PROVECTA PROCESS AUTOMATION

INFORMATION/OPERATIONAL TECHNOLOGY AND CYBERSECURITY

CAPABILITY STATEMENT

provecta
PROCESS AUTOMATION

December 2019

1 INTRODUCTION

Provecta Process Automation Pty Ltd is an Australian owned engineering consultancy company providing services in the fields of control systems. Provecta specialises in providing services to the utility and public infrastructure sectors.

Provecta is a highly specialised organisation with the experience, expertise and resources to provide engineering services to assist with the planning, engineering assessment, specification and implementation of Operational Technology (OT) systems.

Provecta has a strong focus on Operational Technology, backed by our abilities as practitioners in control system technologies that provides deep understanding and knowledge of the technologies involved. This allows Provecta to manage the risks of OT systems from design through to implementation in order to provide robust, reliable and secure systems to support a customer’s digitisation programme.

A key aspect of our services is the development and management of appropriate cybersecurity controls to minimise the risks and impact of malicious attacks.

Further general information about Provecta may be obtained at our web site - www.provecta.com.au.

2 TECHNICAL CAPABILITIES

Provecta has expertise in the provision of consulting and engineering services across a wide range of operational technology and cybersecurity fields. Key services provided by Provecta include the following areas.

2.1 Standards Compliance

Provecta services include implementation and assessment of existing systems against common industry standards including:

- ISA/IEC 62443 (ISA99)
- AS/NZ/ISO 27000 Series
- NERC CIP
- Electricity Subsector Cyber Security Capability Maturity Model (ES-C2M2)
- Australian Energy Sector Cybersecurity Security Framework (AESCSF)

2.2 Threat and Risk Assessments

A key requirement in the design of any operational technology system is understanding the threats and risks to the underlying control and monitoring systems in the key areas of confidentiality, availability and integrity.

Provecta can lead the development of threat and risk assessments for existing systems to identify appropriate controls required to reduce risks to meet target levels specified within corporate risk management policies.

Threat and risk assessments consider threats from internal and external malicious actors, technical vulnerabilities that may be present, as well as risks in system design that may impact the integrity and availability of the system.

The outcome of the threat and risk assessment is used to inform the design of the system architecture as well as develop appropriate incident response and disaster recovery plans.

2.3 Network Architecture

Having undertaken extensive work in critical infrastructure projects Provecta has proven experience in designing and implementing secure and resilient network architectures to maximise system availability.

Network architecture design and implementation services provided by Provecta include:

- Network switching and routing
- Segmentation and zoning
- Demilitarized Zones (DMZs) for external access
- Secure Wireless systems
- Network device configuration and security hardening
- Redundancy and fault tolerance

2.4 Server and System Architecture

Provecta has implemented Operation Technology solutions for multiple customers. Our system-based solutions are individually designed to meet customer requirements depending on the size of the system, risk profile and underlying control system infrastructure. Where appropriate, solutions are aligned to the customers' existing control system or corporate IT solutions to leverage existing support and/or purchasing agreements.

System architecture design and implementation services provided by Provecta include:

- Virtualisation solutions
- Windows Active Directory
- Secure File Transfer Systems
- Backup and Recovery Systems
- Centrally managed anti-malware
- Centrally managed patch management
- System security hardening
- System monitoring

Provecta works with a range of technology suppliers to delivery these solutions including Microsoft, Hewlett Packard, Hewlett Packard Enterprise, Veeam, Symantec Enterprise, Sophos, McAfee, PRTG.

2.5 Integration and Protection of Legacy Systems

Control and monitoring systems typically have long life cycles compared to similar IT based systems. It is often not practical or cost effective to upgrade or replace existing control/monitoring systems, however there is still a requirement to interconnect systems to provide access to data or for support purposes.

Working in asset intensive industries that can have long upgrade cycles, Provecta has regularly encountered this issue and has designed and developed appropriate strategies to support and integrate legacy systems in current systems. Solutions are designed to manage the security of systems and to ensure that appropriate disaster recovery facilities are available.

2.6 Corporate IT Integration and Data Solutions

Integration of data from Operational Technology systems to corporate systems is essential to allow management and support staff to make real time decisions, as well as provide long term historical records of plant performance.

Provecta designs and implements systems to enable the secure interchange of data between corporate and operational technology systems. Depending on requirements this may range from simple file transfer processes through to implementation of corporate data historians such as OSI PI, Wonderware Historian or Yokogawa Exaquantum.

2.7 System Security Hardening

Provecta develops security baselines across the range of systems it encounters to harden systems and minimise the risk of a cyberattack. Security hardening baselines have been developed for the complete range of OT equipment including servers, server operating systems, network equipment and control system hardware and are built on industry standards and best practices.

2.8 Secure Remote Access Systems

Remote access is essential for today's mobile workforce – both to provide workers with immediate access to data, and to provide specialist support services. Provecta develops secure remote access systems based on the criticality and security profiles of the systems being accessed.

2.9 OT System Configuration Management

Configuration management of OT systems such as PLCs, network equipment and other control equipment is essential for backup purposes and for management of change. Manual change management processes may not always capture every change. An automatic configuration change management solution can resolve many issues including:

- Scheduling backups to maintain a master backup repository
- Detecting any unauthorised changes
- Ensuring the current version of the configuration is available for disaster recovery purposes.

2.10 Disaster Recovery

Disaster recovery planning is key to ensuring that systems can be restored to operation following failure – whether the failure has been caused by hardware failure, environment factors or a cyber-attack.

Provecta works with our clients to determine appropriate recovery time and recovery point objectives for systems to determine a suitable backup strategy based on the criticality of the system.

Appropriate backup systems (including offline backups) can then be designed and implemented to meet the desired disaster recovery objectives.

A key aspect of this is the preparation of appropriate disaster recovery plans that document the recovery process in detail to ensure a successful recovery of the system.

Provecta also provides disaster recovery testing services where the disaster recovery plans are exercised to confirm the validity of backups and that the documented processes work as designed.

2.11 Incident Response and Business Continuity

Building on the disaster recovery processes, Provecta provides services to develop incident response and business continuity planning for Operational Technology systems.

Working with stakeholders across the business, Provecta has experience in developing incident response plans for the operational technology systems that integrate with and support the company's overall business continuity strategy.

2.12 Documentation and Drawings

Having detailed and accurate documentation and drawings for systems is essential for maintenance and fault-finding purposes.

Provecta provides extensive documentation for systems it implements and can also develop documentation and drawings for existing systems:

- Hardware and software asset inventories
- Detailed system build procedures
- Maintenance procedures
- System architecture drawings

2.13 System Audits

Provecta is regularly engaged to undertake audits of existing operational technology systems. Audits may be undertaken to develop a baseline for the system configuration (if no existing documentation is available) or to verify that existing documentation and drawings are accurate.

Audits include:

- Physical audits of installed equipment and connections
- Network audits (architecture, port layouts etc).
- Equipment and server configuration verification against as-built documentation
- System hardening and security posture
- Cybersecurity implementation

Audit reports are prepared detailing the findings and providing recommendations for future improvements.

2.14 Upgrades and Modernisation

Provecta provides solutions for systems that have reached the end of their supportable life and require modernisation.

As Provecta is actively working in the control system space, we understand the requirements and implications of upgrading the Operational Technology to underlying control and monitoring systems. We can provide a complete upgrade solution covering OT systems, and control system hardware and software.

This may include hardware refresh, software upgrades and/or replacement of control system hardware.

3 PROJECT CAPABILITIES

Provecta has experience in all aspects of implementing controls projects, from assessment and concept through to implementation and system optimisation. Provecta performs consulting assignments as well as design and construct contract projects. Our diverse portfolio of consulting services in the Operational Technology and Cybersecurity area includes:

- Project definition and specification preparation
- Preparation of conceptual and standard designs
- System architecture design
- System implementation – including procurement, configuration and commissioning
- System audits and investigations
- Expert and technical advisory services
- Project management
- Ongoing system management, support and monitoring

4 REFERENCE EXPERIENCE AND PROJECTS

Provecta has been engaged to provide engineering services on a large number of projects in the operational technology field. The engineering services provided have encompassed a variety of roles including consulting assignments (from project concept development, specification preparation, tender analysis, tender negotiation, design reviews), detailed engineering (project management, design, configuration and commissioning) to ongoing support services (system support, DR testing and maintenance). A brief summary of some of these recent projects is included below. Further examples and referees can be provided upon request.

4.1 Power Generation – NSW (Customer - Confidential)

Provecta was engaged by a major generator within the National Electricity Market to integrate a newly purchased site with their existing corporate IT systems and to align the OT security posture with their established standards. The project included:

- Design and implementation of a new network architecture with increased segmentation of systems into security zones based on the criticality and connectivity of the systems
- Design and implementation of a new DMZ for all external connections to the systems
- Relocation of a number of legacy systems from the corporate environment to the OT environment
- Implementation of a new firewall architecture within the OT environment for connections to the corporate environment
- Implementation of a new high availability VMWare environment with 3PAR storage for the DMZ systems
- Implementation of OSI PI Historian with connectivity to their existing corporate historian, including backfill of old data
- Provision of a new backup system and preparation and testing of disaster recovery plans for the system
- Implementation of improved security hardening of operating systems and network devices

- Preparation of incident response plans

The upgraded architecture interconnected over fifteen different control and monitoring systems.

Provecta continues to manage and maintain the system, including enhancements and modifications as existing systems are upgraded, and new systems are brought online.

4.2 Power Generation – Stanwell Corporation

Provecta was engaged by Stanwell Corporation to upgrade the existing DMZ between the corporate network and the control systems at one of their sites. The design of the existing DMZ was over 10 years old, running non-supported hardware did not meet their requirements of their current security policies.

The scope of work undertaken by Provecta included:

- Development of a detailed design for the DMZ architecture including network architecture, firewall replacement, support software and redundancy
- Design and implementation of new firewalls and implementation of security zones
- Co-ordination of network, firewall and routing changes with corporate IT staff
- Implementation of a VMWare environment for the DMZ systems
- Provision of a new backup system (including offline storage)
- Preparation of documentation and drawings for the system
- Commissioning of the upgraded systems and decommissioning of old systems

Provecta's design has now been adopted as the standard for implementation at a number of Stanwell Corporation sites.

4.3 Control System Wireless Access (Customer - Confidential)

Provecta was engaged to provide a secure wireless system to allow plant technicians and operators to remotely access the site control systems via dedicated tablet computers. The solution empowered technicians and operators with real-time data to resolve faults and make operational decisions while working in the plant. The project included:

- Design and specification of the wireless network including over 220 new Cisco wireless access points and 28 new Cisco switches connected via a blown tube fibre backbone
- Implementation of a secure remote access system using Cisco Identify Services Engine (ISE) and Cisco AnyConnect VPN to protect wireless connections to the OT systems
- Implementation of a Citrix XenApp farm including Citrix Gateway to present the visualisation layer to the remote users to remove direct connectivity requirements between the wireless clients and the critical control system networks
- Deployment of locked down Windows 10 based industrial tablets for remote access including GPS monitoring of equipment location

5 SYSTEM EXPERTISE

5.1 Control System Vendors

Provecta works with a wide range of vendor systems in the control system space. Our experience in developing Operational Technology solutions includes:

- Yokogawa Centum CS, CS3000 and VP DCS
- Siemens T3000 DCS
- Toshiba TOSMAP DCS
- Schneider Electric Geo SCADA Expert (ClearSCADA)
- AVEVA Wonderware System Platform
- AVEVA CitectSCADA
- Allen Bradley, Schneider Electric, Siemens PLCs (amongst many others).
- OSI PI

5.2 Operational Technology Vendors

Provecta works with a range of technology suppliers to deliver these solutions. Major vendors include:

- Microsoft
- Hewlett Packard
- Hewlett Packard Enterprise (including 3PAR)
- Dell
- Cisco
- Fortigate
- Sonicwall
- Aruba
- Tofino
- Veeam
- Symantec
- Solarwinds
- Sophos
- McAfee
- PRTG
- Moxa
- Hirschman
- Advantech

6 CONTACT DETAILS

If you wish to contact Provecta to learn more or discuss Provecta capacity to assist deliver your project please contact either:

- Mr Anthony (Tony) Buncombe, Managing Director
  anthony.buncombe@provecta.com.au
  P 02 8204 5420
  M 0400 496 349
- Mr Andrew Oates, Director - Business Development
  andrew.oates@provecta.com.au
  P 02 8204 5410
  M 0408 256 039