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
Software complex “EKRA MS”
the product of
NPP “EKRA” LLC
3 Yakovlev Ave., Cheboksary, 428020, Chuvash Republic, Russia
hereinafter referred to as «EKRA» respectively.

This Statement of Compatibility of EKRA and Kaspersky Lab 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 mutually run:

EKRA MS is a software package for terminal management used in the field of industrial automation. KICS is an integrated cybersecurity solution for critical infrastructure and industrial automation.

EKRA and Kaspersky Lab tested EKRA MS and KICS compatibility within unified information system. Tests proved the possibility of use the products in 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, EKRASMS products and KICS their functionality ensure that some of the information security requirements are met, approved by Order of FSTEC of the Russian Federation No. 31 of 14.03.2014 “On Approval of Requirements to Ensure Information Protection of Automated Systems of Control of Production Technological Processes at Critical Facilities, Potentially hazardous objects, as well as objects of increased danger to human life and health and to the environment."

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.