STATEMENT OF COMPATIBILITY

between

Kaspersky Industrial CyberSecurity for Nodes 3.0
Kaspersky Industrial CyberSecurity for Networks 3.1

the products of

AO “Kaspersky Lab”
39A/2 Leningradskoe Shosse,
Moscow, 125212, the Russian Federation

hereinafter referred to as “KICS for Nodes”, “KICS for Networks” and “Kaspersky” respectively

and

“DeltaV 13.3.1 (Russian version)”
the product of

“Emerson” LLC
53/5 Dubininskaya Str., Moscow, 115054, the Russian Federation

hereinafter referred to as “DeltaV” and “Emerson” respectively.

Emerson and Kaspersky hereby declare the possibility of mutual apply of the mentioned software products in unified information system, compatibility of these software products, allowing to meet certain information security requirements for automated process control systems (hereinafter referred to as APCS), these products are operated.

KICS for Nodes, KICS for Networks and DeltaV are software products used in industrial automation. KICS for Nodes and KICS for Networks are tools to ensure information security of the APCS. DeltaV is a distributed process control system.

Emerson and Kaspersky have carried out extensive compatibility tests for the joint use of DeltaV and KICS for Nodes. The outcome of the tests was that, subject to the individual requirements of DeltaV workstation environment, KICS for Nodes can be used jointly with DeltaV as complementary software within the same system. The tests have not revealed any compatibility issues in products used within the same system.

KICS for Networks can be used as a passive network monitoring tool for DeltaV, subject to Emerson's general requirements for the installation and use of network traffic analysis software tools.

Due to the fact that KICS for Networks is a passive network monitoring tool and does not affect DeltaV components functioning, Kaspersky have performed the necessary and sufficient testing of this product themselves.
This statement of compatibility is only valid for DeltaV APCS used on the territory of the Russian Federation.

In addition to the installation and use of both products in accordance with recommendations and guidelines for installation and configuration by Kaspersky and Emerson, other security measures may be necessary to implement all information security requirements in each particular security class of automated systems according to Order No. 31 “About approval of Requirements to ensure information protection in automated systems of control of production and technological processes at critical objects, potentially dangerous objects, as well as objects that pose increased danger to human life and health and to the environment” of the Federal Service for Technical and Export Control of the Russian Federation (FSTEC) of March 14, 2014. The actual measures taken will depend on the specific information security requirements for the subject of protection, as well as the architecture of the APCS. Such measures may include, but are not limited to, the installation and use of other software or hardware, the appropriate product configuration, and the creation or adjustment of organizational processes.

Despite the positive result of the compatibility testing of the current versions of KICS for Nodes and DeltaV, as a measure to exclude the possible negative impact of KICS for Nodes on the regular operation of the DeltaV APCS during their joint use, it is allowed to install and use in DeltaV systems only anti-virus signature databases and updates of anti-virus signature databases that have been tested for compatibility with DeltaV in the same system in Kaspersky, as well as anti-virus protection modules and updates of KICS for Nodes that have been tested for compatibility with DeltaV in Emerson.