Risk assessment according to DIN EN ISO 14971 for Kitozoom USB video microscopes and Metric measuring software

DIN EN ISO 14971 offers a systematic approach to risk assessment, which is applied here to the *Kitozoom USB* video microscope and the *Metric* measurement software. The aim is to identify and evaluate potential risks for users and the environment and to control them by means of measures. Both products are viewed as an integrated system, as hardware and software are closely linked in their function.

1st Area of application

1. The Kitozoom USB is an optical video microscope with USB interface for digital inspection and measurement of surfaces, workpieces and components. It is frequently used in industrial quality assurance. The Metric measuring software is used to record and evaluate the data, enables calibrations and generates reports.

---

2. Risk analysis

2.1 Risk identification

The potential risks are divided into the following categories:

1. **Mechanical risks:**
    - Damage to the microscope housing or optics due to a fall.
    - Risk of injury from sharp edges or breakage.
2. **Electrical risks:**
    - Short circuits, overheating or electric shocks due to improper handling or defective cables.
    - Data loss or malfunctions due to unstable power supply.
3. **Optical risks:**
    - Eye fatigue due to prolonged use of the screen without breaks.
    - Unpleasant light reflections or glare if the work area is improperly lit.
4. **Software-related risks:**
    - Misinterpretation of the measurement results due to software errors or incorrect calibration.
    - Crashes or incompatibilities when using the Metric measurement software.
    - Data loss due to improper storage of measurement data.

5. **Usage-related risks:**
    - Incorrect operation by untrained personnel.
    - Damage to the system due to improper maintenance or storage.
6. **Environmental risks:**
    - Malfunctions due to dust, moisture or temperature fluctuations.
    - Excessive wear due to intensive use without regular cleaning.
7. **Cybersecurity risks (software-related):**
    - Manipulation or loss of data due to inadequate security measures.
    - Unauthorized access to the system, especially with a USB connection.

2.2 Risk assessment

The risks are assessed according to severity (S) and probability (P). The risk priority number (RPN) is calculated as:
RPZ=S×P\text{RPZ} = S \times PRPZ=S×P

Risk	S	P	RPZ	Comment
Housing/optical damage	3	3	9	Risk can be minimized through more robust materials and precautionary measures.
Injuries due to broken edges	3	2	6	Low, with regular inspection of the appliance.
Electrical short circuits	4	2	8	Risk can be reduced through high-quality components and safety checks.
Data loss due to power failure	4	3	12	Can be minimized by a UPS (uninterruptible power supply).
Software crash	3	3	9	Regular updates and tests necessary.
Incorrect calibration	5	2	10	Critical, as this strongly influences the measurement results.
Data manipulation	4	2	8	Risk can be limited by encryption and user rights.
Environmental malfunctions	3	3	9	Good design protects against dust and moisture.
Eye fatigue	2	4	8	Ergonomic work instructions can reduce this risk.

3. Risk control

Suitable measures are proposed for each risk in order to minimize the probability of occurrence or the severity of the damage:

Risk	Measures
Housing/optical damage	Robust housing, impact-resistant materials and carrying case.
Injuries due to broken edges	Rounding of edges and regular inspections.
Electrical short circuits	Use of tested power supply units and cables, safety monitoring.
Data loss due to power failure	Use of a UPS and regular automatic data backups.
Software crash	Regular software updates and intensive testing before release.
Incorrect calibration	Calibration instructions, regular training and test intervals.
Data manipulation	Data encryption, password protection and access restrictions.
Environmental malfunctions	Dust and moisture protection thanks to encapsulated housing.
Eye fatigue	Ergonomic workplace design, e.g. screen height and lighting.

---

4. Cybersecurity risks

Increasing digitalization brings with it specific cybersecurity risks, especially with USB-based connectivity. These risks include:

- **Data theft:** Sensitive measurement data could be tapped by unauthorized persons.
- **Manipulation of measurement data:** Altered data could lead to incorrect quality decisions.
- **Malware infections:** Malware could get onto the system via the USB port.

Risk control measures:

1. **Encryption:** Ensure that data transmissions are encrypted.
2. **Access control:** Introduce user roles and passwords.
3. **Firewall and antivirus:** Use of protection software against malware.
4. **USB blocking:** Block unauthorized USB devices.

---

5. Residual risk and monitoring

Despite the proposed measures, residual risks remain, in particular due to unforeseeable operating errors or environmental factors. These residual risks must remain acceptable and be minimized through regular monitoring:

- **Feedback:** Collecting user feedback to identify new risks.
- **Monitoring:** Systematic monitoring of software errors and hardware failures.
- **Improvement:** Continuous optimization of the design and software based on new findings.

---

6. Conclusion

The risks of the Kitozoom USB video microscope and the Metric measurement software can be reduced to an acceptable level by a combination of technical, organizational and security-related measures. Particular attention should be paid to avoiding data loss, software errors and security risks. Continuous monitoring and user training can ensure safe use.