardisation body for cellular communication)
4G	4th Generation Mobile Communication Network, also known as LTE
5G	5th Generation Mobile Communication Network
AAA	Authentication, Authorisation and Accounting
ADN	Active Distribution Network
AES	Advanced Encryption Standard
AH	Authentication Header
AMI	Advanced Metering Infrastructure
AMR	Automatic Meter Reading
API	Application Programming Interface
BMS	Building Management System
BR-GW	Breakout Gateway
CI	Critical Infrastructure
CIMP	Critical Infrastructure Management Platform
CI-SAN	Critical Infrastructure Security Analytics Network
CI-SOC	Critical Infrastructure Security Operations Centre
CoAP	Constrained Application Protocol
COSEM	Companion Specification for Energy Metering
CPS	Cyber-Physical System
dB	decibel (measurement unit for signal)
DDoS	Distributed Denial of Service Attack
DER	Distributed Energy Resources
DG	Distributed Generation
DG	Distribution Grid
DLMS	Device Language Message Specification
DSE	Domain Specific Enabler
DSO	Distribution System Operator
DTLS	Datagram Transport Layer Security
DV	Double Virtualisation
E2E	End-to-end
EAS	European Awareness System
EC-GSM-IoT	Extended Coverage GSM for IoT
EM	Energy Management
EMS	Energy Management System, computer-aided tools used by Critical Infrastructure operators of electric grids to monitor, control, and optimise the performance of the generation and/or transmission system.
eNodeB	Evolved Node B, radio base station in LTE and 5G networks
ENTSO-E	European Network of Transmission System Operators for Electricity
ESP	Encapsulating Security Payload
EV	Electric Vehicle
GBA	Generic Bootstrapping Architecture
GDPR	General Data Protection Regulation
GPRS	General Packet Radio Service, 2. 5th generation mobile communications system.
GSM	Groupe Spécial Mobile, 2nd generation mobile communications system.
HLR	Home Location Register, node in mobile network
HSS	Home Subscriber Server, node in mobile network
HTTP	Hypertext Transfer Protocol
HV	High Voltage
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IoT	Internet of Things
IPsec	Internet Protocol Security
IT	Information Technology, part of ICT supporting business processes
LTE	Long-term Evolution, 4th generation mobile communications system
LV	Low Voltage

MQTT	Message Queue Telemetry Transport
MTC	Machine-type Communication
MV	Medium Voltage
NAC	Network Access Control
NAN	Neighbourhood Area Network
NB-IoT	Narrow-Band Internet-of-Things
NERC	North American Electric Reliability Corporation
NFV	Network Function Virtualisation
NORM	Next-generation Open Real-time Smart Meter
OS	Operating System
OT	Operational Technology, ICT supporting measurement and control
PKI	Public Key Infrastructure
PMU	Phasor Measurement Unit
PTP	Precise Time Protocol
PUF	Physically Unclonable Function
PV	Photo Voltaic
QoS	Quality of Service
RBS	Radio Base Station
RES	Renewable Energy Sources
REST	Representational State Transfer
RSA	Rivest, Shamir und Adleman (asymmetric cryptographical process)
RSC	Regional Security Coordinator
SA Node	Security Analytics Node
SA	Security Association
SCADA	Supervisory Control and Data Acquisition
SDC	Security Data Concentrator
SDN	Software Defined Networking
SHA	Secure Hash Algorithm
SIEM	Security Information/Event Management
SM	Smart Meter
SSS	SUCCESS Security Solution
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TPM	Trusted Platform Module
TSO	Transmission System Operator
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System, 3rd generation mobile communications system
USIM	Universal Subscriber Identity Module
USM	Unbundled Smart Meter
VPN	Virtual Private Network