AUTOMAÇÃO, PROTEÇÃO, COMANDO, CONTROLO E COMUNICAÇÕES

Gateway PLC

Características e ensaios

Elaboração: DIT

Homologação: conforme despacho do CA de 2022-03-30

Edição: 1ª.

Acesso: **Livre** **X** Restrito Confidencial

Emissão: E-REDES – Distribuição de Eletricidade, S.A.
DIT – Direção de Inovação e Desenvolvimento Tecnológico
R. Camilo Castelo Branco, 43 □ 1050-044 LISBOA □ Tel.: 218100100
E-mail: TEC@e-redes.pt

ÍNDICE

0 INTRODUÇÃO

O presente documento destina-se a definir as características construtivas, funcionais, de comunicação e ensaios aplicáveis ao equipamento Gateway PLC.

O código de identificação JUMP da Gateway PLC é indicado na seguinte tabela.

Designação	Código JUMP
Gateway PLC	20151030

1 OBJETIVO E CAMPO DE APLICAÇÃO

A Gateway PLC é um equipamento destinado a ser instalado em Postos de Transformação (PT) MT/BT ou ao longo da rede BT, em local apropriado, em que seja necessário injetar ou regenerar a comunicação PLC existente na linha elétrica.

Face à ausência de uma norma de produto, foi considerada como norma de referência a IEC 60870, referente aos sistemas e equipamentos de telecomando.

2 NORMAS E DOCUMENTOS DE REFERÊNCIA

O presente documento inclui disposições de outros documentos, referenciados nos locais apropriados do seu texto, os quais se encontram a seguir listados, com indicação das respetivas datas de edição.

Quaisquer das referidas edições só serão aplicáveis, no âmbito do presente documento, se forem objeto de inclusão específica, por modificação ou aditamento ao mesmo.

2.1 Documentos E-REDES

Documento	Edição	Título
D00-C10-001/N	2013	Condições de serviço e características gerais da rede de distribuição em AT, MT e BT. Generalidades.
DMA-C44-502/N	2013	Contadores estáticos, combinados, de ligação directa ou por transformador de corrente, para pontos de medição BTE e MT (ligação do lado da BT).
DEF-C44-504/N	2013	Contadores estáticos, combinados, para pontos de medição BTE e MT – Especificação Funcional.
DMA-C44-506/N	2020	Equipamentos de monitorização de rede e de telecontagem estáticos, combinados, para pontos de BTN monofásicos / trifásicos – Características e Ensaios.
DEF-C44-506/N	2020	Equipamentos de monitorização de rede e de telecontagem estáticos, combinados, para pontos de BTN monofásicos / trifásicos – Especificação Funcional.
DEF-C44-507/N	2020	Complemento aos standards para modelo de dados e interfaces de comunicação – Especificação Funcional.
DEF-C44-508/N	2015	Equipamentos de monitorização de rede, de telegestão e de contagem, estáticos, combinados, para pontos de medição de IP.
DMA-C98-104/N	2021	Router para implementação de Arquitetura Integrada de Comunicações ao nível do Posto de Transformação MT/BT
DMA-C98-405/N	2020	Controlador de Transformador de Distribuição (Distribution Transformer Controller – DTC) para instalação em Postos de Transformação MT/BT – Características e Ensaios
DEF-C98-405/N	2020	Controlador de Transformador de Distribuição (Distribution Transformer Controller – DTC) para instalação em Postos de Transformação MT/BT – Especificação funcional
DEF-C98-407/N	2020	Controlador de Transformador de Distribuição (Distribution Transformer Controller – DTC) para instalação em Postos de Transformação MT/BT - Especificação protocolo HES-DTC
DEF-C98-408/N	2020	Controlador de Transformador de Distribuição (Distribution Transformer Controller – DTC) para instalação em Postos de Transformação MT/BT - Security Functional Specification
DEF-C98-409/N	2020	Controlador de Transformador de Distribuição (Distribution Transformer Controller – DTC) para instalação em Postos de Transformação MT/BT - HES-DTC Interface Specification – Use cases

DEF-C98-412/N	2020	Controlador de Transformador de Distribuição (Distribution Transformer Controller – DTC) para instalação em Postos de Transformação MT/BT - Management Information Base (MIB) Specification

2.2 Normas

Norma	Edição	Título
EN 61709	2017	Electric components - Reliability - Reference conditions for failure rates and stress models for conversion
IEC 62208	2011	Empty enclosures for low-voltage switchgear and controlgear assemblies - General requirements
IEC 60068-2-1	2007	Environmental testing – Part 2-1: Tests – Test A: Cold
IEC 60068-2-2	2007	Environmental testing procedures – Part 2-2: Tests – Test B: Dry heat
IEC 60068-2-6	2007	Environmental testing procedures – Part 2-6: Tests – Test Fc: Vibration (sinusoidal)
IEC 60068-2-27	2008	Environmental testing procedures – Part 2-27: Tests – Test Ea and guidance: Shock
IEC 60068-2-78	2012	Environmental testing – Part 2-78: Tests - Test Cab: Damp heat, steady state
IEC 60255-27	2013	Measuring relays and protection equipment – Part 27: Product safety requirements
IEC 60870-2-1	1995	Telecontrol equipment and systems – Part 2: Operating conditions – Section 1: Power supply and electromagnetic compatibility
IEC 60870-2-2	1996	Telecontrol equipment and systems – Part 2: Operating conditions – Section 2: Environmental conditions (climatic, mechanical and other non-electrical influences)
IEC 61000-4-2	2008	Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test
IEC 61000-4-3	2006	Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test
IEC 61000-4-4	2012	Electromagnetic compatibility (EMC) – Part 4-4: Testing and measurement techniques – Electrical fast transient/burst immunity test
IEC 61000-4-5	2014	Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test
IEC 61000-4-8	2009	Electromagnetic compatibility (EMC) – Part 4-8: Testing and measurement techniques – Power frequency magnetic field immunity test
IEC 62477-1	2012 (AMD1 2016)	Safety requirements for power electronic converter systems and equipment - Part 1: General (2012 + AMD1 2016)
IEC 62262	2002	Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code)
IEEE 802.3.i	1990	10BASE-T 10 Mbit/s over twisted pair
IEEE 802.3.u	1995	IEEE Standards for Local and Metropolitan Area Networks: Supplement to Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Media Access Control (MAC) Parameters, Physical Layer, Medium Attachment Units, and Repeater for 100 Mb/s Operation, Type 100BASE-T (Clauses 21-30)
IEEE 802.1Q	2011	IEEE Std. 802.1Q-2011, Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks
NP EN 60529	2013	Graus de protecção assegurados pelos invólucros (Código IP)
TIA/EIA-485	2003	Electrical Characteristics of Generators and Receivers for Use in Balanced Digital Multipoint Systems

3 TERMOS E DEFINIÇÕES

Para efeitos do presente documento, são aplicáveis os seguintes termos e definições:

3.1 Gateway

Equipamento que faz a conversão de protocolos de comunicação, e que funciona como ponte entre dois meios de comunicação diferentes, p.e entre o meio físico (rede PLC) e o meio celular (rede TCP/IP).

3.2 Base Node

Nó mestre que controla e gere os recursos e suas ligações formando uma sub-rede.

3.3 Service Node

Qualquer nó de uma sub-rede que não é *Base Node*.

3.4 Mega DTC

Sistema constituído por vários DTC virtuais, com mecanismos de alta disponibilidade e integração com a rede técnica da E-REDES.

3.5 DTC Virtual

Sistema de informação que permite virtualizar as funcionalidades do DTC físico, usado como peça integrante da arquitetura inovgrid para gerir um EMI que não esteja associado a um DTC físico.

3.6 Invólucro

Parte destinada a assegurar a proteção do equipamento contra certas influências externas e assegurar, sobre todas as suas faces, uma proteção contra os contactos diretos com um grau de proteção mínimo (norma IEC 61439-1, secção 3.4.5).

3.7 Equipamento de classe II

Equipamento, cuja proteção contra o choque elétrico não reside unicamente na isolação principal, dispondo também de medidas de segurança suplementares, tais como, duplo isolamento ou isolamento reforçado. Essas medidas não incluem a utilização de dispositivos para ligação à terra de proteção nem dependem das condições de instalação (norma IEC 61140).

3.8 Grau de poluição

Reporta-se às condições de ambiente para os quais o conjunto de aparelhagem está previsto (IEC 61439-1 secção 7.1.3).

3.9 Altitude

Reporta-se às condições de ambiente para os quais o conjunto de aparelhagem está previsto (IEC 61439-1 secção 7.1.4).

3.10 Evento

Ocorrência de um acontecimento que leva ao seu registo em memória específica (designada log) do equipamento. O registo de eventos é realizado de forma cronológica em memória circular.

3.11 Alarme

Ativação, configurável, de um registo próprio na Gateway PLC como resultado de um qualquer evento, com possibilidade de ser enviado de imediato ou com um atraso (configurável) para os sistemas centrais. Um alarme é ativado por um evento e permanece ativo até ser apagado por comando externo ou por ocorrência de um outro evento (configurável).

3.12 Ensaios de tipo

Ensaios realizados a fim de demonstrarem características satisfatórias tendo em conta as aplicações previstas. São ensaios de natureza tal que, uma vez realizados, não precisam de ser repetidos, a não ser que ocorram mudanças nas matérias-primas, na conceção ou no processo de fabrico, que possam alterar as características do equipamento.

3.13 Ensaios de série

Ensaios realizados de forma repetitiva durante o ciclo de fabricação do produto, quer sob a forma de ensaios individuais quer, sob a forma de ensaios por amostra. Estes ensaios têm como objetivo verificar que uma dada fabricação satisfaz os critérios definidos.

3.14 Ensaios de receção

Ensaios efetuados pelo fabricante, com a presença do cliente ou de uma terceira entidade em sua representação, com o objetivo de verificar a conformidade de um fornecimento com a especificação técnica aplicável.

4 ABREVIATURAS

No presente documento são usadas as seguintes abreviaturas:

AMI	Advanced Metering Infrastructure
AMR	Automated Meter Reading
APN	Access Point Network
BT	Baixa Tensão
BTE	Baixa Tensão Especial
BTN	Baixa Tensão Normal
CLI	Command Line Interface
COSEM	COmpanion Specification for Energy Metering
DEF	Documento de Especificações funcionais da E-REDES
DIN	Deutsches Institut fur Normung e.V.
DLMS	Device Language Message Specification
DMA	Documento normativo de características e ensaios de materiais e aparelhos da E-REDES
DMS	Distribution Management System
DTC	Distribution Transformer Controller
EMI	Equipamento de Medição Inteligente
EMI IP	Equipamento de Medição Inteligente de Iluminação Pública
EN	Norma Europeia
FCAPS	Fault, Configuration, Accounting, Performance, Security
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
GPRS	General Packet Radio Service
GW	Gateway PLC PRIME
HDLC	High-Level Data Link Control
HMI	Human Machine Interface
HTTPS	HyperText Transfer Protocol Secure
HES	Head End System
ICMP	Internet Control Message Protocol
IEC	Comissão Eletrotécnica Internacional

IP	Internet protocol ou Índice (grau) de proteção[1)]
ISO	Organização Internacional de Normalização
LAN	Local Area Network
MAC	Medium Access Control
MIB	Management Information Base
MTBF	Mean Time Between Failures
NAT	Network Address Translation
NHRP	Next Hop Resolution Protocol
NMS	Network Management System
NP	Norma Portuguesa
NTP	Network Time Protocol
PAT	Port Address Translation
PLC	Power Line Communication
PLMN	Public Land Mobile Network
PRIME	PoweRline Intelligent Metering Evolution
PT	Posto de Transformação
SIM	Subscriber Identity Module
RIP	Routing Information Protocol
RADIUS	Remote Authentication Dial In User Service
SCP	Secure Copy
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SSH	Secure Shell
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual LAN
VPN	Virtual Private Network
WAN	Wide Area Network

5 FUNÇÕES

A Gateway PLC é um equipamento para instalação num posto de transformação, ou noutro local da rede de baixa tensão da E-REDES, com objetivo de garantir a comunicação de um DTC físico ou virtual com os EMI que possuem tecnologia de comunicação PLC.

O equipamento Gateway PLC tem como funções principais as que se sumarizam de seguida:

— Função de criação e exploração de uma rede de comunicação PLC:

Nas redes BT com um reduzido número de EMI, em substituição de DTC físico, poderá ser instalado uma Gateway PLC, a funcionar como base node, de forma a criar uma rede de comunicação PLC em que seja possível a exploração da infraestrutura de equipamentos EMI.

1) De acordo com a norma NP EN 60529.

— Função de regeneração da tecnologia de comunicação PLC:

Nas situações em que o nível de sinal-ruído numa rede PLC seja demasiado baixo que não permita a exploração da infraestrutura de equipamentos EMI deverá ser possível a utilização de Gateway PLC que permitam realizar a função de adaptação do meio físico de comunicação, realizando a regeneração do sinal PLC, quando o equipamento está configurado como service node.

— Função de simplificação da gestão da rede PLC:

Nas redes BT extensas, com um elevado número de EMI, que dificulte a gestão e operação de equipamentos num período de tempo aceitável, poderá ser instalado uma Gateway PLC, a funcionar como base ou service node, de forma a que a gestão e operação desses equipamentos seja feita de forma distribuída.

Adicionalmente, em redes extensas a inclusão de Gateway PLC irá diminuir o número de níveis de regeneração da comunicação PLC tornando mais rápido o tempo de polling.

Nota: *As funções requeridas neste documento, entendidas como o mínimo exigível, não limitam a eventual existência de outras, ou da sua maior complexidade, desde que desse facto não resultem inconvenientes para a exploração dos equipamentos.*

Nas figuras 1, 2, 3 e 4 estão indicados os 4 cenários de utilização da Gateway PLC, e a infraestrutura base em cada um deles.

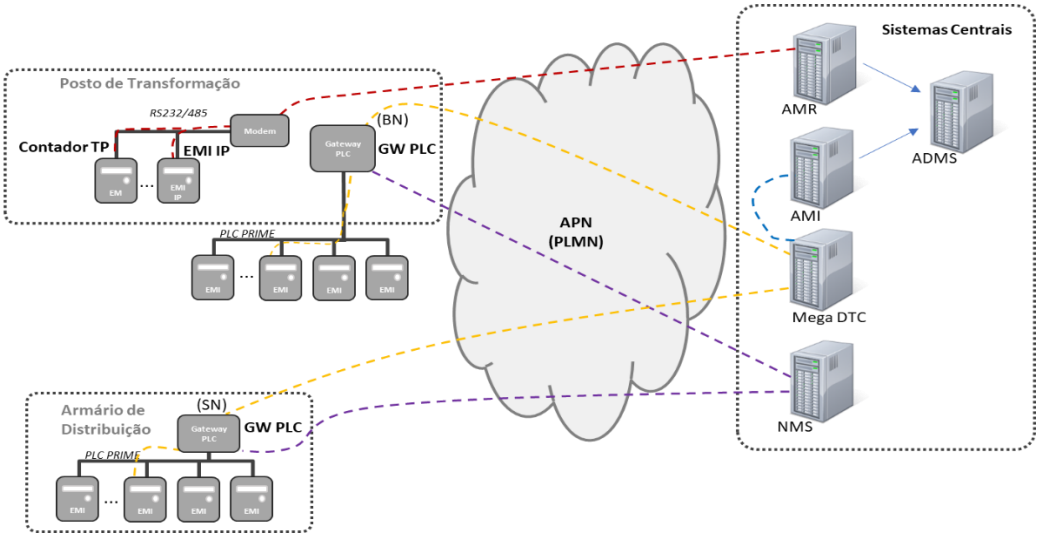


Figura 1 - Instalação de Gateway PLC em PTD com poucos clientes em substituição de DTC físico

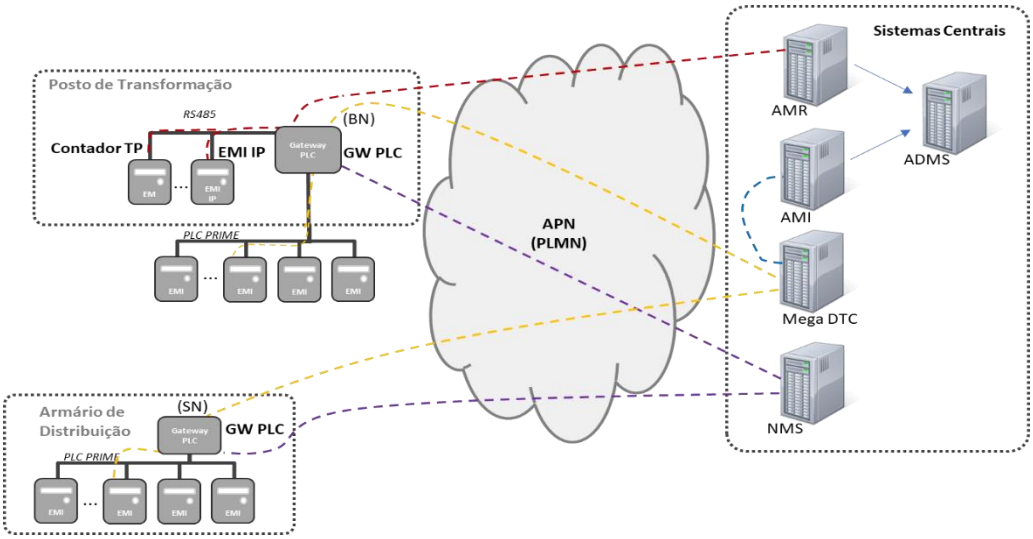


Figura 2 - Instalação de Gateway PLC em PTD com poucos clientes em substituição de DTC físico, com ligação ao EMI IP e contador totalizador através da interface RS485

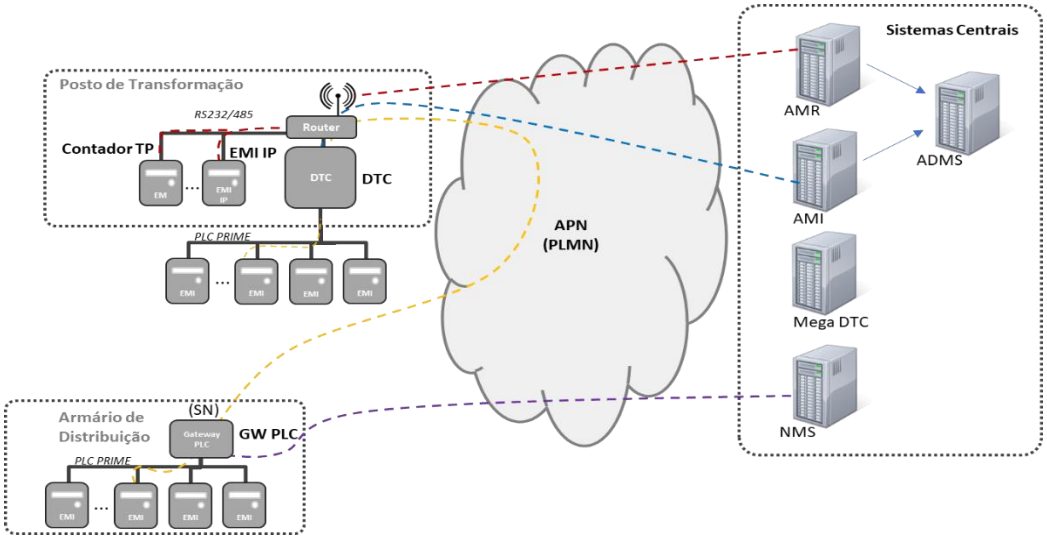


Figura 3 - Instalação de Gateway PLC em determinados troços de rede onde existem dificuldades de comunicação (ruído, atenuação)

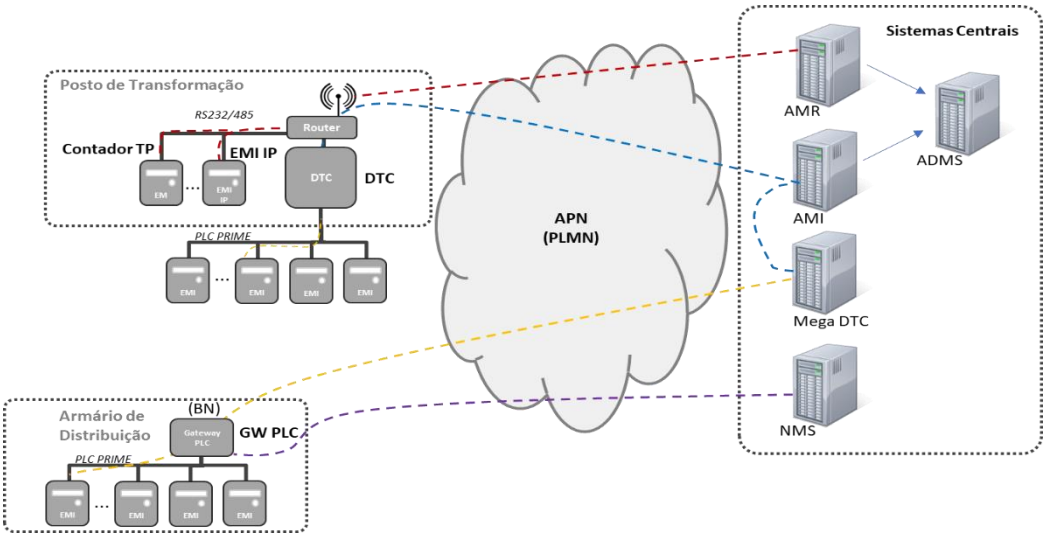


Figura 4 - Instalação de Gateway PLC onde existe dificuldade de comunicação devido à elevada dimensão de rede

6 ARQUITETURA

A Figura 5 apresenta a arquitetura base da Gateway PLC para ligação a dispositivos externos, através da rede LAN, TAN e WAN (Ethernet e celular), permitindo a comunicação com os EMI PLC, EMI IP (preferencialmente), contadores totalizadores (preferencialmente) e sistemas centrais.

A interface LAN utiliza o PLC PRIME para comunicar com os EMI PLC PRIME instalados na rede BT.

A interface TAN utiliza uma porta série RS485, preferencialmente para comunicação com o EMI IP e contador totalizador.

A interface WAN utiliza uma porta Ethernet como consola ou outras comunicações locais. A interface WAN utiliza ainda um modem interno (WAN celular) para as comunicações remotas com os sistemas centrais.

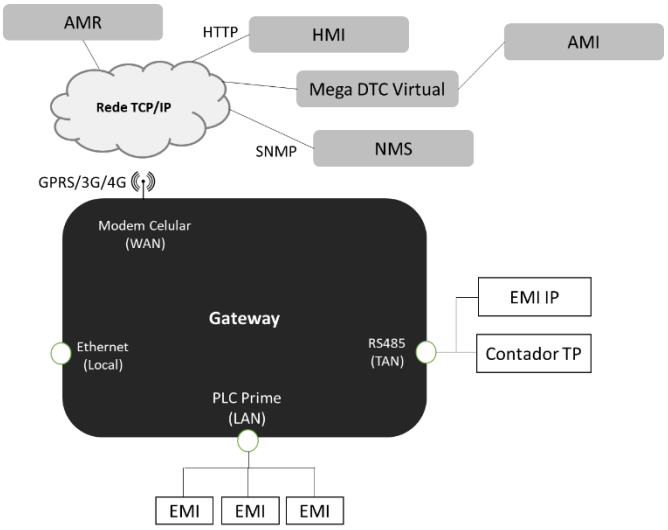


Figura 5 – Arquitetura Gateway PLC – Interfaces e Protocolos

A Gateway PLC é um equipamento constituído pelos seguintes componentes unitários:

— Gateway;

— Antena (incluindo suporte e cabo);

— Adaptador externo para a interface RS485, se aplicável.

As componentes de gestão do equipamento, que fazem parte da especificação e do Produto a fornecer, são as seguintes indicadas:

— Gestor de Elemento;

— Gestor de Rede (preferencial).

7 TIPO DE REQUISITOS

Nesta especificação, os requisitos aplicáveis a Gateway PLC estão agrupados em conjuntos correspondentes a diferentes funções. Cada requisito tem um identificador próprio e uma classificação (que só é explícita para os requisitos não obrigatórios):

- Obrigatório – requisito que tem obrigatoriamente de ser cumprido; por omissão, os requisitos são obrigatórios.
- Preferencial (PREF) – requisito cujo cumprimento não é obrigatório, mas que pode ser valorizado pela E-REDES por reconhecer valor acrescentado ao equipamento que o apresente.
- Opcionais (OP) – requisito que pode ser ou não implementado, por opção da E-REDES. Não é obrigatório que o equipamento consiga implementar os requisitos opcionais, mas, caso não os implemente, não será adequado nas situações em que as funções associadas a esses requisitos sejam requeridas pela E-REDES.

8 CONDIÇÕES GERAIS E NORMAIS DE SERVIÇO

As Gateways PLC objeto da presente especificação deverão ser concebidas para funcionamento nas características ambientais climáticas, mecânicas, de compatibilidade eletromagnética e de alimentação indicadas no seguimento.

8.1 Condições ambientais climáticas e altitude

Requisito	Descrição
R001	**Condições ambientais climáticas** Os equipamentos destinam-se a ser instalados em locais cujas condições ambientais climáticas são caracterizadas da seguinte forma: — temperatura de funcionamento (valores nominais): -20 ºC a +55 ºC;

	— temperatura de armazenamento e transporte (valores extremos): -40 ºC e +70 ºC; — humidade relativa até 95%, sem condensação. A comprovação da satisfação deste requisito será efetuada através da realização dos ensaios descritos na secção 12.3.3 do presente documento.
R002	**Condições ambientais de poluição (Grau de poluição)** O equipamento deverá operar em ambientes com grau de poluição 3.
R003	**Condições ambientais em serviço - altitude** O equipamento deverá operar sem constrangimentos em ambientes até altitudes de 2000 metros.

8.2 Condições ambientais mecânicas

Requisito	Descrição
R004	**Vibração (Sinusoidal)** De acordo com os locais onde os equipamentos vão ser instalados, considera-se o equipamento incluído na classe Bm, de acordo com o disposto na norma IEC 60870-2-2. A comprovação da satisfação deste requisito será efetuada através da realização do ensaio descrito na secção 12.3.4.1 12.3.3 do presente documento.
R005	**Choque** De acordo com os locais onde os equipamentos vão ser instalados, considera-se o equipamento incluído na classe Bm, de acordo com o disposto na norma IEC 60870-2-2. A comprovação da satisfação deste requisito poderá ser efetuada através da realização do ensaio descrito na secção 12.3.4.2 12.3.3 do presente documento.

8.3 Condições de compatibilidade eletromagnética

Requisito	Descrição
R006	**Imunidade a transitórios conduzidos e perturbações de alta frequência** De acordo com os locais onde os equipamentos vão ser instalados, considera-se que o equipamento deve estar incluído no nível de severidade 3, de acordo com o disposto na tabela 12 da norma IEC 60870-2-1, no que respeita a: — Transitório elétrico rápido (IEC 61000-4-4); — Ondas de choque (IEC 61000-4-5); — Ondas oscilatórias amortecidas (IEC 61000-4-12) - Preferencialmente. A comprovação da satisfação deste requisito será efetuada através da realização dos ensaios descritos na secção 12.3.7.1.1 , 12.3.7.1.2 e 12.3.7.1.3 do presente documento.
R007	**Imunidade a descargas eletrostáticas (IEC 61000-4-2)** De acordo com os locais onde os equipamentos vão ser instalados, considera-se que o equipamento deve estar incluído no nível de severidade 3, de acordo com o disposto na tabela 13 da norma IEC 60870-2-1. A comprovação da satisfação deste requisito será efetuada através da realização dos ensaios descritos na secção 12.3.7.2 do presente documento.
R008	**Imunidade a campos magnéticos (IEC 61000-4-8)** De acordo com os locais onde os equipamentos vão ser instalados, considera-se que o equipamento deve estar incluído no nível de severidade 3, de acordo com o disposto na tabela 14 da norma IEC 60870-2-1. A comprovação da satisfação deste requisito será efetuada através da realização dos ensaios descritos na secção 12.3.7.3 do presente documento.

R009	**Imunidade a campos eletromagnéticos radiados (IEC 61000-4-3)** De acordo com os locais onde os equipamentos vão ser instalados, considera-se que o equipamento deve estar incluído no nível de severidade 3, de acordo com o disposto na tabela 15 da norma IEC 60870-2-1. A comprovação da satisfação deste requisito será efetuada através da realização dos ensaios descritos na secção 12.3.7.4 do presente documento.

9 REQUISITOS GERAIS E CONSTRUTIVOS

9.1 Requisitos Genéricos

Requisito	Descrição
R0010	**Arquitetura** O equipamento deverá possuir uma arquitetura que permita a integração de novas funcionalidades através de upgrade remoto e local do seu software e/ou firmware.
R0011	**Materiais Construtivos** O equipamento deve ser construído com materiais capazes de suportar os constrangimentos mecânicos, elétricos e térmicos, e também os efeitos de humidade, suscetíveis de serem encontrados nas condições de armazenamento, transporte e de funcionamento, definidas na secção 8 do presente documento.
R0012	**Invólucro** O equipamento deverá possuir um invólucro de material isolante que garanta proteção de grau II contra choques elétricos. O invólucro deverá assegurar a proteção de pessoas contra contactos com peças em tensão. O equipamento não deverá necessitar de ligação à terra de proteção.
R0013	**Índice (grau) de proteção IP** O equipamento deve garantir o grau de proteção mínimo IP 31. A comprovação da satisfação deste requisito será efetuada através da realização dos ensaios descritos na secção 12.3.5.1 do presente documento.
R0014 (PREF)	**Índice (grau) de proteção IP** Preferencialmente, o equipamento deverá garantir grau de proteção IP 55. A comprovação da satisfação deste requisito será efetuada através da realização dos ensaios descritos na secção 12.3.5.1 do presente documento.
R0015	**Grau de proteção mecânica** O invólucro do equipamento deve assegurar uma proteção mecânica que permita resistir a choques. A comprovação da satisfação deste requisito será efetuada através da realização dos ensaios descritos na secção 12.3.5.2 do presente documento.
R0016 (PREF)	**Grau de proteção mecânica** Preferencialmente, o equipamento deve apresentar uma proteção mecânica que permita resistir a choques de pelo menos 10J, ou seja não inferior ao código IK09. A comprovação da satisfação deste requisito será efetuada através da realização dos ensaios descritos na secção 12.3.5.2 do presente documento.
R0017	**Sistema de Fixação** O equipamento deverá possuir um mecanismo que permita a sua fixação numa calha DIN. Uma vez fixado deverá ser possível continuar a consultar os seus leds de sinalização, a marcação ou outro tipo de registos que contenham a sua identificação.

R0018 (PREF)	**Cor invólucro** Preferencialmente, o equipamento deve apresentar uma cor neutra, por exemplo cinzento ou bege. A cor do involucro está sujeita a aceitação pela E-REDES.
R0019	**Vida útil** A vida útil do equipamento no seu conjunto deverá ser no mínimo de 15 anos, de acordo com os critérios da norma EN 61709. Deve ser apresentado relatório detalhado dos testes ao tempo de vida útil, segundo a norma acima referida, emitido por entidade acreditada para o efeito Deverá ser fornecido informação dos componentes críticos do equipamento submetido a testes. Eventuais outros métodos de cálculo de vida útil deverão ser acordados com a E-REDES.
R0020	**Consumo** O consumo do equipamento não deve exceder, considerando a situação mais exigente de consumo para o Interface WAN Celular e todas as interfaces remanescentes ativas, em média 10W. A aceitação de valores de consumo do equipamento superiores a 10W está sujeita a aprovação da E-REDES, e ao mérito técnico da proposta global.
R0021	**Ventilação e sistema de arrefecimento** O equipamento não deve ter ventilação forçada, e nas condições de humidade atmosférica e variação de temperatura previstas, o equipamento deve garantir uma ventilação por convecção natural adequada, de forma a prevenir condensações prejudiciais no seu interior.

9.2 Propriedades Dielétricas

Requisito	Descrição
R0022	**Circuitos de entrada e saída** As entradas de alimentação e as interfaces de comunicação do equipamento devem ser isoladas galvanicamente e capazes de suportar: — a tensão de ensaio à onda de choque; — a tensão de ensaio à frequência industrial. A verificação da capacidade para suportar a tensão da onda de choque será efetuada através da realização dos ensaios descritos na secção 12.3.6.1 do presente documento. A verificação da capacidade para suportar a tensão à frequência industrial será efetuada através da realização dos ensaios descritos na secção 0do presente documento.

9.3 Condições de Alimentação

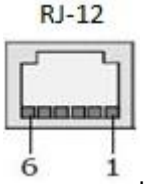
Requisito	Descrição
R0023	**Alimentação** O equipamento destina-se a ser instalado em locais cujas condições de alimentação são caracterizadas da seguinte forma: — 230 VAC, classe AC3 (-20%, +15%), de acordo com o disposto na tabela 1 e 2 da norma IEC 60870-2-1.
R0024	**Frequência** O equipamento destina-se a ser instalados em locais cujas condições de alimentação são caracterizadas da seguinte forma: — 50Hz, classe F3 (-5%, +5%), de acordo com o disposto na tabela 3 da norma IEC 60870-2-1.
R0025	**Ligação ao ponto de alimentação**

	A ligação ao ponto de alimentação deverá poder ser efetuada por intermédio de cabo e ficha adequada (i.e., a ficha de ligação não deverá estar acoplada ao equipamento), contemplando as situações em que a ligação é efetuada diretamente sobre uma régua de bornes. Deverá ser fornecido um cabo para alimentação do equipamento com as seguintes características: — Cabo H05VV-F 2x1 redondo; — Comprimento de 120cm; — 5cm descarnado em ambas as extremidades com ponteiras;
R0026	**Ligações elétricas** Os conectores devem permitir a substituição dos cabos neles ligados, sem apresentar qualquer tipo de deterioração nesse processo, ou seja, deve ser possível apertar e desapertar os cabos as vezes necessárias sem comprometer o funcionamento do equipamento As ligações elétricas, no equipamento, devem ser realizadas por intermédio de conectores apropriados, que devem permitir preferencialmente em caso de necessidade a sua rápida substituição. Estes conectores deverão permitir uma conexão estável.
R0027 (PREF)	**Last/Dying Gasp (Preferencial)** O equipamento em caso de perda de alimentação, deve ser capaz de detetar e comunicar o alarme de falha de alimentação. Esta ação deverá ser considerada evento, e consequentemente registadas em log (com identificação da causa).

9.4 Dimensões

Requisito	Descrição
R0028	**Dimensões máximas** Em virtude das condições existentes nos locais de instalação, o equipamento deverá ter as seguintes dimensões máximas, em mm: — 145 x 195 x 85 mm (Largura x Altura x Profundidade). A aceitação de valores superiores está sujeita a aprovação da E-REDES, e ao mérito técnico da proposta.

9.5 Interface série

Requisito	Descrição
R0029	**Interface série RS485** O equipamento deve apresentar uma interface série TIA-EIA-485, também designado RS485, que permita estabelecer comunicação local.
R0030 (PREF)	**Interface série RS485 – Tipo de conector (Preferencial)** A interface série RS485 deve possuir um conector RJ12 (fêmea) de acordo com a figura seguinte: 
R0031 (PREF)	**Interface série RS485 – *Pinout* dos conectores (Preferencial)** O *pinout* do conector deverá estar de acordo com a tabela seguinte:

Pino 1	Pino 2	Pino 3	Pino 4	Pino 5	Pino 6

Requisito	Descrição
	<table><tr><td>GND</td><td>A (+)</td><td>B (-)</td><td>B (-)</td><td>A (+)</td><td>----</td></tr></table>
R0032	**Interface série RS485 – Adaptador externo** Caso a interface série RS485 nativa do equipamento possua um conector de tipo distinto do indicado no requisito R0030, ou que não cumpra o *pinout* referido no requisito R0031, deverá ser fornecido um adaptador externo para garantir a conversão do tipo de conector e respetivo *pinout*. O adaptador externo deve ser de material isolante.
R0033	**Interface série RS485 – Modo de comunicação** A interface RS485 deverá funcionar em modo *half-duplex*.
R0034	**Interface série RS485 – Robustez de comunicação** O dispositivo deve ser concebido de forma a evitar ruído e flutuações de tensão durante a comunicação no barramento RS485.
R0035	**Interface série RS485 – Parâmetros de comunicação** Deve ser possível configurar, local e remotamente, os parâmetros de comunicação da interface série RS485: — Velocidade de comunicação; — *Data bits, Parity bits, Stop bits* (tipicamente 8N1); — Tempo de inatividade (*timeout*). Poderá adicionalmente disponibilizar *Flow Control*, devendo nesse caso permitir a sua configuração: SW, *None*.
R0036	**Interface série RS485 – Velocidade de comunicação** A interface RS485 deverá apresentar uma velocidade por omissão de 9600 bps. A interface RS485 deverá permitir comunicar com uma velocidade máxima de, pelo menos, 19200 bps. Preferencialmente, a interface RS485 deverá permitir comunicar com uma velocidade máxima de, pelo menos, 115200 bps.
R0037 (PREF)	***Gateway* série** Preferencialmente, o equipamento deve implementar a função de *serial gateway*, entre a secção "*HDLC over RS485"* e a secção "*HDLC over TCP*", e o protocolo PPP de modo transparente, tal como indicado na **Error! Reference source not found.**. Caso o equipamento não cumpra nativamente esta funcionalidade, deve ser possível adiciona-la através de uma atualização remota de Firmware.
R0038 (PREF)	**Parâmetros de Configuração da *Gateway* Série** Preferencialmente, o equipamento deve permitir a configuração dos parâmetros relevantes para o segmento "*HDLC over TCP*": — Tamanho máximo do pacote TCP; — *Time-out* para envio do pacote TCP; — *Idle-time* da sessão TCP; — *Keep-alive* da sessão TCP; O equipamento deve permitir a configuração do porto de escuta da interface série.
R0039 (PREF)	**Terminação do barramento RS485 (Preferencial)** Preferencialmente, o equipamento deve permitir a configuração de terminação do barramento RS485 (ON, OFF; tipicamente OFF). Deverá ser possível efetuar esta configuração por software.
R0040 (PREF)	**Gestão de acesso ao barramento RS485**

Requisito	Descrição
	Preferencialmente, o equipamento deve implementar a gestão de acesso ao barramento RS485 de modo a que, do ponto de vista da camada HDLC, uma única *Primary Station* remota possa aceder, num dado instante temporal e no decurso da respetiva comunicação, ao barramento RS485 onde estão fisicamente conectados os contadores. Desejavelmente esta gestão de acesso deve ser implementada através da configuração do número máximo de sessões TCP que será possível estabelecer, em simultâneo, para a *Gateway* da interface série RS485. Para a utilização prevista deste equipamento, o referido limite será igual a 1.

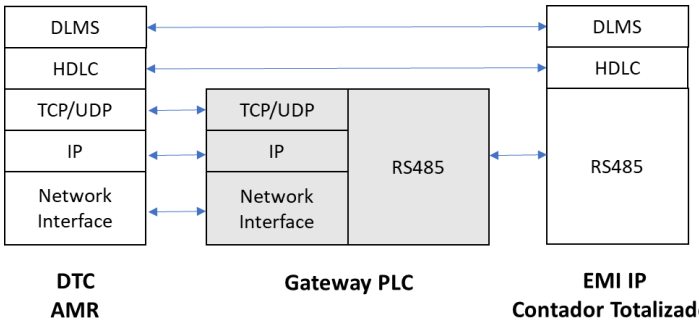


Figura 6 – Diagrama das camadas de protocolos para a implementação do *serial gateway*

9.6 Interface Ethernet

Requisito	Descrição
R0041	**Interface Ethernet** O equipamento deve apresentar uma interface Ethernet sobre cabo de par entrelaçado, 10/100BASE-T(X), de acordo com a norma 802.3 do IEEE.
R0042	**Interface Ethernet – Tipo de conector** A interface Ethernet deve possuir um conector RJ45 (fêmea).
R0043	**Interface Ethernet – Funcionalidade Base** A interface Ethernet deve suportar auto-negociação e auto-MDI.
R0044	**Interface Ethernet – LAN** A interface Ethernet deve poder ser utilizada como LAN, quando ligada a um dispositivo externo que não possua tecnologia de comunicação remota, p.e Controlador IP.
R0045	**Interface Ethernet – WAN** A interface Ethernet deve poder ser utilizada como WAN, quando ligada a um dispositivo de comunicação externo, p.e um router.
R0046	**Interface Ethernet – Protocolo IP** A interface Ethernet deve suportar IPv4. Preferencialmente, deverá suportar também IPv6.
R0047	**Interface Ethernet – IP fixo** A interface Ethernet deverá funcionar com IP fixo, sendo possível configurar o endereço IP, *subnet mask* e *default gateway*. Esta funcionalidade deve estar disponível quando a interface Ethernet estiver a ser utilizada como WAN ou LAN.
R0048	**Interface Ethernet – IP dinâmico**

Requisito	Descrição
	A interface Ethernet deverá suportar funcionar com IP dinâmico. O equipamento deve disponibilizar um cliente DHCP, de forma a receber um endereço IP dinâmico atribuído por equipamento de comunicação externo ligado na porta Ethernet. A interface Ethernet deverá disponibilizar um servidor DHCP, de forma a atribuir endereços IP dinâmicos aos equipamentos ligados na porta Ethernet.

9.7 Interface PLC

Requisito	Descrição
R0049	**Interface PLC PRIME** O equipamento deve apresentar uma interface de comunicação PLC PRIME, que permita estabelecer comunicação com os EMI PLC PRIME, instalados na sua rede de baixa tensão. Deverá ser possível comunicar com os diversos modelos de EMI PLC PRIME homologado pela E-REDES. Os EMI, monofásicos e trifásicos, regem-se funcionalmente pelos documentos DEF-C44-506/N e DEF-C44-507/N.
R0050	**Interface PLC PRIME – Protocolo** O equipamento deverá suportar o protocolo PLC PRIME v1.3.6.
R0051 (PREF)	**Interface PLC PRIME – Protocolo adicional (Preferencial)** Adicionalmente à versão v1.3.6, preferencialmente o equipamento deve suportar o protocolo PLC PRIME v1.4. Caso o equipamento suporte o protocolo v1.3.6 e v1.4 deverá ser possível definir o protocolo em uso.
R0052	**Interface PLC PRIME – Modo de funcionamento** O equipamento deverá funcionar como *Base Node* ou *Service Node* na arquitetura de rede PLC PRIME.
R0053	**Interface PLC PRIME – Dimensão rede PLC PRIME** O equipamento deve permitir o estabelecimento de uma rede PLC PRIME de pelo menos 100 EMI, quando estiver a operar como *Service Node* ou *Base Node*.
R0054 (PREF)	**Interface PLC PRIME – Dimensão rede PLC PRIME (Preferencial)** Preferencialmente, o equipamento deve permitir o estabelecimento de uma rede PLC PRIME de pelo menos 200 EMI, quando estiver a operar como *Service Node* ou *Base Node*.
R0055	**Interface PLC PRIME – Injeção sinal PLC PRIME** A interface PLC PRIME deverá apresentar injeção monofásica do sinal PLC PRIME.
R0056 (PREF)	**Interface PLC PRIME – Injeção sinal PLC PRIME, escolha de fase (Preferencial)** Preferencialmente, o equipamento deverá permitir definir, por software, em qual das fases é injetado o sinal PLC PRIME.
R0057 (PREF)	**Interface PLC PRIME – Injeção trifásica sinal PLC PRIME (Preferencial)** O equipamento deverá apresentar injeção trifásica do sinal PLC PRIME. O equipamento deverá permitir definir, por software, se a injeção do sinal PLC é monofásica ou trifásica.
R0058	**Topologia rede PLC PRIME** Deverá ser possível consultar a árvore de EMI, via FTP ou HMI, quando o equipamento estiver configurado como *Base Node*.

9.8 Interface Celular

Requisito	Descrição
R0059	**Interface Celular** O equipamento deverá apresentar interface celular que disponibilize acesso remoto sobre uma rede móvel terrestre com comutação de pacotes. A ligação referida deve ser estabelecida em modo contínuo, always on, pelo que o equipamento deve garantir, através de mecanismos intrínsecos, a estabilidade e continuidade da mesma.
R0060 (OPC)	**Interface Celular – módulos radio (opcional)** Opcionalmente, a interface celular poderá ter 2 módulos rádio independentes.
R0061	**Interface Celular – Tecnologia** O equipamento deverá suportar cumulativamente GPRS, EDGE, UMTS, HSPA, HSPA+, LTE CAT1. O equipamento deve permitir a seleção, quer dinâmica quer estática, da tecnologia. Adicionalmente, o débito efetivo deverá estar otimizado para cada tecnologia (de acordo com as normas aplicáveis e em vigor, nomeadamente do 3GPP), especialmente no sentido uplink (ex: suporte de multi-slot class 12 para GPRS, …), de modo a que se possa maximizar o canal de comunicações para a aplicação em questão.
R0062 (PREF)	**Interface Celular – Tecnologia (Preferencial)** Preferencialmente, o equipamento deverá suportar cumulativamente EDGE, UMTS, HSPA, HSPA+, LTE CAT1 e LTE CAT4. O equipamento deve permitir a seleção, quer dinâmica quer estática, da tecnologia. Adicionalmente, o débito efetivo deverá estar otimizado para cada tecnologia (de acordo com as normas aplicáveis e em vigor, nomeadamente do 3GPP), especialmente no sentido uplink (ex: suporte de multi-slot class 12 para GPRS, …), de modo a que se possa maximizar o canal de comunicações para a aplicação em questão.
R0063	**Interface Celular - Banda de operação** A interface celular deverá suportar todas as bandas de frequência licenciadas para Portugal (800/900/1800/2100/2600 MHz). — As frequências de transmissão devem estar alocadas, respetivamente, nas janelas: 832-862/880-915/1710-1785MHz/1920-1980/2510-2570 MHz. — As frequências de receção devem estar alocadas, respetivamente, nas janelas: 791-821/925-960/1805-1880/2110-2170/2570-2690 MHz. Para a tecnologia LTE o equipamento deverá suportar pelo menos as bandas B1 (2100MHz), B3 (1800MHz), B7 (2600MHz), B20 (800MHz).
R0064 (PREF)	**Interface Celular – Operador (Preferencial)** Preferencialmente, o equipamento deverá permitir gerir a seleção, quer dinâmica quer estática, de operador.
R0065	**Interface Celular – Protocolo IP** A interface WAN deve suportar IPv4. Preferencialmente, deverá suportar também IPv6.
R0066	**Interface Celular – Monitorização** Deve ser possível verificar o nível (RSSI) e qualidade (BER) de sinal celular disponibilizado ao longo do tempo. Adicionalmente deve ser apresentado o operador de rede, a célula e a tecnologia associada. Deverá ser possível configurar os parâmetros de monitorização da qualidade e nível de sinal. Esta informação deve estar disponível quer no Gestor de Elemento quer no Gestor de Rede.
R0067	**Cartão SIM – Formato** O equipamento deverá suportar o formato Mini-SIM (2FF).

Requisito	Descrição
R0068 (PREF)	**Cartão SIM – Formato (Preferencial)** O equipamento deverá suportar Dual SIM, devendo um dos cartões funcionar como backup em caso de mau funcionamento da interface celular principal. Neste contexto o equipamento deve permitir gerir a seleção, quer dinâmica quer estática, de cartão SIM.
R0069	**Cartão SIM – Interface** O equipamento deve dispor de interface mecânica para colocação/remoção do cartão SIM que otimize o compromisso entre facilidade de acesso e segurança/robustez. Preferencialmente, a sua localização não deverá implicar a abertura e fecho do invólucro para execução das ações de colocação/remoção. Se a colocação/remoção do cartão SIM implicar a abertura e fecho do invólucro, deverá ser garantido que o acesso ao interior do equipamento e aos seus componentes é limitado, e que não constitui um perigo para o operador. Deverá ainda ser garantido que a ação de abertura e fecho do invólucro para colocação do cartão SIM não inviabiliza a garantia do equipamento.
R0070	**Cartão SIM – Aplicações SIM/USIM** O equipamento deve suportar cartões com aplicações SIM de acordo com a norma STK, SIM Application Toolkit, e USAT, USIM Application Toolkit, de acordo com a norma ETSI 102.223.
R0071	**Comandos AT** O equipamento deve suportar comandos AT remotos via SMS, de acordo com as normas aplicáveis e em vigor (3GPP TS 27.007 e 3GPP TS 27.005), que permitam atuar como ferramenta de último recurso para recuperação remota da Interface WAN Celular caso todos os outros mecanismos de nível superior (Gestor de Rede/Elemento, Watchdog, Mecanismos “always on”, …) falhem. Exemplos de comandos AT passiveis de serem realizados remotamente: — Reboot do módulo radio e total; — Comando para testar conectividade; — Configuração da APN e todos os seus parâmetros — Consulta das configurações da APN — Consulta de modelo do módulo de comunicações, versão firmware e outra informação — Consulta do IP do equipamento Adicionalmente, deve disponibilizar uma White List configurável dinamicamente de modo a definir e controlar os números autorizados a enviar comandos AT (os restantes deverão ser descartados). A White List deverá suportar no mínimo dois números. O fabricante poderá propor uma solução alternativa, mas funcionalmente equivalente, para cumprir este requisito. Qualquer solução alternativa terá que ser validada previamente pela E-REDES.
R0072	**Funcionalidade OTA** O equipamento deve suportar a funcionalidade OTA.
R0073	**Conector Antena** A interface celular do equipamento deve possuir 1 conetor SMA para ligação de uma antena externa.
R0074 (PREF)	**Diversidade espacial (Preferencial)** Preferencialmente, o equipamento deverá permitir diversidade espacial com pelo menos duas antenas, para maximizar a qualidade da comunicação rádio, mitigando problemas de multipath causados por reflexões do sinal. Para o efeito, o equipamento deverá possuir um conector SMA fêmea, para ligação de cada uma das antenas. As interfaces SMA deverão estar devidamente identificadas como primária e auxiliares

Requisito	Descrição
R0075	**Antena** O equipamento deve apresentar uma antena com as seguintes características: — Tipo omnidireccional; — Multibanda 800/900/1800/2100/2600 MHz (como definido no requisito R0063); — Ganho mínimo de 2 dBi; — Eficiência superior a 50%; — VSWR (Voltage Standing Wave Ratio) inferior a 2.5:1; — Em virtude das condições existentes nos locais de instalação, o elemento de antena deverá ter uma dimensão máxima de 22 x 275 (Diâmetro da Base x Altura em mm); — Cabo integrado com comprimento de 3 m (atenuação inferior a 0.85 dB/m @2GHz, eficiência superior a 75%, raio mínimo de curvatura de 25mm); — Conector SMA (fêmea na Gateway e macho na terminação do cabo da antena); — Impedância de 50 ohm; — Estrutura de suporte e fixação revestida com material isolante. A distância do elemento de antena à zona de fixação, que deverá otimizar a qualidade do sinal celular, deve estar compreendida no intervalo [10 … 30] cm. Desejavelmente deve estar preparada para suportar, sem impacto na posição inicial de instalação da antena, os constrangimentos associados a eventual instalação exterior (nomeadamente rajadas de vento até 150 km/h, tempestades de granizo, etc.), maximizando em paralelo a proteção contra vandalismo; — Deve possuir, no mínimo, IP 65.

9.9 Interface de engenharia

Requisito	Descrição
R0076	**Interface de engenharia** Para o acesso local, deverá ser disponibilizado uma interface de engenharia - interface Ethernet ou em alternativa porta de consola série - para executar os serviços de engenharia. Deverá ser possível aceder ao equipamento, para efeitos de reinicialização, configuração, consulta de informação, recolha de eventos e alarmes, execução de comandos, diagnóstico e atualização de firmware. O acesso poderá ser feito usando a interface gráfica (HMI) com privilégios de administração do equipamento ou através da linha de comandos usando metodologia "*command-line interface*".
R0077	**Interface de engenharia – Protocolo** Para o acesso à interface de engenharia através da linha de comandos deve ser usado o protocolo SSH. Para o acesso à interface de engenharia através da interface HMI deve ser usado o protocolo HTTP ou HTTPS. O equipamento deverá permitir a configuração integral de todos os parâmetros de configuração e gestão do equipamento, através da interface HMI e linha de comandos.

9.10 LEDs

Requisito	Descrição
R0078	**LEDs de sinalização** O equipamento deve apresentar LEDs, visíveis após fixação e ligação à alimentação, para sinalização do seu funcionamento. Deverá ser possível observar, pelo menos, e por intermédio de um ou mais LEDs, os seguintes estados de operação: — equipamento alimentado; — equipamento registado na rede WAN celular do operador;

	— indicação de nível de sinal celular; — Indicação de presença de cartão SIM; — indicação de funcionamento da interface PLC PRIME; — indicação de funcionamento da interface Ethernet; — indicação de funcionamento da interface série RS485. O fabricante poderá propor uma solução alternativa, mas funcionalmente equivalente, para cumprir este requisito. Qualquer solução alternativa terá que ser validada previamente pela E-REDES.

10 CARACTERISTICAS FUNCIONAIS

10.1 Networking

Requisito	Descrição
R0079 (PREF)	**Routing** Preferencialmente, o equipamento deve suportar routing IPv4, estático e dinâmico (distance vector e link state). Relativamente ao último, os protocolos a observar são respetivamente: RIP, e OSPF.
R0080 (PREF)	**VPN** Preferencialmente, o equipamento deve suportar: — IPSec/GRE e DMVPN (multi-GRE e NHRP) de acordo com as RFCs aplicáveis e em vigor; — A configuração dos parâmetros aplicáveis, nomeadamente: o Tecnologia de encriptação de dados AES128, AES-192 e AES256 e NULL para IKE Phase I e II IKEv2; o Tecnologia de suporte à Integridade dos Dados SHA256, SHA384, SHA512 e NULL; o Keying (Assimétrica, Simétrica e PSK); o Certificados Digitais - X.509 Compliance; o Diffie-Hellman: Group 1 (768 bit), Group 2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit); o VPN IPSEC Site to Site Full Mesh (all to all) ou Star (Remote to center); o Suporte de IKE com PKI e pre-shared Secret; o SCEP certificate enrollment and certificate renewal; o Pre-installed MIC certificate, from vendor CA (MIC = Manufacturer Installed Certificate). Adicionalmente, deverá estar preparado para integração numa Public Key Infrastructure (PKI).
R0081 (PREF)	**VPN – Requisitos para Integração com Concentrador VPNs** Preferencialmente, o equipamento deve conter nativamente uma configuração pré-instalada, assim como um certificado de aprovisionamento emitido pelo fabricante - MIC certificate, from vendor CA (MIC = Manufacturer Installed Certificate); Deve permitir uma ordem remota para comissionamento, a instalação remota de tabelas de NAT e respetiva configuração SCEP - Simple Certificate Enrollment Protocol - SCEP certificate enrollment; Deve ter capacidade para, após efetuar com sucesso o SCEP enrollment do certificado de produção, estabelecer uma nova ligação VPN com novo certificado de produção.
R0082 (PREF)	**VLAN** Preferencialmente, deve suportar a implementação de VLANS de acordo com a norma 802.1Q do IEEE – VLAN Tagging.
R0083 (PREF)	**QoS** Preferencialmente, deve permitir, para todas as interfaces internas/lógicas e externas/físicas, a implementação avançada (correlação dinâmica destino/origem quer para a camada de rede, quer para a camada de transporte) de estratégias de QoS de acordo com as recomendações aplicáveis nomeadamente do grupo de trabalho 802.1p do IEEE.

Requisito	Descrição
	As políticas associadas serão especialmente relevantes na priorização de escoamento de tráfego através das interfaces WAN (quer Celular, quer Ethernet).
R0084 (PREF)	**QoS – Descrição** Preferencialmente, deve ser fornecida descrição explícita, para cada interface, quer internas/lógicas quer externas/físicas, das estratégias/políticas de QoS implementadas/disponíveis (nomeadamente nível/camada de implementação, número de classes, …).
R0085 (PREF)	**NAT/PAT** Preferencialmente, o equipamento deve suportar NAT/PAT (outbound). Adicionalmente, deve suportar NAT (outbound/inbound) com um número de entradas na tabela respetiva, bem como de endereços de loopback, no mínimo igual ao número de portos Ethernet do equipamento em questão.
R0086	**Protocolos** O equipamento deverá suportar no mínimo os seguintes protocolos: IP, TCP, UDP, ICMP, HTTP, HTTPS, FTP, FTPS (em alternativa SCP ou SFTP), SSH, Telnet, SNTP, SNMPv2c e SNMPv3.
R0087 (PREF)	**Bridge** Preferencialmente, deve suportar a criação de interfaces Bridge, interfaces de Routing/NAT.

10.2 Autodiagnóstico

Requisito	Descrição
R0088	**Watchdog** O equipamento deverá possuir mecanismos de watchdog, que monitorizem o seu estado, por software e/ou hardware (preferencialmente), tomando ações em caso de mau funcionamento, tais como: — reinicialização de uma função do equipamento; — reinicialização do equipamento. Deve ser registado os eventos associados.
R0089 (PREF)	**Diagnóstico de arranque** Preferencialmente, o equipamento deve implementar mecanismo de autodiagnóstico de arranque, que permita, logo após ser alimentado, identificar eventuais problemas com os seus diversos módulos e interfaces. Devem ser registados todos os eventos associados.
R0090 (PREF)	**Monitorização do estado do equipamento** Preferencialmente, o equipamento para efeitos de monitorização remota, deve ter informação que permita caracterizar: — Estado de cada um dos blocos funcionais (operacional ou não operacional); — Estado das interfaces com o exterior (interfaces de comunicações, etc.); Existência de erros internos do equipamento.
R0091	**Reinicialização periódica e automática** Deve ser garantida a existência de mecanismos de reinicialização periódica e automática do equipamento, os quais, desejavelmente, deverão estar disponíveis e ativos mesmo em situações de falha do software. Estas ações deverão ser consideradas eventos, e consequentemente registadas em log (com identificação da causa).

10.3 Eventos e Relógio

Requisito	Descrição
R0092	**Registo de eventos** O equipamento deve registar e armazenar eventos em memória não volátil, identificados com data, hora, minuto e segundo de ocorrência. Os eventos devem ser armazenados no log de eventos, o qual deverá estar associado, para envio, a um servidor Syslog.
R0093	**Log de eventos** O log de eventos do equipamento deverá dispor de uma capacidade de armazenamento nunca inferior a 100 eventos. Os eventos devem ser armazenados por ordem cronológica de sua geração, e uma vez atingida a capacidade máxima de armazenamento, deverá ser guardado os eventos mais recentes e descartado os mais antigos (*First In, first out).*
R0094	**Lista de eventos** O fabricante deverá fornecer uma listagem de todos os eventos gerados pelo equipamento
R0095	**Erros internos** Deve prever a deteção de erros internos do equipamento como resultado de auto-avaliações ao seu funcionamento (ex: testes à memória), resultando na ocorrência dos respetivos eventos.
R0096	**Alarmes** Deve ter a capacidade para gerar alarmes como consequência da ocorrência de eventos. Por exemplo através do envio de Traps SNMP para um NMS.
R0097	**Data e hora** O equipamento deverá dispor de relógio interno para registo cronológico de eventos, caso a sincronização externa, através de servidor NTP não esteja disponível. O RTC interno deve ter a capacidade, no mínimo, de discriminar e apresentar valores do tempo até ao segundo. Deverá ser possível executar o acerto do relógio.
R0098	**Data e hora – Sincronização por sistema externo** O relógio do equipamento deverá poder ser sincronizado com um sistema externo através do protocolo NTP ou SNTP.
R0099	**Data e hora – Resolução calendário** O equipamento deverá possuir um calendário perpétuo, incluindo dia do mês, mês e ano (4 dígitos). Deve ser possível executar o acerto do calendário.

10.4 Comunicações

Requisito	Descrição
R00100	**Comunicação DTC** O equipamento deve suportar a comunicação com o DTC virtual (Mega DTC) ou DTC físico, com o perfil de comunicação adequado ao modo de funcionamento em que se encontra, ou seja, *Service Node* ou *Base Node.*
R00101	**Comunicação com DTC - *Service Node*** O equipamento no modo *Service Node* deve estabelecer comunicação com o DTC via UDP/IP. O equipamento deve possibilitar o envio e receção de mensagens do protocolo PLC PRIME via UDP/IP.
R00102	**Comunicação com DTC - *Base Node***

	O equipamento no modo *Base Node* deve estabelecer comunicação com o DTC via TCP/IP. O equipamento deve possibilitar o envio e receção de mensagens do protocolo PLC PRIME via TCP/IP.
R00103	**Comunicação – Interface PLC PRIME** O equipamento deve possibilitar a comunicação entre o DTC e os EMI PLC ligados através da interface PLC PRIME. O equipamento deve implementar a função de PLC *gateway*, tal como indicado na Figura **7**. Os EMI PLC, monofásicas e trifásicas, regem-se funcionalmente pelos documentos DEF-C44-506/N e DEF-C44-507/N.
R00104	**Exploração da Infraestrutura de EMI** O equipamento deverá permitir a realização de tarefas programadas, ordens e serviços, sobre os EMI.
R00105	**Deteção automática de EMI em PLC PRIME** O equipamento deverá ser capaz de detetar de forma automática os EMI que se ligam à rede através da tecnologia PLC PRIME (Plug&Play) e gerir de forma autónoma o seu registo e o fim do seu registo.
R00106	**Eventos espontâneos** O equipamento deverá permitir enviar de forma espontânea para montante, por UDP/IP ou TCP/IP, os eventos espontâneos gerados pelos EMI PLC PRIME.
R00107	**Informação sobre a topologia da rede PLC** O equipamento quando a operar como *Base Node* deve apresentar, de uma forma gráfica no HMI, a topologia da rede PLC PRIME em tempo real, com identificação de todos os nós da rede, sua dependência hierárquica e estado funcional de cada equipamento de rede (terminal, *switch*, etc). O equipamento deve ter a capacidade para permitir forçar um refrescamento total da topologia da rede PLC PRIME, obrigando a novo registo de todos os EMI com tecnologia PLC PRIME. Esta funcionalidade deve estar também disponível na interface HMI.
R00108	**Protocolo de comunicação entre DTC e Gateway PLC – *Service Node*** Deve ser implementado o protocolo de comunicação entre o DTC e a Gateway PLC, com base no definido no documento "PRIME_AuxiliaryNodesConnectivityProposal_v1-121126" da Prime Alliance para este tipo de interface, quando o equipamento estiver a operar como *Service Node.* Para mais detalhe consultar anexo I da especificação técnica DEF-C98-405/N.
R00109	**Protocolo de comunicação entre DTC e Gateway PLC – *Base Node*** Deve ser implementado o protocolo de comunicação entre o DTC e a Gateway PLC, com base no definido no documento "TCP transport layer for DLMS: extension for optimal multiplexing 4-32 connections" da Prime Alliance, quando o equipamento estiver a operar como *Base Node.* Para mais detalhe consultar anexo J da especificação técnica DEF-C98-405/N.

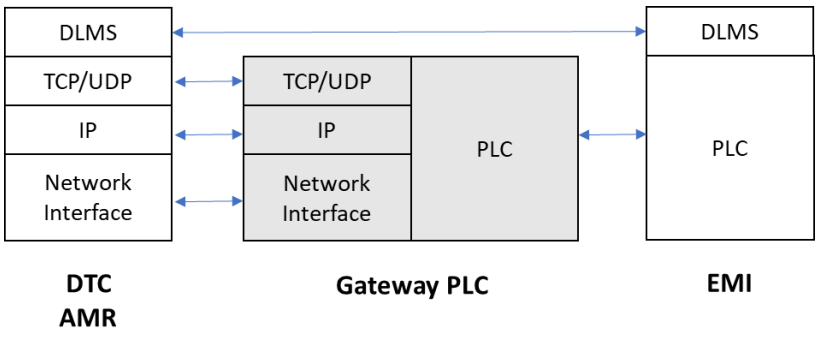


Figura 7 – Diagrama das camadas de protocolos para a implementação do *PLC gateway*

10.5 Gestão de Comunicações

Requisito	Descrição
R00110	**Monitorização das comunicações** Para efeitos de gestão das comunicações, deve ser possível efetuar o respetivo trace em profundidade nas diversas interfaces de comunicação. Os eventos de comunicações devem poder ter registo em log próprio, com detalhe efetivo das comunicações, este deverá estar associado, para envio, a um servidor Syslog. Esta informação deve estar disponível quer no Gestor de Elemento quer no Gestor de Rede.
R00111	**Reset informação estatística** Deve ser possível efetuar a reinicialização unitária ou total da informação estatística relativa às comunicações. Esta funcionalidade deve estar disponível quer no Gestor de Elemento quer no Gestor de Rede.

10.6 Gestor de Elemento

Requisito	Descrição
R00112	**Disponibilização** O equipamento deve disponibilizar uma ferramenta de configuração web, com acesso local e remoto, respeitando os requisitos de cibersegurança da E-REDES. O HMI deverá ser amigável do ponto de vista da sua utilização.
R00113	**Língua** O HMI deverá utilizar a língua portuguesa ou inglesa.
R00114	**Menus** O HMI terá aspeto gráfico, funcionando por menus. Deverão ser disponibilizados menus com capacidade para a configuração do equipamento, consulta de informação, efeitos de reinicialização, recolha de eventos e alarmes, execução de comandos, diagnóstico e atualização de firmware.
R00115	**Perfil de acesso** Devem existir os seguintes perfis de acesso ao HMI, protegidos por user e password, respeitando os requisitos de cibersegurança da E-REDES: — Consulta; — Configuração.
R00116	**Perfil de Consulta** Através do perfil de consulta deve ser possível realizar apenas leituras de informação, não podendo adicionar, editar, remover ou alterar nenhuma configuração, nem atualizar firmware. Deverá ser possível ler a informação disponibilizada através do perfil de configuração, e indicada no requisito R00117.
R00117	**Perfil de Configuração** Através do perfil de configuração deve ser possível ler e/ou alterar pelo menos a seguinte informação: — Identificação do equipamento e respetivas coordenadas geográficas; — Gestão dos perfis de acesso ao HMI; — Configurações de sessão (Preferencial); — Data e hora (Time zone) (Preferencial); — Reinicialização periódica do equipamento (Preferencial); — Eventos (Preferencial); — Configurações interface Ethernet (IP Fixo, máscara, DHCP, etc);

	— Configurações Interface WAN celular (ativar/inibir, SIM prioritário, ativar/inibir dual SIM, parâmetros qualidade e nível de sinal, configurações cartão SIM, default route, ping keep alive, e túneis); — Configurações PRIME (ativar/inibir, modo de operação, fase injeção sinal, IP e porto DTC, etc); — Configurações portas séries (velocidade, porto TCP, Data bits, Parity bits, Stop bits, etc); — Routing estático e dinâmico, se aplicável; — Configuração VPN (Tuneis, IKE policies, Preshared keys, IPSec, etc), se aplicável; — Agente e Traps SNMP; — Servidor NTP; — Acessos TACACS+ (Preferencial). Através do perfil de configuração deve ser possível consultar: — a informação estatística das interfaces de comunicações (WAN, Ethernet, interfaces série, interface PLC PRIME, Routing e VPN); — Informação estatística de utilização de memoria e CPU; — Informação da topologia da rede PLC (Nível na rede, Número de série, Mac address, tecnologia, estado, LNID, SID, tempo ligado, % tempo ligado, etc). Através do perfil de configuração deverá ser possível executar os comandos seguintes: — Reset de estatísticas de comunicação (Preferencial); — Upload de ficheiro de configuração; — Download de ficheiro de configuração; — Atualização de firmware; — Reboot ao equipamento. Deverá cumprir o especificado no Anexo B do presente documento.

10.7 Gestor de Rede

Requisito	Descrição
R00118	**Protocolo SNMP** O equipamento deve suportar o protocolo SNMP, que deverá monitorizar as variáveis de sistema incluindo cada uma das interfaces existentes (Ethernet, RS485, PLC PRIME, etc). O agente SNMP deverá implementar o protocolo SNMPv2c e SNMPv3, de modo a sustentar a integração com o Sistema Central de Gestão Transversal, Gestor de Rede Transversal, existente na plataforma de Gestão de Rede da E-REDES.
R00119	**Acessos SNMP** O equipamento deve permitir definir uma *community string* e/ou password de acesso à informação.
R00120	**Management Information Base** O equipamento deve possuir uma MIB dinâmica, com capacidade de adaptação para incorporar evoluções futuras. Do conteúdo da MIB deverão constar pelo menos os seguintes OIDs: — Modelo do equipamento; — Número de série do equipamento; — Código de modelo (atribuído pela E-REDES); — Versão de firmware; — Tempo de Uptime; — Memória em uso (percentual); — IMEI do equipamento; — ICCID do cartão SIM; — Tecnologia de rede WAN em utilização; — Informação do operador;

	— Informação do CELL ID à qual está ligado; — Nível de sinal. O fabricante deverá fornecer a MIB implementada no equipamento. O conteúdo final da MIB deverá ser definido pela E_REDES.
R00121	**Envio de *traps* SNMP** O equipamento deverá permitir a aquisição de OID e o envio de *traps* SNMP.
R00122	**Sistema Central de Gestão Transversal** O equipamento deve poder ser integrado no Sistema Central de Gestão Transversal, Gestor de Rede Transversal, existente na plataforma de Gestão de Rede da E-REDES.
R00123 (PREF)	**Sistema Central de Gestão Proprietário** Preferencialmente, deve ser disponibilizado um Sistema Central de Gestão proprietário, Gestor de Rede, que permita implementar uma estratégia clássica FCAPS. Este poderá, ou não, ser integrado com o Sistema Central de Gestão Transversal existente na plataforma de Gestão de Rede da E-REDES (pelo que deverá disponibilizar interface de integração a nível de sistema). Deverá ser possível gerir os equipamentos com o Gestor de Rede disponibilizado, sem encargos adicionais (licenciamento ou outra natureza), durante pelo menos o tempo de vida útil definido para o equipamento no R0019.
R00124 (PREF)	**Configuração em massa** Preferencialmente, deverá ser disponibilizada uma ferramenta que permita automática e centralmente configurar os equipamentos já instalados fisicamente. No mínimo deverá permitir o carregamento remoto de uma configuração base em ficheiro de texto ou similar (provisionamento automático por scripting). Também deverá ser possível efetuar o upgrade de firmware dos equipamentos de forma massiva, individual ou em conjuntos pré-definidos.
R00125 (PREF)	**Requisitos de segurança do Gestor de rede** Preferencialmente, o gestor de rede fornecido deverá cumprir integralmente os requisitos de segurança e arquitetura definidos no documento "SGSI-IIMC SPEC 01-Cybersecurity Requirements for Applications_V_NMS".

10.8 Firmware e Configuração

Requisito	Descrição
R00126	**Atualização Firmware** Deve ser possível a atualização de firmware do equipamento, local e remotamente, por carregamento de novas versões.
R00127	**Validação Firmware** Antes da instalação de uma nova versão de firmware, deve validar a coerência da mesma. Esta validação deve garantir que o ficheiro com a nova versão de firmware está completo e não corrompido, possuindo todos os blocos necessários.
R00128 (PREF)	**Mecanismos de recuperação** Preferencialmente, em caso de falha ou erro na atualização de firmware, o equipamento deve ter mecanismos que permitam manter ou repor a versão anterior do mesmo.
R00129 (PREF)	**Registo da atualização de Firmware** Preferencialmente, o equipamento deve registar, através de evento próprio, cada atualização de firmware que lhe é realizada, devendo ser registada informação da versão introduzida, data e hora de atualização.
R00130	**Informação a preservar**

	Na atualização de firmware deve ser garantido que não é eliminada ou alterada a informação armazenada, bem como todos os parâmetros de configuração do equipamento.
R00131	**Ficheiro de configuração** Deverá ser possível efetuar o download do ficheiro de configuração do equipamento. Deverá ser possível a alteração dos parâmetros de configuração do equipamento através do upload de um ficheiro de configuração.

10.9 Segurança

Requisito	Descrição
R00132	**Perfil de acesso** Deve existir pelo menos dois perfis de acesso ao equipamento, protegidos por user e password, tanto no acesso local como remoto, via Gestor de Rede ou Gestor de elemento: — Perfil consulta - Deverá permitir apenas a leitura de informação, não podendo adicionar, editar, remover ou alterar nenhuma configuração, nem atualizar firmware; — Perfil de configuração - Deverá permitir a leitura e escrita de informação, podendo adicionar, editar, remover ou alterar as configurações e atualizar firmware.
R00133	**Password** Para cada nível de acesso deve existir uma palavra-chave, que deverá ser autenticada em cada sessão de comunicação local ou remota que seja estabelecida com o equipamento. O equipamento deve permitir a definição de morfologia da password. Para efeitos considerem-se os seguintes requisitos como obrigatórios: — Número máximo de espaços internos: 0 — Máximo de repetitivos: 3 — Máximo de sequências: 3 — Número mínimo de caracteres: 8 — Número mínimo de regras de tipo de caracteres que devem passar: 3 a) Número mínimo de caracteres alfabéticos maiúsculos: 1 b) Número mínimo de caracteres alfabéticos minúsculos: 1 c) Número mínimo de caracteres numéricos: 1 d) Número mínimo de caracteres especiais: 1 i. Os caracteres especiais são: @#$%&*()_+=-{}[]|\:";'<>,./ Todas as entradas com sucesso, assim como as tentativas de entrada sem sucesso, devem ser devidamente registadas através de eventos próprios.
R00134 (PREF)	**Firewall** Preferencialmente, o equipamento deve implementar por software, desejavelmente por hardware, firewall interna com capacidade de controlo avançado das camadas 3 (Rede/IP) e 4 (Transporte/TCP, UDP).
R00135	**Autenticação Centralizada** Deve ser considerado a possibilidade de autenticação e autorização centralizada, através do protocolo TACACS+ ou RADIUS.
R00136 (PREF)	**Cibersegurança** Preferencialmente, o equipamento deverá cumprir os requisitos de cibersegurança disposto no anexo A do presente documento. Os requisitos associados à componente de processo serão partilhados em documento próprio.

10.10 Código de Modelo

<table>
<tr><th>Requisito</th><th>Descrição</th></tr>
<tr><td>R00137</td><td>
Código de modelo Gateway PLC

Cada equipamento deverá dispor de um código de modelo, com o formato apresentado na tabela seguinte, que identificará de forma hexadecimal (2 bytes) a tipologia do equipamento, a sua tecnologia de comunicação remota e a versão do seu hardware (número sequencial):
<table>
<tr><th colspan="4">Código de modelo</th></tr>
<tr><th>caracteristícas</th><th>Tipo de comunicação
ponto-a-ponto</th><th colspan="2">Nº sequencial</th></tr>
<tr><td>0 a F</td><td>0 a F</td><td>0 a F</td><td>0 a F</td></tr>
<tr><td>0 – gateway PLC com 1 interface RS-485
1 a F - utilização futura</td><td>0 – 1 módulo WAN
1 – 2 módulos WAN (redundância)
2 a F - utilização futura</td><td colspan="2">00, 01, …., FF (255)</td></tr>
</table>
O código de modelo será atribuído pela E-REDES a cada equipamento em função do seu código de material e fabricante, e deverá ser imutável ao longo da sua vida útil.

Qualquer alteração de hardware, nomeadamente nos designados componentes críticos, deverá ser comunicada previamente à E-REDES de forma a ser validada e verificada a necessidade de atribuição de um novo código de modelo (incremento do número sequencial).

O código de modelo deve constar na informação da MIB.
</td></tr>
</table>

11 MARCAÇÃO

<table>
<tr><th>Requisito</th><th>Descrição</th></tr>
<tr><td>R00138</td><td>
Placa de características

O equipamento deve ser dotado de uma placa de características colocada em local bem visível, com marcação durável, indelével e bem legível, em que conste:
— número de série do equipamento;
— Identificação do fabricante;
— referência do modelo;
— símbolo de duplo isolamento (de acordo com a IEC 62103);
— ano de fabrico;
— código de barras formado por 27 dígitos: concatenação de “0” com o código do material E-REDES de 8 dígitos, código de fabricante de 3 dígitos e número de série JUMP do equipamento com 15 dígitos)

Note-se que os 15 dígitos do número de série JUMP são compostos pela concatenação de zeros à esquerda, e o nº de série sequencial do equipamento à direita (caso o nº de série do equipamento tenha menos de 15 dígitos): p.e 000000xxxxxxxxx.

Preferencialmente, o número de série do equipamento deve ter os 15 dígitos, sendo os 2 primeiros indicativos do ano de fabrico, exemplo: 210000000000001, primeira Gateway PLC produzida no ano 2021.

O código de barras deverá estar colocado no equipamento e caixa individual.
</td></tr>
<tr><td>R00139</td><td>
Fixação

A fixação da placa de características não deve ser feita com parafusos, rebites ou outros dispositivos semelhantes, a fim de que a mesma não possa vir a prejudicar os graus de proteção especificados.
</td></tr>
<tr><td>R00140</td><td>
Marcações conectores

Todos os conectores da Gateway PLC devem estar devidamente identificados (por exemplo a identificação das fases e neutro, e interfaces de comunicação).
</td></tr>
</table>

12 ENSAIOS

12.1 Generalidades

As características das Gateways PLC devem ser confirmadas através da realização de ensaios, a efetuar em laboratórios acreditados para o efeito.

É da responsabilidade do fabricante a realização dos ensaios necessários à confirmação da sua conformidade com a presente especificação.

12.2 Execução dos ensaios

Salvo indicação contrária, os ensaios devem ser realizados:

— a uma temperatura ambiente compreendida entre 15 °C e 30 °C;

— com os equipamentos na sua posição normal de serviço e devidamente equipado.

No fim de qualquer ensaio ou pré-condicionamento deve ser feita uma observação visual com o intuito de detetar eventuais anomalias (mossas, riscos, bolhas, fissuras, lascas, marcas de contornamento ou de perfuração, etc.) as quais, em qualquer caso e se nada for especificado em contrário no presente documento ou nas prescrições das normas pelas quais se regem os ensaios, são consideradas não conformidades.

Se o estipulado nas normas de referência (referidas na presente secção) contrariar, no relativo à conformidade ou ao modo de procedimento dos ensaios, o especificado no presente documento, toma-se como válido o disposto neste último. No omisso, é válido o especificado nas normas de referência.

12.3 Ensaios de tipo

12.3.1 Ensaio de inspeção visual

Requisito	Descrição
E001	**Verificação Visual** Os equipamentos selecionados para os ensaios devem ser previamente sujeitos a uma verificação visual nos seguintes aspetos: — eventuais defeitos de fabrico; — disposição do equipamento; — dimensões do equipamento; — verificação das marcações.

12.3.2 Ensaio de verificação da indelebilidade da marcação

Requisito	Descrição
E002	**Ensaio de verificação da marcação** Este ensaio destina-se à verificação da indelebilidade da marcação acima referida na secção 11 . O ensaio deve ser realizado de acordo com o especificado na norma IEC 62208. Após o ensaio, a marcação deve manter-se legível e não deve ser possível retirá-la com facilidade. **Nota:** As marcações feitas por moldagem, puncionagem, gravação ou processo similar não devem ser submetidas a este ensaio.

12.3.3 Ensaios climáticos

12.3.3.1 Frio

Requisito	Descrição
E003	**Ensaio Frio** O ensaio deve ser realizado de acordo com o especificado na norma IEC 60068-2-1. O grau de severidade do ensaio é o seguinte: — ensaio Ae; — aceitação: realização, com sucesso, de um conjunto de ensaios funcionais durante e após o período de ensaio; — temperatura: -15 °C ± 3 °C; — duração: 16 horas.

12.3.3.2 Calor seco

Requisito	Descrição
E004	**Ensaio Calor Seco** O ensaio deve ser realizado de acordo com o especificado na norma IEC 60068-2-2. O grau de severidade do ensaio é o seguinte: — ensaio Be; — aceitação: realização, com sucesso, de um conjunto de ensaios funcionais durante e após o período de ensaio; — temperatura: +55 °C ± 3 °C; — duração: 16 horas.

12.3.3.3 Calor húmido

Requisito	Descrição
E005	**Ensaio Calor Húmido** O ensaio deve ser realizado de acordo com o especificado na norma IEC 60068-2-78. O grau de severidade do ensaio é o seguinte: — temperatura: +40 °C± 2 °C; — duração: 4 dias (96 horas); — humidade: 93 ± 2%.

12.3.4 Ensaios mecânicos

12.3.4.1 Vibração (sinusoidal)

Requisito	Descrição
E006	**Ensaio Vibração (sinusoidal)** O ensaio deve ser realizado de acordo com o especificado na norma IEC 60068-2-6. O grau de severidade do ensaio (classe B_m da norma IEC 60870-2-2) é o seguinte: — amplitude da aceleração: 1 g; — gama de frequência: 9 Hz a 200 Hz. (em alternativa poderão ser utilizados os valores de referência da norma IEC 60068-2-6: 10Hz a 200Hz).

12.3.4.2 Choque (Ensaio Opcional)

Requisito	Descrição
E007	**Ensaio Choque (Opcional)** O ensaio deve ser realizado de acordo com o especificado na norma IEC 60068-2-27. O grau de severidade do ensaio (classe B_m da norma IEC 60870-2-2) é o seguinte: — amplitude da aceleração: 10 g; — duração do impulso: 11 ms.

12.3.5 Verificação do grau de proteção do invólucro

12.3.5.1 Código IP

Requisito	Descrição
E008	**Ensaio de verificação código IP** A verificação do índice (grau) de proteção IP deve ser feita de acordo com o especificado na norma EN 60529. Grau de proteção mínimo do invólucro: IP 31. Preferencialmente, grau de proteção mínimo do invólucro: IP55.

12.3.5.2 Código IK

Requisito	Descrição
E009	**Ensaio de verificação código IK** A verificação do grau de proteção mecânica deve ser feita de acordo com o especificado na norma IEC 62262. Preferencial, o invólucro deve resistir a impactos de pelo menos 10J (IK09).

12.3.6 Ensaios dielétricos

12.3.6.1 Ensaio à onda de choque

Requisito	Descrição
E0010	**Ensaio à onda de choque** Aplicam-se, na generalidade, as condições definidas na secção 5.2.3.2 da norma IEC 62477-1 e no Anexo C da norma IEC 60255-27. 1. Valor da tensão de ensaio aplicada entre cada um dos circuitos galvanicamente independentes seguidamente indicados e todos os restantes circuitos ligados entre si e à "massa": — entradas de alimentação: 4 kV (desejavelmente 5 kV); — interfaces de comunicação: 2 kV (desejavelmente 2.5 kV); 2. Preferencialmente, valor da tensão de ensaio aplicada entre todos os circuitos ligados entre si e a "massa": 6 kV. **Nota:** considera-se "massa" uma superfície equipotencial constituída por uma folha metálica que envolve completamente o invólucro do equipamento em ensaio.

12.3.6.2 Ensaio à frequência industrial

Requisito	Descrição
E0011	**Ensaio à frequência industrial** Aplicam-se, na generalidade, as condições definidas na secção 5.2.3.4 da norma IEC 62477-1 e no Anexo C da norma IEC 60255-27. 1. Valor da tensão de ensaio aplicada entre cada um dos circuitos galvanicamente independentes seguidamente indicados e todos os restantes circuitos ligados entre si e à "massa": — entradas de alimentação: 2 kV; — interfaces de comunicação: 0,5 kV (desejavelmente 2 kV); 2. Preferencialmente, valor da tensão de ensaio aplicada entre todos os circuitos ligados entre si e a "massa": 4 kV. **Nota:** considera-se "massa" uma superfície equipotencial constituída por uma folha metálica que envolve completamente o invólucro do equipamento em ensaio.

12.3.7 Ensaios de imunidade

Os ensaios devem ser realizados de acordo com o especificado na norma IEC 60870-2-1.

Para cada ensaio são definidos os critérios de performance de acordo com as designações da norma IEC 61000-6-2, nomeadamente:

— Critério A: Não é permitida nenhuma degradação do desempenho especificado pelo fabricante, quando o equipamento é usado como previsto.
— Critério B: Durante o ensaio, a degradação de desempenho é permitida, contudo não é permitida nenhuma mudança de estado real ou de armazenamento de dados.
— Critério C: É permitida uma perda de função temporária, desde que seja auto recuperável ou possa ser restaurada através de controladores.

12.3.7.1 Ensaios de imunidade a transitórios conduzidos e perturbações de alta frequência

12.3.7.1.1 Transitório elétrico rápido

Requisito	Descrição
E0012	**Transitório elétrico rápido** O ensaio será realizado de acordo com a norma IEC 61000-4-4. Aplicam-se as condições definidas na secção 8.3 do presente documento e na tabela 12 da norma IEC 60870-2-1 (ensaio A.2.3). Pontos de aplicação e níveis de severidade do ensaio: — entradas de alimentação: 2 kV; — interfaces de comunicação: 1 kV; Critério de aceitação: B.

12.3.7.1.2 Ondas de choque

Requisito	Descrição
E0013	**Ondas de choque** O ensaio será realizado de acordo com a norma IEC 61000-4-5. Aplicam-se as condições definidas na secção 8.3 do presente documento e na tabela 12 da norma IEC 60870-2-1 (ensaio A.2.2).

	Pontos de aplicação e níveis de severidade do ensaio: — entradas de alimentação: 2 kV; — interfaces de comunicação: 1 kV; Critério de aceitação: A.

12.3.7.1.3 Onda oscilatória amortecida

Requisito	Descrição
E0014 (PREF)	**Onda oscilatória amortecida (Preferencial)** O ensaio será realizado de acordo com a norma IEC 61000-4-12. Aplicam-se as condições definidas na secção 8.3 do presente documento e na tabela 12 da norma IEC 60870-2-1 (ensaio A.2.5). Pontos de aplicação e níveis de severidade do ensaio: — entradas de alimentação: 2,5 kV; — interfaces de comunicação: 1 kV; Critério de aceitação: B.

12.3.7.2 Ensaio de imunidade a descargas eletrostáticas

Requisito	Descrição
E0015	**Descargas eletrostáticas** O ensaio será realizado de acordo com a norma IEC 61000-4-2. Aplicam-se as condições definidas na secção 8.3 do presente documento e na tabela 13 da norma IEC 60870-2-1 (ensaio A.3.1). Pontos de aplicação e níveis de severidade do ensaio: — invólucro: 6 kV (ao contacto); Critério de aceitação: B.

12.3.7.3 Ensaio de imunidade a campos magnéticos à frequência da rede

Requisito	Descrição
E0016	**Campos magnéticos à frequência da rede** O ensaio será realizado de acordo com a norma IEC 61000-4-8. Aplicam-se as condições definidas na secção 8.3 8.3 do presente documento e na tabela 14 da norma IEC 60870-2-1 (ensaio A.4.1). Pontos de aplicação e níveis de severidade do ensaio: — invólucro: 30 A/m em contínuo; 300 A/m durante 1 s; Critério de aceitação: A.

12.3.7.4 Ensaio de imunidade a campos eletromagnéticos radiados

Requisito	Descrição
E0017	**Campos eletromagnéticos radiados** O ensaio será realizado de acordo com a norma IEC 61000-4-3.

	Aplicam-se as condições definidas na secção 8.3 do presente documento e na tabela 15 da norma IEC 60870-2-1 (ensaio A.5.1). Pontos de aplicação e níveis de severidade do ensaio: — invólucro: 10 V/m; Critério de aceitação: A.

12.4 Ensaios de receção

Requisito	Descrição
E0018	**Ensaios de funcionamento** Devem ser realizados os seguintes ensaios de funcionamento: — Inspeção visual; — Ensaio funcional da Gateway PLC; — Ensaio funcional das comunicações entre a Gateway PLC e o DTC/Mega DTC Virtual; — Ensaio funcional das comunicações entre a Gateway PLC e os sistemas centrais; — Ensaio funcional das comunicações entre a Gateway PLC e os EMI, contadores totalizadores (se aplicável) e EMI IP (se aplicável). — Outros ensaios que se considere adequados a serem realizados.
E0019	**Inspeção Visual** Este ensaio consiste na análise visual da Gateway PLC, incluindo todos os seus componentes, com o objetivo de verificar o seu aspeto geral e a conformidade com o especificado no presente documento no que se refere aos requisitos construtivos e marcação.
E0020	**Ensaio funcional da Gateway PLC** Este ensaio consiste em verificar o cumprimento dos requisitos funcionais da Gateway PLC especificados no presente documento.
E0021	**Ensaio funcional das comunicações entre a Gateway PLC e o DTC/Mega DTC Virtual** A compatibilização das comunicações entre a Gateway PLC e o DTC/Mega DTC Virtual será da responsabilidade do fornecedor da Gateway PLC, devendo estar em conformidade com o descrito no presente documento.
E0022	**Ensaio funcional das comunicações entre a Gateway PLC e os Sistemas Centrais** A compatibilização das comunicações entre a Gateway PLC e os Sistemas Centrais E-REDES será da responsabilidade do fornecedor da Gateway PLC, devendo estar em conformidade com o descrito no presente documento.
E0023	**Ensaio funcional das comunicações entre a Gateway PLC e os EMI, Contadores Totalizadores (se aplicável) e EMI IP (se aplicável)** A compatibilização das comunicações entre a Gateway PLC e os EMI, Contadores Totalizadores (se aplicável) e EMI IP (se aplicável), será da responsabilidade do fornecedor da Gateway PLC, devendo estar em conformidade com o descrito no presente documento.

13 EMBALAGEM

Requisito	Descrição
R00141	**Entrega do equipamento** O equipamento, incluindo todos os seus componentes, deve ser fornecida devidamente embalada e acondicionada em embalagem única. A embalagem deve ser dotada de uma etiqueta, em que conste o nome do fabricante ou a sua marca comercial, o modelo do equipamento e código de barras tal como referido em R001380.

	A embalagem coletiva e/ou palete deverá conter um *QR Code*, cujo conteúdo deverá ser acordado com a E-REDES. Quanto à forma e método de etiquetagem e conceção das etiquetas, devem ser seguidas as instruções definidas no documento "Programa JUMP – Etiquetagem de Materiais e Equipamentos".

14 LEGISLAÇÃO DE SEGURANÇA E AMBIENTE

Requisito	Descrição
R00142	**Legislação de segurança e ambiental** Os produtos, e respetivos constituintes, devem estar conforme as normas técnicas europeias aplicáveis e cumprir toda a legislação aplicável em vigor, designadamente as Diretivas Reach, RoHs, WEE e diretiva 2009/125/EU.
R00143	**Utilização de substâncias perigosas** Os produtos devem cumprir com as disposições relativas à utilização e restrições de determinadas substâncias perigosas em equipamentos elétricos e eletrónicos (EEE), rotulagem e colocação no mercado, designadamente as previstas no Decreto-Lei n.º 79/2013, de 11 de Junho, retificado pela Declaração de Retificação n.º 35/2013, de 5 de Agosto, e alterado pelos Decreto-Lei n.º 119/2014, de 6 de Agosto, Decreto-Lei n.º 30/2016, de 24 de Junho e Decreto-Lei n.º 61/2017, de 9 de Junho. O Adjudicatário deve fazer prova deste enquadramento legal.
R00144	**Marcação CE** Os produtos devem cumprir os requisitos da União Europeia em matéria de segurança, saúde e proteção do ambiente. Devem apresentar Declaração CE de conformidade.

15 REQUISITOS INFORMATIVOS

Requisito	Descrição
R00145	**Informação índice fiabilidade MTBF** Deve ser apresentado o índice de fiabilidade MTBF do equipamento e por componentes críticos. Deve ser apresentada a metodologia preconizada (cálculos/ensaios/processos construtivos, seleção de componentes, etc.) utilizada para determinação do MTBF do sistema e dos respetivos componentes. Além disso, devem ser apresentados os pontos críticos do equipamento, componentes e condições de funcionamento considerados na determinação do MTBF.

ANEXO A
REQUISITOS DE CIBERSEGURANÇA

(Normativo)

Req.	Description
A1.1	It shall have sufficient reserves in memory and computing power to allow updates to security functions that security experts anticipate are necessary during its lifecycle.
A1.2	It shall support updating all security functions through remote software updates, being EDP Distribuição responsible for providing performing and secure remote access conditions at WAN communications interface.
B1.1	It shall use for security functions only cryptographic algorithms for which a description is publicly available, and which have been thoroughly reviewed by independent cryptographers.
B1.2	It shall not use for security functions a choice of cryptographic algorithms, protocols, and parameters if there are vulnerabilities known for them.
B1.3	If for a security function algorithms are available in the "ENISA algorithms, key size and parameters report", NIST 800-57 and NIST SP 800-175B reports, it shall use one of these algorithms.
B1.4	It shall use from the ENISA and NIST reports only those cryptographic algorithms, and parameters considered suitable for legacy or future use.
B1.5	It shall use the algorithms in the ENISA and NIST reports implemented exactly as they are described there without any modifications.
B1.6	It shall support AES and SHA.
B2.1	It shall use a dedicated cryptographic pseudo-random number generator, as defined in FIPS 186-2, FIPS 140-2 (Annex C), AIS 20, or AIS 31, to generate random numbers used for security functions.
B3.1	It must support remote updates of all credentials and cryptographic keys.
B3.2	It must support limiting the duration of an idle session to a time length that is configurable by EDP Distribuição.
B3.3	It should support establishing a fresh key for each communication session.
B3.4	It should support using different keys for different services and applications.
C1.1	It shall protect the confidentiality of communication with the central systems by encrypting it using a protocol allowed by the B1 requirements.
C1.2	It shall store passwords together with a salt using a cryptographic hash function allowed by the B1 requirements.
C2.1	It shall verify the integrity of application layer messages received on the WAN, LAN and Local Maintenance interfaces using a message authentication algorithm allowed by the B1 requirements.
C2.2	If it detects that a message has been modified or if it cannot verify the integrity of the message, it shall reject or drop the message.
C2.3	It shall allow parties it communicates with on the WAN, LAN and Local Maintenance interfaces to verify the integrity of application layer messages it sends by using a message authentication algorithm allowed by the B1 requirements.
C2.5	It shall allow the field devices it communicates with to verify the integrity of application layer messages it sends by using a message authentication algorithm allowed by the B1 requirements.
C3.1	It shall verify the integrity of software updates before they are applied.
C3.2	It shall reject software updates if it detects the firmware has been modified, or it cannot verify the software's integrity.
C4.1	It shall be able to detect replay attacks on the WAN, LAN and Local Maintenance interfaces.
C4.2	If it detects that a message is replayed, it must reject or drop the message.
C4.3	It shall be able to detect replay attacks from the field devices.
C5.1	It shall be able to determine that the sender of a configuration change or a software update has a certain role.
C6.1	It shall support non-repudiation for firmware: when it installs software, it shall be able to prove that the firmware came from the Vendor.
C7.1	It shall use secure communication protocols, such as: HTTPS, SSH and SFTP, in replacement of insecure protocols (with known vulnerabilities), such as: HTTP, TELNET and FTP, supporting the same functionality.
C7.2	It shall encapsulate insecure communication protocols (with known vulnerabilities) in others that provide security functions, such as TLS version 1.2 or greater.
D1.1	It shall have all unneeded services and applications removed, or disabled if removal is not possible.

Req.	Description
D1.2	It shall not use services or applications for security functions if there are vulnerabilities known for them.
D1.3	It shall use only communication protocols that are needed to meet the functional requirements.
D2.1	It shall have any unneeded interfaces and ports removed, or disabled if removal is not possible. In particular, all hardware interfaces that are used for debugging must be completely removed after production.
D3.1	It must not contain active default, guest and anonymous accounts.
D3.2	It must not allow remote access to its root accounts.
D3.3	It shall have Vendor-owned accounts removed where feasible.
D3.4	It shall support enforcing a password policy that only allows passwords compliant with the rules: - No spaces allowed - At least 8 characters - At least 3 out of the following 4 complexity rules: - At least 1 uppsercase character (A-Z) - At least 1 lowercase character (a-z) - At least 1 digit (0-9) - At least 1 special character (@#$%&*()_+=-{}[]|\:";'<>,./) - It should not contain the username.
D4.1	It should deploy security-enhancing features of the underlying platform, implementation language and tool chain when this enhances its security.
E1.1	It shall verify the validity of all messages it receives.
E1.2	It shall reject or drop messages that are invalid or for which the validity cannot be verified.
E2.1	It shall be fail-secure, i.e., it shall be designed to fail in a manner that limits any security compromise of its own operation and security compromise of other devices.
E2.2	It shall not leak confidential information, such as keys or credentials, on any interface during a failure.
E2.3	It shall protect the integrity of security critical data during failures.
E2.4	It shall not allow access controls to be bypassed remotely during failures.
E2.5	It shall restore availability after software failures as soon as possible.
F1.1	It shall allow to set access privileges for configuration and software update functions per role.
F1.2	It shall only grant access to configuration and software update functions if a user's role has the right privileges.
F1.3	It shall allow new roles to be defined for future applications.
F1.4	It shall allow to assign to each role individual security credentials and keys.
F1.5	It shall allow to set access privileges to sinalization and measurement reading and control functions per host.
F1.6	It shall only grant access requests to sinalization or measurement reading and control functions if the host has the right privileges.
F1.7	It should support central user authentication and authorization through a centralized server.
F1.8	At least with two local accounts (with write and read privileges) should be configured as a backup in case of central authentication server unavailability.
F2.1	It should authenticate the communication parties on the network interfaces using a challenge-response protocol based on either message authentication codes or public-key certificates.
F2.2	It should terminate the connection if the user authentication fails.
F2.3	It should authenticate the communication parties on the Local Maintenance interface.
F2.4	It should support blocking authentication requests, either temporarily or permanently, from an account after a number of failed login attempts. The number of failed login attempts and the time the account is blocked should be configurable.
G1.1	It shall log security events in a locally stored log.
G1.2	It shall take measures to prevent that attackers can modify, delete or overwrite the security log to hide their traces.
G1.3	It shall support automatically sending security log events to a central logging server or SIEM or, as an alternative, their retrieval through an equivalent automated process to be implemented in a joint effort by the vendor and the client.
G1.4	It shall support synchronization with a centrally maintained time, using NTP.
G1.5	It shall support synchronization with a centrally maintained time, using PTP.
G1.6	It should allow remote monitoring of information about the device status such as processor and memory usage.
G1.7	It shall support automatically sending or the retrieval of information about the device status such as processor and memory usage through SNMP or equivalent.

Req.	Description
G1.8	It should store for each security event at least the interface, the event type, a time stamp, and the user, role, or process causing the event.
G1.9	It shall record at least the following security events: - User Activities: - Successful logins - Failed login attempts - Updates or changes: - Firmware updates or patches - Configuration changes
G1.10	It should record at least the following security events: - User Activities: - Changes of security credentials - Unauthorized file access - Possible signs of attacks: - Resource exhaustion (DoS) - Messages whose integrity could not be verified - Invalid messages - Attempted replay attacks - Alarms on physical manipulation
H1.1	It shall be possible to remotely perform backups.
H1.2	It shall be possible to perform backups to external storage, available through the network (e.g., an SFTP server).

ANEXO B
INFORMAÇÃO HMI

A interface HMI do equipamento, através do perfil de configuração, deve possibilitar a leitura e/ou alteração dos parâmetros indicados na tabela seguinte.

Descrição	Classificação
— Identificação do equipamento e respetivas coordenadas geográficas: o Modelo (ler); o Número de Série (ler); o Versão de Firmware (ler); o Código de modelo (ler); o Localização (ler e configurar); o Hostname (ler e configurar).	Obrigatório
— Gestão dos perfis de acesso ao HMI: o *Users* (ler); o Passwords de cada *User* (configurar).	Obrigatório
— Configurações de sessão: o Timeout sessão (ler e configurar); o Número máximo de acessos simultâneos (ler e configurar).	Preferencial
— Interface de engenharia (CLI): o Ativar/inibir Telnet (ler e configurar); o Ativar/inibir SSH (ler e configurar); o Porto SSH (ler e configurar).	Preferencial
— Data e hora: o Time zone (ler e configurar);	Preferencial
— Reinicialização periódica do equipamento o Ativar/inibir reinicialização periódica (ler e configurar); o Data inicial de reinicialização periódica (ler e configurar); o Periodicidade de reinicialização do equipamento (ler e configurar).	Preferencial
— TCP socket: o TCP socket timeout (ler e configurar);	Preferencial
— Eventos o Ativar/inibir o(s) log(s) de eventos (ler e configurar); o Formato de armazenamento dos dados (log, XML, etc), se aplicável (ler e configurar).	Preferencial
— Interface(s) Ethernet o Ativar/inibir DHCP (ler e configurar); o Ativar/inibir IP Fixo (ler e configurar); o Endereço IP fixo (ler e configurar); o Máscara (ler e configurar); o Mac address (ler);	Obrigatório
— Interface WAN celular: o Ativar/inibir WAN celular (ler e configurar); o Cartão SIM primário (selecionar SIM A, SIM B, alternado, etc), se aplicável (ler e configurar); o Preferencialmente, número máximo de tentativas de ligação (ler e configurar); o Preferencialmente, tempo máximo para estabelecer ligação (ler e configurar); o Nível de cobertura baixa para gerar alarme (ler e configurar); o Período de cobertura baixa para gerar alarme (ler e configurar); o Tempo máximo no cartão SIM secundário (ler e configurar); o Período de amostragem de qualidade sinal (ler e configurar);	Obrigatório

○ Período de evolução da qualidade de sinal (ler e configurar); ○ Preferencialmente. Período de evolução da qualidade de sinal EC/n0 (ler e configurar); ○ Ativar/inibir dual SIM, se aplicável (ler e configurar). • SIM A e/ou SIM B: ○ PIN (ler e configurar); ○ Rede preferencial (UMTS, GPRS, etc) (ler e configurar); ○ APN (ler e configurar); ○ Método de autenticação (none, pap, chap, etc) (ler e configurar); ○ User (ler e configurar); ○ Password (ler e configurar); ○ Min. sinal GPRS, em dBm (ler e configurar); ○ Min. sinal UMTS, em dBm (ler e configurar); ○ Preferencialmente, Max. EC/n0, dB (ler e configurar); ○ Preferencialmente, Min coverage, em % (ler e configurar); ○ Preferencialmente, Critério de qualidade (sinal, cobertura, EC/n0) (ler e configurar); ○ Ativar/inibir default route (ler e configurar); • Ping keep alive: ○ IP remoto (ler e configurar); ○ Preferencialmente, frequência (ler e configurar); ○ Preferencialmente, timeout (ler e configurar); ○ Preferencialmente, tamanho pacotes ICMP (ler e configurar); ○ Preferencialmente, Número de pacotes ICMP (ler e configurar); ○ Preferencialmente, modelo de avaliação (sigular, periódico) (ler e configurar); ○ Preferencialmente, período de avaliação (ler e configurar); ○ Preferencialmente, Racio max. de perdas, em % (ler e configurar); ○ Preferencialmente, Acção (nenhuma, reconectar, reboot, etc). • Definição de túnel: ○ Configurar tipo de túnel (ler e configurar); ○ Configurar túnel ID Preshared Key (configurar).	
— PRIME ○ Ativar/inibir PRIME (ler e configurar); ○ Modo de operação, *Service Node* ou *Base Node* (ler e configurar); ○ Tipo de transmissão, série ou TCP, se aplicável (ler e configurar); ○ Seleção canal/Fase de transmissão TX, se aplicável (ler e configurar); ○ Seleção canal/Fase de recessão RX, se aplicável (ler e configurar); • Prime over UDP ○ Ativar/inibir PRIME over UDP (ler e configurar); ○ IP e porto DTC ou HES (ler e configurar); ○ UDP ALV Timeout (ler e configurar); ○ Equipamentos registados (PLC, UDP, todos), (ler e configurar)	Obrigatório
— PRIME • Log topologia de rede PRIME, configurações FTP (ler e configurar); ○ Ativar/inibir log (ler e configurar); ○ Filename (ler e configurar); ○ Host IP (ler e configurar); ○ Porto (ler e configurar); ○ Path (ler e configurar); ○ User (ler e configurar); ○ Password (ler e configurar); ○ Número máximo de linhas por envio (ler e configurar); ○ Timout envio informação, em segundos (ler e configurar); ○ Preferencialmente, Número de tentativas (ler e configurar); ○ Preferencialmente, Tempo entre tentativas (ler e configurar);	Preferencialmente

• Log notificações 432, configurações FTP (ler e configurar). o Ativar/inibir log (ler e configurar); o Periodo, em segundos (ler e configurar); o Filename (ler e configurar); o Host IP (ler e configurar) o Porto (ler e configurar); o Path (ler e configurar); o User (ler e configurar); o Password (ler e configurar); o Preferencialmente, Número de tentativas (ler e configurar); o Preferencialmente, Tempo entre tentativas (ler e configurar);	
— Configurações porta série o Velocidade porta série baud (ler e configurar); o Data bits, Parity bits, Stop bits (ler e configurar); o Timeout (ler e configurar); o Porto de escuta. • HDLC over TCP o Preferencialmente, Tamanho máximo do pacote TCP; o Preferencialmente, Time-out para envio do pacote TCP; o Preferencialmente, Idle-time da sessão TCP; o Preferencialmente, Keep-alive da sessão TCP;	Obrigatório
— Routing • Static routes; o Static Routes (ler e configurar); o Default Static Routes (ler e configurar); • Dinamic Routes, RIP (ler e configurar).	Obrigatório (se aplicável)
— Configuração VPN (ler e configurar); • Definição do túnel o Túnel ID (ler e configurar) o Rede local (ler e configurar); o IP remote gateway (ler e configurar); o Rede remota (ler e configurar); o Associar IKE Policy (ler e configurar); o Associar IPsec Security association (ler e configurar); o Ativar/inibir o túnel (ler e configurar); • IKE policies (ler e configurar); • Preshared keys (ler e configurar); • IPSec Security associations (ler e configurar);	Obrigatório (se aplicável)
— SNMP o Ativar/inibir agente SNMP (ler e configurar); o Community, definir perfis de acesso e direitos de acesso de cada perfil (ler e configurar); o Preferencial, SNMPv3 engine ID (ler e configurar); o Preferencial, Lista de utilizadores (ler e configurar); • SNMP Traps o Preferencial, Ativar/inibir Traps (ler e configurar); o Preferencial, SNMPv1/v2c traps (ler e configurar); o Preferencial SNMP v3 traps (ler e configurar); o Preferencial, Trap v1 agent adress (ler e configurar); o Preferencial, Ativar/inibir WAN linkup trap (ler e configurar); o Preferencial, Ativar/inibir WAN low coverage trap (ler e configurar); o Preferencial, Ativar/inibir WAN high couverage trap (ler e configurar);	Obrigatório
— NTP	Obrigatório

○ Ativar/inibir NTP (ler e configurar); ○ Chave de autenticação (ler e configurar); ○ IP Servidor NTP (ler e configurar).	
— Acessos TACACS+ ○ IP Servidor, outros parâmetros (ler e configurar); ○ Console access (ler e configurar); ○ Web access (ler e configurar); ○ Telnet access (ler e configurar); ○ SSH access (ler e configurar).	Preferencial
— Estatísticas de comunicação • Geral ○ Data/hora (ler); ○ Preferencialmente, Temperatura (ler); ○ Preferencialmente, Utilização memória, em % (ler); ○ Preferencialmente, Utilização CPU longa duração, em % (ler); ○ Preferencialmente, Utilização CPU curta duração, em % (ler) • WAN ○ Modem (ler); ○ IMEI (ler); ○ IMSI (ler); ○ CID (ler); ○ Preferencialmente, PIN status (ler); ○ SIM ativo (ler); ○ Operador (ler); ○ Roaming (ler); ○ Rede (ler); ○ Código localização área (ler); ○ Identificação célula (ler); ○ Força sinal (ler); ○ RSCP (ler); ○ Preferencialmente, EC/n0 (ler); ○ Preferencialmente, Número de falhas de sessões (ler); ○ SIM A Tx (ler); ○ SIM A Rx (ler); ○ SIM B Tx (ler); ○ SIM B Rx (ler); • Sessão atual ○ Status (ler); ○ Endereço IP interface WAN (ler); ○ Data de ligação (ler); ○ Tx, em bytes (ler); ○ Rx, em bytes (ler); ○ Tx, rate em bps (ler); ○ Rx, rate em bps (ler); • LAN (Ethernet) ○ Preferencialmente, Status (Ativo/Inativo) (ler); ○ Data de Status (ler); ○ Tx, em bytes (ler); ○ Rx, em bytes (ler); • TAN (interface série) ○ Preferencialmente, Status (Ativo/Inativo) (ler); ○ Data de Status (ler); ○ Tx, em bytes (ler);	Obrigatório

○ Rx, em bytes (ler); • Routing ○ Routing rules (ler) • VPN ○ Preferencialmente, Status (Ativo/Inativo) (ler); ○ Data de Status (ler); ○ Tx, em bytes (ler); ○ Rx, em bytes (ler); ○ Outros.	
— Informação da topologia da rede PLC, quando o equipamento estiver configurado como *Base Node* (Nível na rede, Número de série, Mac address, tecnologia, estado, LNID, SID, tempo ligado, % tempo ligado, etc);	Preferencial
Deverá ser possível executar os comandos seguintes: — Preferencialmente, Reset de estatísticas de comunicação; — Upload de ficheiro de configuração; — Download de ficheiro de configuração; — Atualização de firmware; — Reboot ao equipamento;	Obrigatório