SIEMENS

Embedded Software

Product Specific Maintenance Services Terms

These Embedded Product Specific Maintenance Services Terms ("EMB-EPS Maintenance Terms") supplement the General SISW Maintenance Services Terms and apply solely to Products identified on the Order Form as "EMB-EPS". These EMB-EPS Maintenance Terms, together with the General SISW Maintenance Services Terms, the EULA and other applicable Supplemental Terms, form the agreement between the parties ("Agreement").

1. DEFINITIONS. Capitalized terms used herein have the meaning as defined in the Agreement. The following additional definitions apply to these EMB-EPS Maintenance Terms:

(a) "Reference Platform" shall mean a supported target hardware and/or host environment.

(b) "Target Response Time" means the time period that starts when an Error is received by SISW and ends once SISW acknowledges its reception.

(c) "Target Resolution Time" means the time period that starts when a reproducible test case is received by SISW and ends when SISW provides a response to the Customer.

2. MAINTENANCE OF PRIOR VERSIONS. SISW actively supports EMB-EPS Products for a period of five years from the initial date of each Major Release on SISW´s support center ("Support Lifecycle"). All Point Releases will inherit the support term of the associated Major Release. Generally, support in years 4 and 5 of the Support Lifecycle will consist only of Errors defined as S1 below.

3. SECURITY UPDATES (CVE MONITORING). SISW shall regularly monitor various sources for Common Vulnerabilities and Exposures ("CVE") for components and configurations applicable to EMB-EPS' Linux products. SISW uses the CVSS v3.0 ratings from the National Vulnerability Databases (https://nvd.nist.gov/vuln-metrics/cvss) definition of what a critical CVE is, a CVE with a score of 9-10 is critical. SISW shall provide security updates as follows: (i) Cumulative Point Releases for selected non-critical CVEs; and (ii) Non-cumulative Point Releases for selected Critical CVEs. All such releases shall be made available via the electronic customer support system and within a reasonable time after release of the identified security updates by the relevant communities (depending on the criticality of the vulnerability).

4. ERROR CORRECTION.

4.1. **Eligibility.** To be eligible for Error correction, the reported test case must be reproducible on a SISW Reference Platform. SISW must also receive from the Customer all required information to enable SISW's Error analysis. This information includes, but is not limited to:

- Detailed Error description
- Information to reproduce the Error on supported hardware
- Any available recordings or traces of the system software on the target platform of the Products
- Information about corresponding hardware and software versions of the target system where the Error occurred

4.2. **Error severity, target response and target resolution time.**

Errors are divided, at the reasonable discretion of SISW, into 4 categories:

Severity	Impact
S1	System is down, cannot perform. No work around available
S2	System is impaired, but some functionality is available. No work around available
S3	System is degraded, but most of it is functional. Work around is available
S4	Trivial

Once an Error is reported to Support, the following Target Response and Target Resolution Times will apply:

Severity	Target Response Time	Target Resolution Time
S1	2 business days	2 business days
S2	2 business days	10 business days
S3	2 business days	Commercially reasonable effort
S4	2 business days	At SISW discretion

4.3. **Response Types.** Once Customer is eligible for Error correction, SISW will evaluate the Error and provide a response, according to the response types specified below:

- Propose a timetable for a fix, or a work around, or both
- Error cannot be reproduced, need more information
- Not an Error, and rationale why
- Enhancement request
- Duplicate
- Will not fix