STATEMENT OF COMPATIBILITY

between
Kaspersky Industrial CyberSecurity
the product of
AO “Kaspersky Lab”
39A/2 Leningradskoe Shosse,
Moscow, 125212, the Russian Federation
hereinafter referred to as “KICS” and “Kaspersky” respectively
and
OIC Dispatcher NT
the product of
“NTK Interface” LLC
77 Zavodskaya Str., Ekaterinburg, 620043, Russia
hereinafter referred to as “OIC Dispatcher NT” and “NTK Interface” respectively.

NTK Interface and Kaspersky Lab hereby declare the possibility of mutual application of the mentioned software products in a 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 mutually run:

OIK Dispatcher NT and KICS are software products used in automation of electric power transmission and distribution. OIK Dispatcher NT is the automated process control system. KICS is an integrated cybersecurity solution for critical infrastructure and industrial automation.

NTK Interface and Kaspersky Lab conducted extensive testing of the OIK Dispatcher NT and KICS compatibility within a unified information system. Tests proved the possibility of use the products in a unified information system, taking into account their individual environmental requirements. The tests have not revealed any compatibility problems in products.
Installed together, according to requirements and installation and control guidelines, in the unified information environment, **OIK Dispatcher NT** products and **KICS** their functionality ensure that some information security requirements are met, specified in 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.

Besides installing and using both products, other measures may be necessary to complete all information security requirements for each specific class of automated systems. The actual measures taken should depend on the specific information security requirements for the object, as well as the APCS architecture of the object. Such measures may include, but are not limited to, installation and implementation of other software or hardware products, appropriate product configuration, and creation or adjustment of organizational processes.