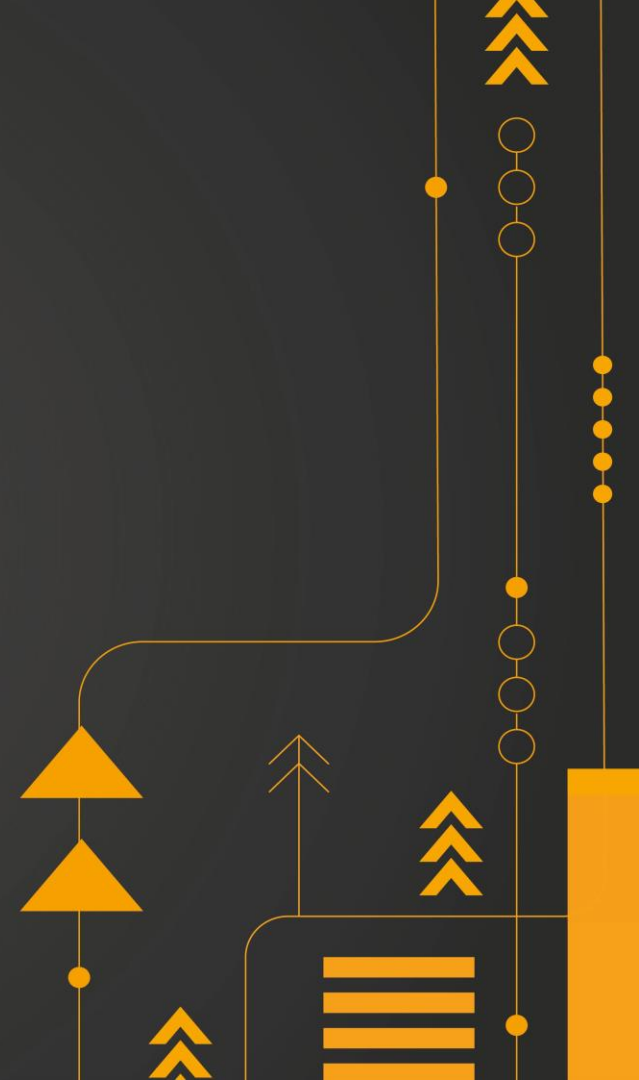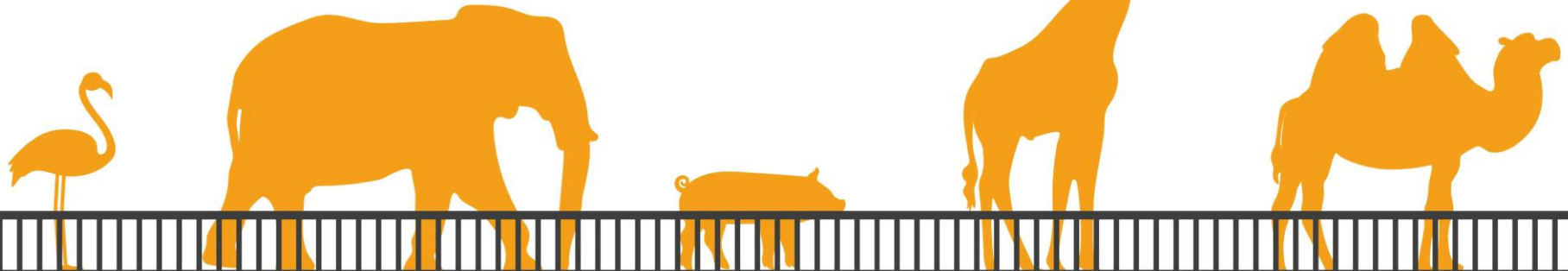# PROBLEMS OF PROTECTING COMPLEX ICS

Critical Infrastructure System must be protected to comply with Federal Law #187

COMPLEX ICS CLASSIFICATION

- By system architecture - SCADA, DCS, SIS, etc.

- By base network IT-infrastructure (specialized network equipment, proprietary data protocols, etc.)

- By extended IT-infrastructure (services used for correct ICS functioning)

SECURITY SYSTEM IMPLEMENTATION

1 — Preliminary tender procedures and design specification forming

2 — Contract signing

3 — Concept designing and technical project

4 — Detailed designing and implementation

5 — Reliability field testing and acceptance procedures

SECURITY SYSTEM IMPLEMENTATION

1

2

3 APPROVED

4

5

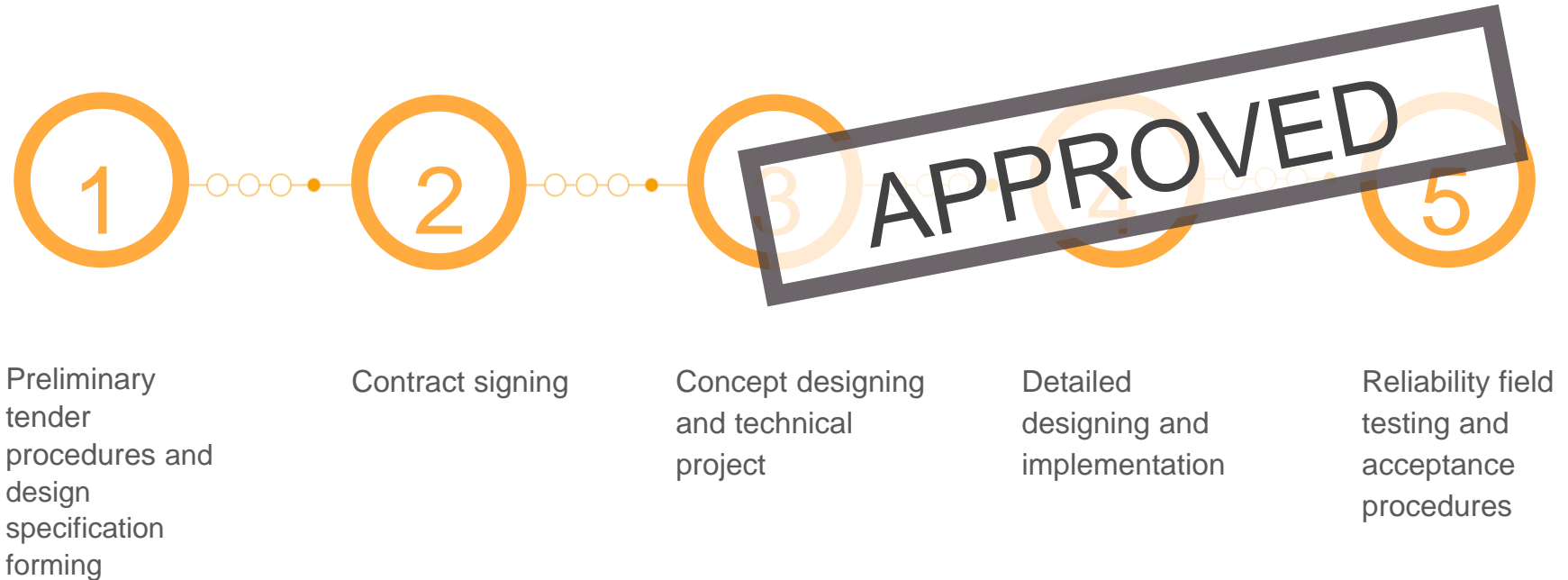Preliminary tender procedures and design specification forming

Contract signing

Concept designing and technical project

Detailed designing and implementation

Reliability field testing and acceptance procedures

PROTECTED OBJECT CONCEPT

Black Box

White Box

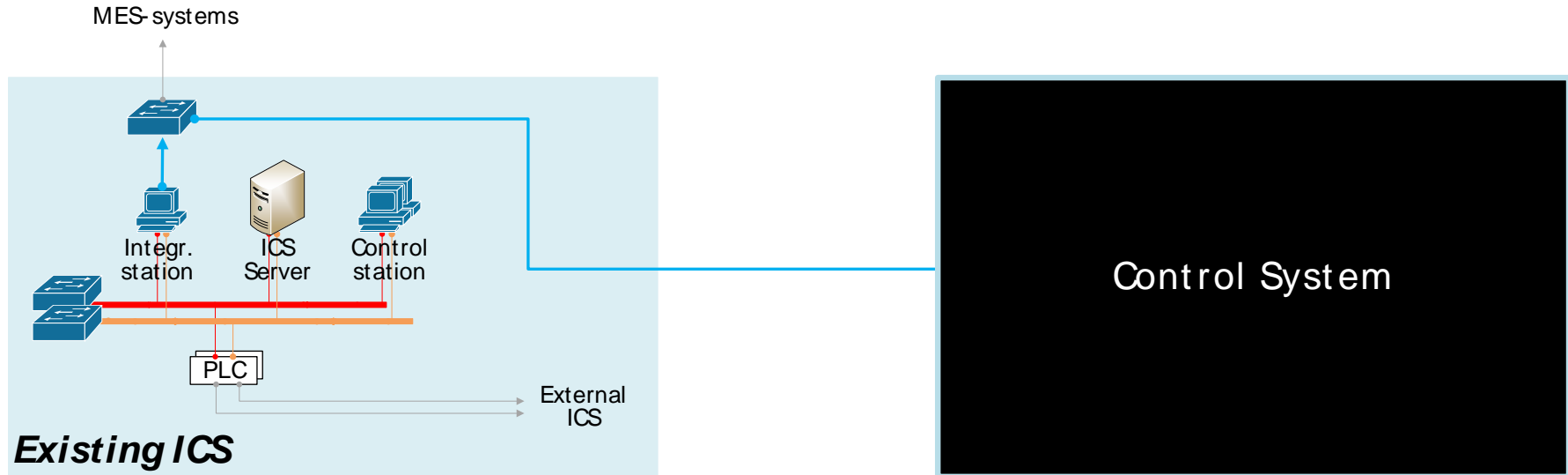# PROTECTED OBJECT
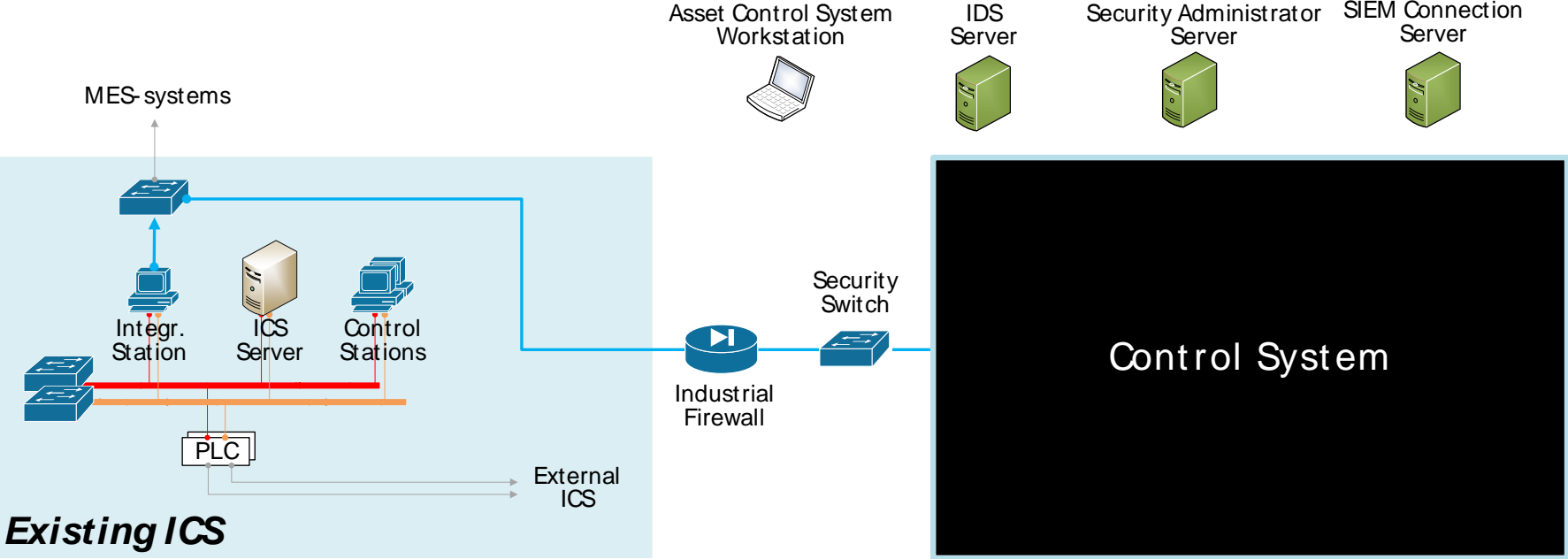
BLACK BOX

MES-systems

Integr. Station

ICS Server

Control Stations

PLC

External ICS

Existing ICS

Asset Control System Workstation

IDS Server

Security Administrator Server

SIEM Connection Server
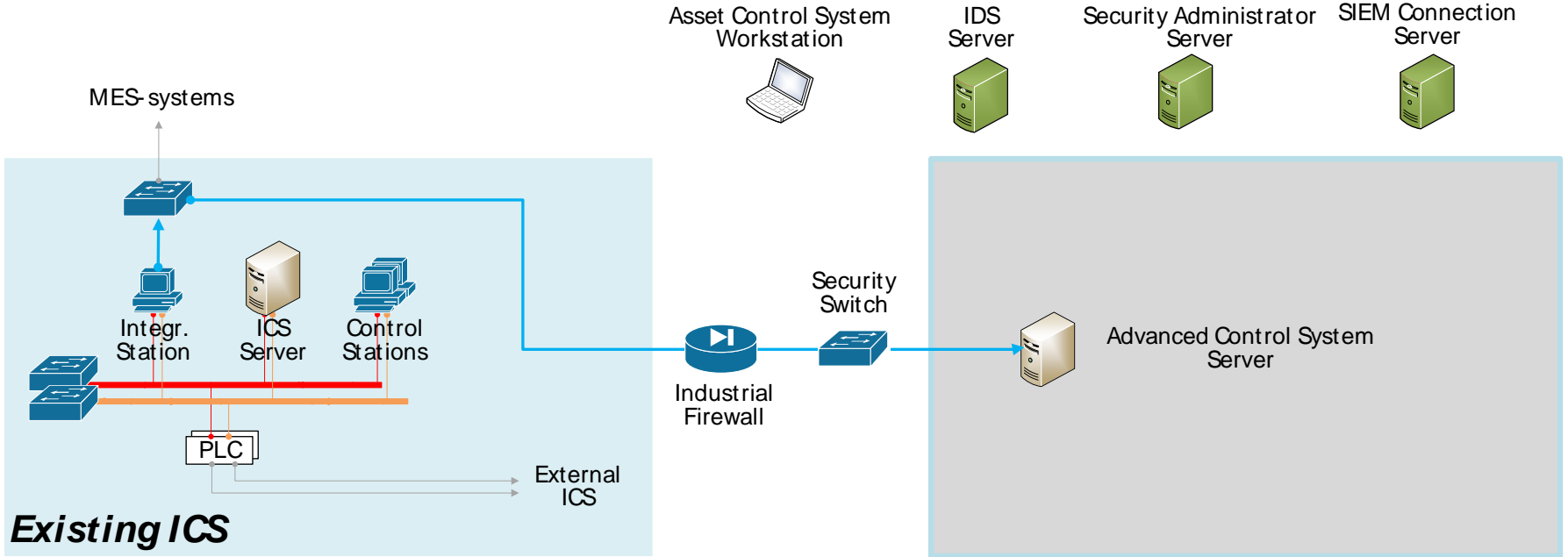
Security Switch

Industrial Firewall

Control System

WHITE BOX

BLACK BOX

+

- Easier designing stage

- Relatively low operational costs

-

- Enlargement of responsibility gap between security and technological maintenance units

- High chances of project deadlocking

DEADLOCK

How to break the deadlock?

- Test designed security solutions compatibility with existing control system components

- Look into security solutions, approved by ICS vendors (also in other countries) and implement them in the project
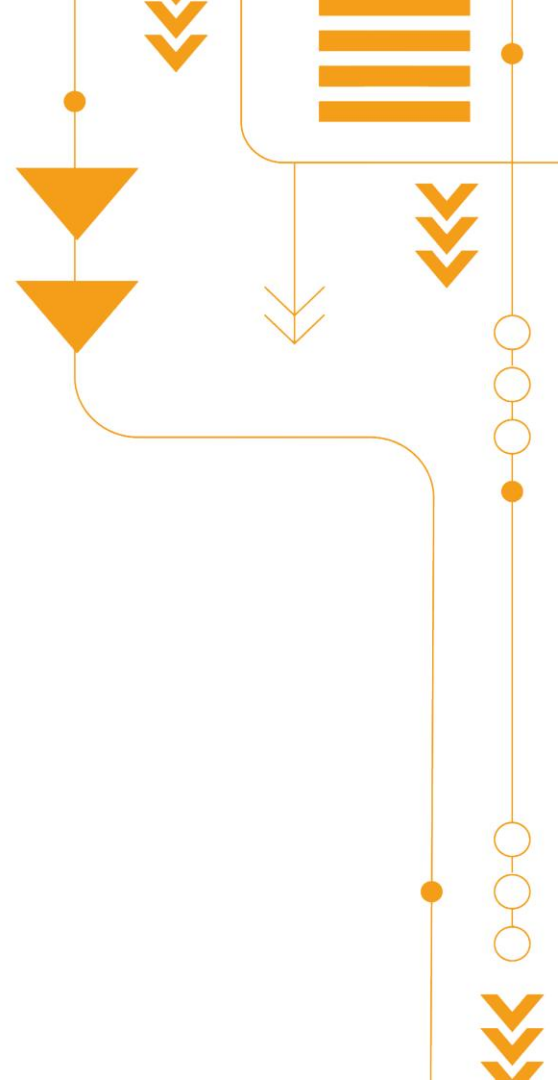
WHITE BOX

+

- More reliable solutions – security system is more homogeneous with control system

- Lower external security solutions cost

- High-level integration with existing maintenance processes

-

- Require high expertise in ICS

- Relatively high operational costs

INTERNAL ICS SECURITY MECHANISMS ANALYSIS

- Identification and authentication

- Access control

- Security audit

- Accessibility provision

- Control system software protection

- Configuration control

CONCLUSION: FURTHER DEVELOPMENT DIRECTIONS

Security Integrators	Control systems Integrators	Security Vendors	ICS Vendors	Critical ICS Owners
Increase ICS expertise – hire analytics and experts with background in various industrial sectors	Consider ICS security beforehand in order to avoid deadlocks	Certify their security solutions compatibility with major control systems solutions on the market. Help ICS Owners in deadlock situations	Improve security of recent control systems, continue to patch major security flaws in legacy systems	Account all foresaid factors and risks before the starting ICS security projects

CONTACT US

Angara Technologies Group
121087, Moscow, Bagrationovskiy proezd,
7/2, BP «Rubin»

info@angaratech.ru
www.angaratech.ru
+7 (495) 269-26-06

Angara Professional Assistance
121087, Moscow, Barklaya st., 6/3,
BP «Barklay Park»

support@angaratech.ru
www.angarapro.ru
+7 (495) 269-26-06