Citicus ICS – Risk management for industrial control systems

Citicus ICS is a special implementation of our award-winning web-based **Citicus ONE** software that is optimized for measuring and managing risks to industrial control systems (ICS). These include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and other technologies used to automate industrial processes, eg using programmable logic controllers (PLC) and remote telemetry units (RTU).

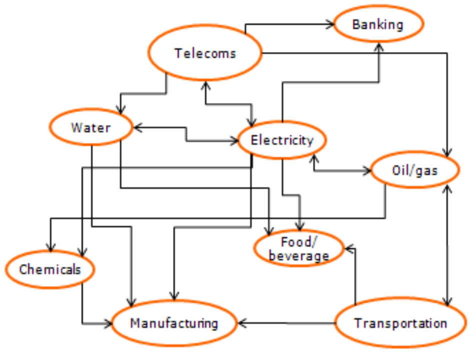
Such real-time systems have particular characteristics that need to be taken into account to yield a risk management process that is viable and optimized for the industrial control system environment.

Characteristics of industrial control systems

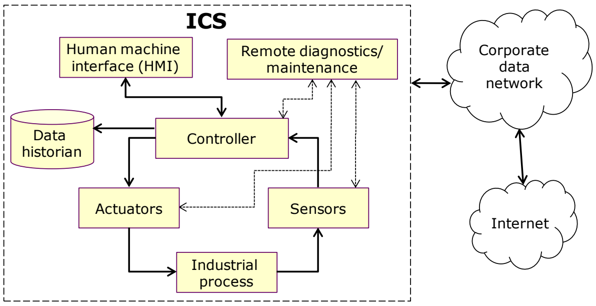
Effective risk management is crucial, since industrial control systems underpin the critical national infrastructure and are essential for the success of critical industries such as:

- electricity production and distribution
- water supply and treatment
- food production
- oil and gas production and supply
- chemical and pharmaceutical production
- telecommunications
- manufacturing of components and finished products
- paper and pulp production.

Disruption of these industries can have a rapid and escalating effect on society. This is exacerbated by the high-levels of interdependence between the critical industries as illustrated in the diagram below.



The implementation of automated control systems across these different industrial processes varies in detail but generally follows a common 'control architecture' as illustrated below.



Such architectures are made up of**:**

- A **control loop** consisting of actuators such as valves, switches and motors; sensors that detect the status of variables associated with the industrial process (eg temperature, pressure, flow rates) and a controller that manages the actuators based on sensor readings and operator input.
- A **human-machine interface** (HMI) that allows operators to monitor the controlled process and influence it
- A **data historian** that logs all process control activity to allow reporting at multiple levels
- **Remote diagnostics and maintenance** that allows ICS support staff and vendors access to diagnose and correct operational problems.

ICS security challenges

The importance and nature of industrial control systems creates particular challenges for ensuring their continued security. Some of the factors that set them apart from standard application systems are:

- SCADA systems are often highly distributed geographically with limited physical security for field devices.
- Many ICS components (particularly remote telemetry units) are legacy devices that provide limited security features and little prospect of firmware upgrades.
- Security patch management is a challenge as changes need to be kept to a minimum to avoid the risk of ICS disruption through the unexpected side effects of operating system, or application changes.
- Network protocols are typically unauthenticated and transmit in plain text.
- A migration from closed, proprietary protocols and operating systems to open source or COTS technology means that documented information about architecture is more readily available.
- As the primary operational requirement is continuous and correct function, many security features are not tolerated if they risk compromising these objectives; for example anti-virus software, IDS/IPS, operator lock-out through repeated bad passwords, etc often cannot be implemented.
- Nation states with substantial resources are motivated to invest considerable effort into finding and exploiting weaknesses in systems that contribute to their enemies' critical national infrastructure.

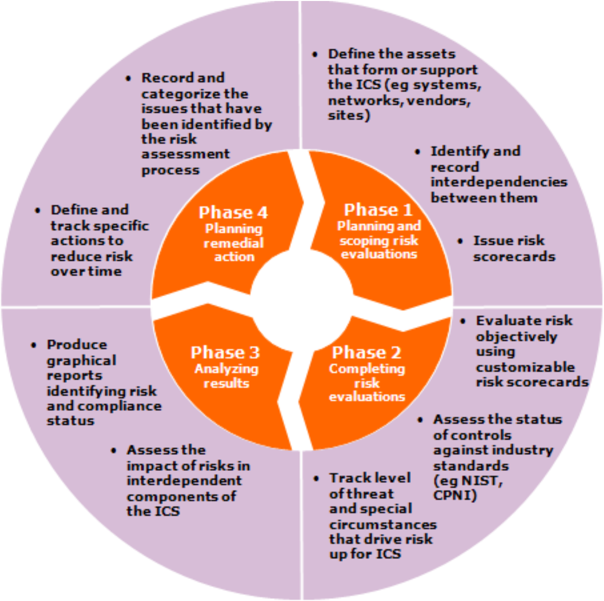
Whereas, in the past process control networks were effectively protected by an 'air gap' segregating them from other internal and external systems; this is generally no longer the case and firewalls with complex rule sets are now needed to replace the air gap.

Information security and risk practitioners are often surprised at the impact these differences have on the approaches that can be taken to managing risk.

Securing your industrial control systems

Citicus ICS was developed through a UK Government research grant awarded to Citicus and its industrial partners for innovation in protection of critical national infrastructure. It provides a platform for managing risk that brings together the skills and experience of IT risk experts and ICS engineers with specialist knowledge of their environment and its requirements.

Citicus ICS supports a complete security / risk management lifecycle that follows the four-phase **Plan-Do-Check-Act** process illustrated below.


Phase 1
Planning and scoping risk evaluations
• Define the assets that form or support the ICS (eg systems, networks, vendors, sites)
• Identify and record interdependencies between them
• Issue risk scorecards
Phase 2
Completing risk evaluations
• Evaluate risk objectively using customizable risk scorecards
• Assess the status of controls against industry standards (eg NIST, CPNI)
• Track level of threat and special circumstances that drive risk up for ICS
Phase 3
Analyzing results
• Assess the impact of risks in interdependent components of the ICS
• Produce graphical reports identifying risk and compliance status
Phase 4
Planning remedial action
• Define and track specific actions to reduce risk over time
• Record and categorize the issues that have been identified by the risk assessment process

Together with local co-ordinators in subsidiary parts of your enterprise, you can use **Citicus ICS** to:

- define and characterize individual ICS assets and processes (including external suppliers and administrative systems that they depend on)
- issue criticality assessments, risk scorecards and supporting checklists that ICS 'owners' can complete on-line
- oversee evaluations (eg chasing late responses, accepting completed scorecards and assessments or returning them for correction)
- consolidate collected risk and compliance data into informative results for decision-makers
- develop and manage ICS remediation plans.

How risk is evaluated

The **Citicus ICS** risk scorecard that is central to this process probes five key factors that determine or indicate the level of risk posed by an industrial control system. These five factors are identified below.

Criticality	This is evaluated by identifying the maximum potential impact of ICS incidents leading to a loss of availability of the process control capability, integrity of control data or confidentiality of information. Availability disruption can be measured on a scale from milliseconds to days or longer, depending on the nature of the controlled process.
Status of controls	The status of controls is assessed against a library of industry best practice controls drawn from many sources such as CPNI *Good Practice Guides to process control and SCADA security* and NIST *800-82.* Organizations can use the Citicus-supplied control framework off-the-shelf or augment/replace it with their own set of controls.
Special circum-stances	Particular characteristics of the ICS are identified that can heighten the probability of incidents, such as high degree of change, complexity, interconnection to other systems, accessibility by external parties.
Level of threat	A further indicator of incident probability is gained by identifying experience of actual incidents such as malfunctions, human error, malicious action, disruption from environmental events.
Business impact	The actual business harm caused by previous ICS incidents, if any is also assessed. Harm is measured in an objective and consistent way and covers all types of business impact such as financial loss, reputational damage, environmental and safety impacts.

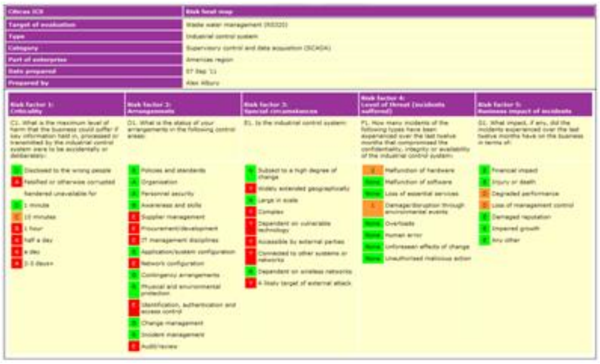
Citicus ICS risk reporting

Citicus ICS provides high-quality graphical reports for all those with an interest in the status of industrial control system risk across the enterprise. This includes 'owners' of individual industrial control systems and senior management with responsibility for risk across the organization.

Examples of reports produced by **Citicus ICS** include:

- **Risk status reports** and **risk heat maps** for individual ICS implementations and their component parts
- **Compliance status** and **trend reports** benchmarking industrial control systems according to their compliance with a specified set of controls, such as relevant NIST and CPNI standards
- **Risk dashboard** showing the overall level of ICS risk across the enterprise and its key drivers
- **High-level risk status report** showing key industrial control system risk factors for the enterprise and the impact of actual ICS-related incidents
- **Risk league table** ranking different industrial control systems and/or their components parts according to their measured risk
- **Dependency risk maps** showing relationships between ICS components and other assets and processes from a risk perspective
- **Incident statistics** including breakdowns by type of incident, their cause and impact on the business.

Results produced by **Citicus ICS** are designed so that they can be readily understood by business people as well as those fulfilling specialized roles.



Citicus ICS	Risk heat map
Target of evaluation	Waste water management (RS320)
Type	Industrial control system
Category	Supervisory control and data acquisition (SCADA)
Part of enterprise	Americas region
Date prepared	07 Sep '11
Prepared by	Alex Albury

Risk factor 1: Criticality

C1. What is the maximum level of harm that the business could suffer if key information held in, processed or transmitted by the industrial control system were to be accidentally or deliberately:

- 🟩 Disclosed to the wrong people
- 🟥 Falsified or otherwise corrupted
- Rendered unavailable for
- 🟩 1 minute
- 🟧 15 minutes
- 🟥 1 hour
- 🟥 half a day
- 🟥 a day
- 🟥 2-3 days+

Risk factor 2: Arrangements

D1. What is the status of your arrangements in the following control areas:

- 🟩 Policies and standards
- 🟩 Organisation
- 🟩 Personnel security
- 🟩 Awareness and skills
- 🟥 Supplier management
- 🟥 Procurement/development
- 🟥 IT management disciplines
- 🟩 Application/system configuration
- 🟥 Network configuration
- 🟩 Contingency arrangements
- 🟩 Physical and environmental protection
- 🟥 Identification, authentication and access control
- 🟩 Change management
- 🟩 Incident management
- 🟥 Audit/review

Risk factor 3: Special circumstances

E1. Is the industrial control system:

- 🟩 Subject to a high degree of change
- 🟥 Widely extended geographically
- 🟩 Large in scale
- 🟥 Complex
- 🟥 Dependent on vulnerable technology
- 🟥 Accessible by external parties
- 🟥 Connected to other systems or networks
- 🟩 Dependent on wireless networks
- 🟥 A likely target of external attack

Risk factor 4: Level of threat (incidents suffered)

F1. How many incidents of the following types have been experienced over the last twelve months that compromised the confidentiality, integrity or availability of the industrial control system:

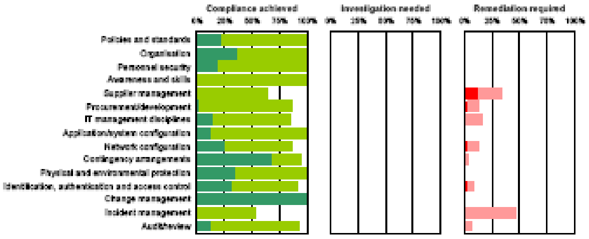
- 🟧 Malfunction of hardware
- None Malfunction of software
- None Loss of essential services
- 🟧 Damage/disruption through environmental events
- None Overloads
- None Human error
- None Unforeseen effects of change
- None Unauthorised malicious action

Risk factor 5: Business impact of incidents

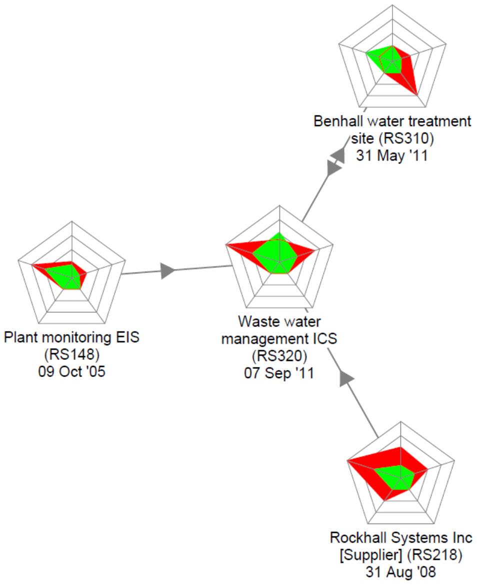
G1. What impact, if any, did the incidents experienced over the last twelve months have on the business in terms of:

- 🟩 Financial impact
- 🟩 Injury or death
- 🟧 Degraded performance
- 🟧 Loss of management control
- 🟩 Damaged reputation
- 🟩 Impaired growth
- 🟩 Any other

Sample risk heat map



Sample compliance status chart

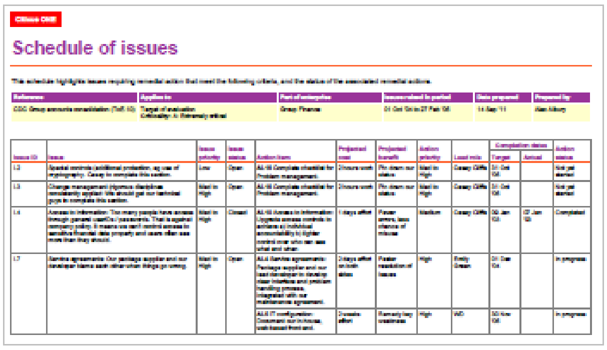


Sample of a dependency risk map

Remediation activity planning

Citicus ICS records key **issues** raised by risk assessments and maintains **action plans** to help manage them through to resolution. Issue schedules and action plan are maintained at three levels:

- For **individual ICS components** enabling their 'owners' to identify and manage the control improvements called for by risk and compliance evaluations
- For **specific parts of the enterprise**, enabling local co-ordinators to identify and manage actions they need to take within their business units
- For **the enterprise as a whole**, enabling risk managers to identify and manage actions needed at corporate level (eg new policies, standards or procedures).



Citicus ONE

Schedule of issues

[illegible]

Reference	Applies to	Part of enterprise	Issues raised in period	Date prepared	Prepared by
[illegible]	Target of evaluation Criticality: [illegible]	Group Finance	[illegible]	11 Sep '11	Alex Albury

Issue ID	Issue	Issue priority	Issue status	Action item	Projected cost	Projected benefit	Action priority	Lead role	Completion dates		Action status
									Target	Actual	
I2	[illegible]	Low	Open	[illegible]	2 hours work	[illegible]	Med to High	[illegible]	01 Oct 08		Not yet started
I3	[illegible]	Med to High	Open	[illegible]	2 hours work	[illegible]	Med to High	[illegible]	01 Oct 08		Not yet started
I4	[illegible]	Med to High	Closed	[illegible]	1 days effort	[illegible]	Medium	[illegible]	30 Jan 09	07 Jan 09	Completed
I7	[illegible]	Med to High	Open	[illegible]	3 days effort	[illegible]	High	[illegible]	01 Dec 08		In progress
				[illegible]	[illegible]	[illegible]	High	[illegible]	30 Nov 08		In progress

Sample Schedule of issues

Deploying Citicus ICS

Citicus ICS has a highly flexible licensing model allowing implementations on any scale. It is available as a:

- Server-based software application installed in-house and accessed across your corporate intranet
- Single-user desktop or laptop implementation suitable for a localized project
- a hosted 'on-demand' service from Citicus, accessed over the Internet, capable of handling multi-site deployments.

Multi-lingual capability

Citicus ICS provides multi-lingual support in the following languages:

Dutch	French
English (UK)	German
English (US)	Japanese.

Additional languages can be accommodated, at extra cost.

Contact details

For further information about **Citicus ICS**, please contact us as follows:

Head office

Citicus Limited
71-75 Shelton Street, Covent Garden
London WC2H 9JQ
United Kingdom.

E-mail:	info@citicus.com
Web:	www.citicus.com
Tel:	+44 (0)20 3126 4999.