dexcent

STRATEGIZE | TRANSFORM | EVOLVE

PROACTIVE MAINTENANCE FOR AVEVA™ ENTERPRISE SCADA:

How Pipeline Operators Reduce Downtime, Strengthen Compliance & Cut OPEX Waste Before It Happens

DEXCENT.COM | (833) 482-4100 | SALES@DEXCENT.COM

EXECUTIVE SUMMARY

Pipeline operators running **AVEVA™ Enterprise SCADA** are under pressure to deliver reliable operations with aging infrastructure, tighter compliance expectations, and limited internal capacity. In many environments, maintenance becomes reactive by default: teams stabilize incidents quickly, but the underlying conditions that create repeat failures remain in place. The result is predictable OPEX waste through repeat triage, forced change windows, operator workarounds, and audit evidence scrambles.

This eBook reframes reliability as a discipline that must be engineered, not hoped for. Proactive maintenance is defined as an operating rhythm built on four pillars:

VISIBILITY
Detect weak signals early

STABILITY
Govern change and maintain patch discipline

PERFORMANCE
Prevent drift that erodes operator confidence

DOCUMENTATION
Make reliability repeatable across shifts and turnover

When these pillars are inconsistent, organizations see the same symptoms repeatedly: alarm overload, patch deferral, latency-driven workarounds, hygiene-related rework, and fragile recovery readiness.

Readers will learn how to translate proactive maintenance into a business case leadership understands, using recurrence reduction as the primary ROI lever.

ONBOARDING > ONGOING SUPPORT > DIGITAL EXPERIENCE > CONTINUOUS IMPROVEMENT

The eBook outlines a practical delivery model, guidance for defining service levels without formal SLAs, pipeline-relevant KPIs to track progress, and a clear build-versus-partner decision rubric. It concludes with a maturity model checklist to benchmark current readiness and prioritize the next best step:

ELIMINATE ONE RECURRING CLASS OF PROBLEMS END-TO-END, DOCUMENT THE FIX, AND EMBED PREVENTION INTO THE MAINTENANCE CADENCE.

CHAPTER 1

The Hidden Costs of a Reactive Enterprise SCADA Culture

REACTIVE MAINTENANCE IS NOT IRRATIONAL

In a critical control environment, it often feels like the only responsible option. Operators need stability now. Operations needs throughput now. Leadership needs risk contained now.

The issue is that reactive maintenance is a reliability strategy built on lagging indicators. It waits for disruption, then responds. In AVEVA™ Enterprise SCADA, that produces a predictable outcome: issues repeat, costs accumulate, and the environment drifts until a failure forces attention.

Reliability is no longer "BY CHANCE." It must be "BY DESIGN."

1.1 "STABLE ENOUGH" IS OFTEN UNMEASURED FRAGILITY

Many teams equate "system up" with "system stable." In Enterprise SCADA, uptime can hide instability. A system can be operational while:

- **Response time** slowly degrades
- **Alarms drift** into noise
- **Databases accumulate** clutter and growth pressure
- **Redundancy exists**, but failover behaviour is not verified
- **Patch posture drifts** further from recommended baselines

This is why **"we've been fine for years"** is not a reliability statement. It is a lagging observation.

IF THE INCIDENT ONLY BECOMES REAL WHEN IT IS PAINFUL, YOUR RELIABILITY PROGRAM BEGINS TOO LATE.

1.2 WHY REACTIVE MAINTENANCE PERSISTS

Reactive maintenance persists because it feels efficient in the moment:

1. **It optimizes for the urgent.** The loudest pain gets attention first.
2. **It rewards heroics.** The late-night fix is visible. Prevention work is quiet.
3. **It hides true cost.** Repeat work is absorbed into OPEX as "normal operations."

Over time, this trains the organization to prioritize firefighting over prevention, even when prevention would cost less.

1.3 WHERE THE MONEY LEAKS (AND WHY IT'S HARD TO SEE)

Reactive cultures create hidden costs that don't show up neatly on a single line item. In Enterprise SCADA, they typically leak in four places.

A) REPEAT TRIAGE

Recurring issues carry recurring overhead: re-diagnose, re-build context, re-test, re-communicate. Even when the fix is fast, the repeated effort is not.

If the same class of issue repeats, you are not paying for reliability. You are paying for recurrence.

B) CHANGE RISK AMPLIFICATION

Reactive fixes happen under time pressure, which increases compromise: changes without rollback planning, patching without full validation, documentation deferred, and workarounds that become permanent. This creates change debt, which makes future changes more risky and increases drift.

C) OPERATOR CONFIDENCE EROSION

In SCADA, a high-cost failure mode is decision friction. If operators don't trust what they see, they compensate with extra confirmations, extra calls, and delayed decisions. That adds operational drag and raises risk under abnormal conditions.

D) AUDIT AND COMPLIANCE SCRAMBLE

Compliance pressure isn't only policy. It's evidence. If patch posture, governance, redundancy checks, and operating procedures are informal, the organization ends up scrambling when asked to prove readiness.

1.4 PROACTIVE MAINTENANCE DEFINED

(IN ENTERPRISE SCADA TERMS)

Proactive maintenance is not a quarterly checkup. It is an operating rhythm that reduces recurrence by design. The discipline is simple, and it rests on four pillars:

1. **Visibility:** detect weak signals early
2. **Stability:** govern change and maintain patch discipline
3. **Performance:** prevent drift that impacts operator experience
4. **Documentation:** make reliability repeatable and resilient to turnover

Reactive maintenance responds to incidents. Proactive maintenance reduces the number of incidents that occur in the first place.

1.5 A REALITY CHECK ON REDUNDANCY

Enterprise SCADA architectures are designed around redundancy for a reason. But there is a practical truth most teams learn the hard way:

If redundancy isn't validated, it isn't a reliability capability. It's an assumption.

Proactive maintenance makes redundancy real by treating it as an operational capability that must be checked and verified, not a checkbox that can be trusted indefinitely.

1.6 WHAT TO DO IN THE NEXT 30 DAYS

You don't need a major project to start improving reliability. You need cadence.

WEEK 1: BASELINE

- **Identify** top recurring incident classes from the past 90 days
- **Capture** recurring operator pain points
- Document current monitoring, patch, and change habits

WEEK 2: PUT MONITORING ON THE CALENDAR

- **Schedule** two weekly monitoring blocks
- **Define** what gets checked and how findings become a backlog

WEEK 3: FIX ONE RECURRING ISSUE END-TO-END

- **Pick one** recurring class of issue and finish it fully, including documentation. **One solved problem beats five half-fixes.**

WEEK 4: TURN EXECUTION INTO GOVERNANCE

- **Review** outcomes
- **Define** next month's priorities
- **Confirm** how you will track evidence and KPIs

RELIABILITY IMPROVES WHEN YOU REDUCE RECURRENCE, NOT WHEN YOU INCREASE ACTIVITY.

1.7 THE SHIFT THIS CHAPTER IS ASKING YOU TO MAKE

If this chapter does its job, it changes the mental model:

- **"Stable Enough"** is often unmeasured fragility
- **Reactive Work** is an operating tax
- **Proactive Maintenance** is a cadence, not a project
- **Redundancy Only Delivers Reliability** when it is maintained and validated

CHAPTER 2

Enterprise SCADA Is Not **“Set It and Forget It”**

ENTERPRISE SCADA ENVIRONMENTS DO NOT STAY STABLE ON THEIR OWN. THEY DRIFT.

That drift is rarely dramatic at first. It shows up as small changes in performance, alarm behavior, database growth, patch posture, and operator experience. The system stays "up," so the organization assumes it is fine. Then a routine change window, a forced patch, or an unexpected load condition exposes how much fragility has accumulated.

The outline calls this out directly: Enterprise SCADA is a multi-tier distributed system with RealTime services, applications, databases, displays, scripts, reports, and ongoing patch and hotfix behavior that requires domain expertise to manage well.

IN ENTERPRISE SCADA, RELIABILITY IS NOT A STATE YOU REACH. IT IS A CONDITION YOU MAINTAIN.

2.1 COMPLEXITY CREATES HIDDEN SINGLE POINTS OF FAILURE

When teams talk about single points of failure, they often focus on hardware. In Enterprise SCADA, single points of failure are frequently operational:

- A critical workflow exists only in one person's head.
- A display or script is **"too risky to touch,"** so it never gets improved.
- Patching is delayed until it becomes urgent.
- Redundancy exists on paper, but failover behavior is unverified.

Complexity is manageable when it is governed. It becomes dangerous when it is merely tolerated.

2.2 THE DRIFT PROBLEM HAPPENS BETWEEN PROJECTS

Projects stabilize systems at go-live. Operations then inherits an environment that changes continuously:

- **Configuration adjustments to meet operational needs**
- **Hotfix and patch decisions over time**
- **Evolving operator usage patterns**
- **New reporting and interface demands**
- **Turnover and knowledge gaps**

This is why **"we'll clean it up later"** rarely happens. Later gets consumed by the next incident.

DRIFT IS WHAT HAPPENS WHEN RELIABILITY WORK HAS NO CALENDAR SPACE. INCIDENT WORK ALWAYS WINS.

2.3 PROACTIVE MAINTENANCE IS A RHYTHM, NOT A CLEANUP EVENT

A proactive program begins with a simple operational rule:

Schedule reliability work the same way you schedule operational work.

The Service Offering model defines a practical baseline for preventive attention as **2 to 4 hours of Enterprise SCADA system monitoring on a twice-weekly basis.** The importance is not the exact number. The importance is the discipline: recurring monitoring produces findings, findings produce actions, and actions reduce recurrence.

The offering also notes that Enterprise SCADA is regularly upgraded to assure reliability and performance, and that customers maintain and extend their investment by upgrading from one version to the next to respond to new challenges and opportunities. The operational takeaway is straightforward:

Upgrades, patching, performance tuning, and hygiene are not exceptions. They are part of the lifecycle.

2.4 WHAT MIDDLE MANAGEMENT NEEDS TO LEAD

As a SCADA leader in middle management, you own the intersection of operational pressure and budget reality. The most useful mindset shift is this:

- **Reactive work** is not proof of control. It is proof the system is pulling you into response mode.
- **Proactive work** is not "extra." It is how you reduce repeat work and forced change.

Your job is not to eliminate every incident. Your job is to reduce the incidents that are predictable, recurring, and preventable.

YOUR BEST LEVERAGE IS REDUCING RECURRENCE.
THAT IS WHAT CREATES CAPACITY WITHOUT ADDING HEADCOUNT.

2.5 THE PRACTICAL OUTCOME OF THIS CHAPTER

If Chapter 2 does its job, it equips you with a clear internal message:

1. **Enterprise SCADA complexity is structural, not temporary.**
2. **Drift accumulates unless you run a consistent maintenance rhythm.**
3. **A proactive rhythm is schedulable, measurable, and repeatable.**
4. **Lifecycle upgrades are part of operational reliability, not just project work.**

CHAPTER 3

The Four Pillars of Proactive Maintenance in AVEVA™ Enterprise SCADA

PROACTIVE MAINTENANCE IS NOT A SLOGAN.

Proactive maintenance is not a slogan. It is a set of repeatable practices that prevent drift from turning into outages, forced change windows, and recurring incidents.

This chapter defines the Four Pillars that make proactive maintenance practical and defensible in an AVEVA™ Enterprise SCADA environment: Visibility, Stability, Performance, and Documentation.

IF YOU WANT PREDICTABLE RELIABILITY, YOU NEED PRACTICES THAT RUN EVEN WHEN NOTHING IS BROKEN.

3.1 PILLAR 1: VISIBILITY AND EARLY DETECTION

Visibility is the ability to detect weak signals early enough that you can act during normal working hours, not during incident response.

The outline calls out Enterprise SCADA visibility practices that matter:

- **Error Log Analysis**
- **Alarm Trending**
- **Application Performance Checks**
- **Database Hygiene**
- **Display Performance Diagnostics**

WHAT "GOOD" VISIBILITY LOOKS LIKE

- Monitoring produces a short list of findings, not a vague "looks fine."
- Findings are classified by risk and recurrence likelihood.
- Findings become actions and get closed with simple documentation.

IF YOUR MONITORING OUTPUT IS "EVERYTHING LOOKS FINE," YOU ARE GLANCING, NOT MONITORING.

3.2 PILLAR 2: STABILITY THROUGH GOVERNANCE AND PATCH DISCIPLINE

Stability is controlled change. It is how you protect reliability while the environment evolves.

THE OUTLINE LINKS STABILITY TO:

- Scheduled hotfix and patch management
- Change governance
- Version alignment across Liquids and Gas applications

WHAT "GOOD" STABILITY LOOKS LIKE

- You can answer quickly:
- What changed?
- Why did it change?
- What was the expected impact?
- What did we validate?

IF YOUR PATCH STRATEGY IS "WE'LL DO IT WHEN WE HAVE TIME," IT WILL BECOME "WE'LL DO IT WHEN WE ARE FORCED."

- What is the rollback path?

3.3 PILLAR 3: PERFORMANCE OPTIMIZATION

Performance is not cosmetic in SCADA. It directly affects operator confidence and decision quality.

THE OUTLINE CALLS OUT PERFORMANCE PRACTICES, INCLUDING:

- Application fine-tuning
- Script, ACE, and action sequence optimization
- Display refactoring
- Slow-point remediation

WHAT "GOOD" PERFORMANCE LOOKS LIKE

- Slow points are identified early and fixed systematically.
- High-friction displays are refactored before workarounds become standard behaviour.
- Best practices are captured so the same issues do not get reintroduced.

WHEN PERFORMANCE DETERIORATES, OPERATORS COPE FIRST. BY THE TIME TICKETS APPEAR, DRIFT HAS OFTEN BEEN BUILDING FOR WEEKS.

3.4 PILLAR 4: DOCUMENTATION AND REPEATABILITY

Documentation is not overhead. It is how reliability survives turnover and operating pressure.

THE OUTLINE INCLUDES:

- Standard Operating Procedures
- Training and Knowledge Retention
- Redundancy and Backup Health Checks

WHAT "GOOD" DOCUMENTATION LOOKS LIKE

- SOPs exist for the maintenance routines you actually run.
- Knowledge from incidents and changes is captured and reused.
- Backup and redundancy readiness is checked as an operating habit, not assumed.

IF RECOVERY DEPENDS ON CALLING "THE PERSON WHO KNOWS," YOU DO NOT HAVE A RECOVERY PLAN. YOU HAVE KEY-PERSON DEPENDENCY.

3.5 HOW THE FOUR PILLARS WORK TOGETHER

THE PILLARS REINFORCE EACH OTHER:

- **Visibility** finds weak signals early.
- **Stability** prevents risky change and version drift.
- **Performance** protects operator trust and reduces friction.
- **Documentation** makes reliability repeatable across shifts and turnover.

If one pillar is weak, the others work harder to compensate, and reliability becomes less predictable.

3.6 WHERE MOST TEAMS SHOULD START

If you are moving from reactive to proactive, do not try to build all four pillars at once.

A PRACTICAL SEQUENCE IS:

1. **Visibility** (so you can see drift)
2. **Stability** (so you can control change)
3. **Performance** (so operations feels improvement quickly)
4. **Documentation** (so gains stick)

THE FASTEST WAY TO BUILD SUPPORT IS TO ELIMINATE ONE RECURRING PROBLEM CLASS AND DOCUMENT THE PREVENTION STORY.

3.7 WHAT HAPPENS WHEN THE FOUR PILLARS ARE MISSING

When the pillars are missing or inconsistent, the same outcomes show up repeatedly in Enterprise SCADA operations:

- **Alarm overload** overwhelms the control room
- **Patch deferral** increases compliance exposure
- **Application latency** increases operational drag
- **Hygiene gaps** contribute to commissioning errors and rework
- **Documentation gaps** delay onboarding and slow incident recovery

This is why proactive maintenance is not a **"nice to have."** It is the operating foundation that keeps reliability predictable.

IT SHOWS UP AS REPEAT WORK, FORCED CHANGE WINDOWS, AND AVOIDABLE OPERATIONAL FRICTION.

CHAPTER 4

The OPEX Reality Check

Where Money Leaks in AVEVA™ Enterprise SCADA Operations

DEXCENT.COM | (833) 482-4100 | SALES@DEXCENT.COM

OPEX WASTE IN ENTERPRISE SCADA RARELY SHOWS UP AS A SINGLE DRAMATIC INVOICE.

It shows up as a pattern: repeat incidents, repeat escalations, repeat meetings, and repeat stabilization work that the business starts treating as normal.

This chapter gives you a clear way to describe SCADA maintenance economics to leadership: recurrence, interruption, and avoidable labor. The outline highlights common leak areas, including alarm overload, patch deferral, application latency, commissioning errors tied to hygiene issues, and documentation gaps that delay onboarding and recovery.

IF RELIABILITY WORK IS MOSTLY TRIAGE, YOU ARE FUNDING RECURRENCE.

4.1 LEAK #1: REACTIVE TRIAGE AS "NORMAL OPERATIONS"

Reactive triage often looks small in the moment, commonly framed as 0 to 1 hour to "take a look" and stabilize symptoms.

THE REAL COST IS WHAT SURROUNDS IT:

- Ramp-up time to rebuild context
- Stakeholder coordination and escalation overhead
- Validation under time pressure
- Rework when the first fix does not stick
- Reporting and evidence reconstruction after the fact

Now compare that to a proactive baseline that is scheduled and repeatable. The service model describes 2 to 4 hours of Enterprise SCADA system monitoring on a twice weekly basis. The goal is not the exact number. The goal is predictable execution that prevents repeat incidents and reduces surprises.

4.2 LEAK #2: ALARM OVERLOAD AND OPERATOR DRAG

Alarm overload leaks OPEX because it increases cognitive load and decision friction. The cost is not limited to the control room.

IT SPREADS:

- More calls to confirm conditions
- More unnecessary escalations
- More time distinguishing signal from noise
- Reduced confidence during abnormal operations

Alarm overload is a common symptom when proactive Visibility routines are missing, especially trending and remediation over time.

ALARM OVERLOAD IS NOT JUST AN ALARM PROBLEM.
IT IS A MAINTENANCE MATURITY PROBLEM.

4.3 LEAK #3: PATCH DEFERRAL AND FORCED CHANGE WINDOWS

PATCH DEFERRAL CREATES A TRAP:

- Patches get delayed because the system is "too critical to touch"
- Drift accumulates
- Defects, instability, or exposure forces urgency
- Patching happens under pressure, increasing the risk of mistakes
- The outline calls out patch discipline and governance as core stability practices for a reason.

THE OPEX IMPACT IS TWOFOLD:

- Higher-cost execution due to urgency and coordination overhead
- Higher likelihood of secondary issues because validation and rollback planning get compressed

FORCED CHANGE IS THE MOST EXPENSIVE CHANGE.
DISCIPLINE IS WHAT KEEPS CHANGE PLANNED.

4.4 LEAK #4: LATENCY THAT TRAINS WORKAROUNDS

Latency costs more than time. **It trains behaviour.**

When the system slows, operators compensate with workarounds and manual checks. That becomes an invisible cost, because it is spread across shifts and treated as normal friction.

The outline connects performance improvement to practices like display refactoring and slow-point remediation.

> **PERFORMANCE DRIFT IS EXPENSIVE BECAUSE IT CHANGES HOW PEOPLE OPERATE LONG BEFORE ANYONE FILES A TICKET.**

4.5 LEAK #5: DOCUMENTATION GAPS THAT MULTIPLY EVERY INCIDENT

Documentation gaps multiply costs in three ways:

- **Onboarding takes longer,** so capability is slower to scale
- **Diagnosis takes longer,** so incidents last longer
- **More dependence on a small number of people,** increasing fragility

The outline treats documentation, training, and redundancy and backup health checks as core foundations of proactive maintenance, not administrative extras.

> **YOU DON'T FEEL DOCUMENTATION DEBT UNTIL YOU NEED IT. THEN YOU PAY FOR IT ALL AT ONCE**

4.6 WHAT TO SAY TO LEADERSHIP

If you need one sentence to use with leadership, use this:

Proactive maintenance reduces repeat labor, reduces forced change, and reduces operational drag.

The most defensible starting point is to formalize cadence and convert findings into a prioritized backlog, because cadence produces evidence and evidence builds support.

CHAPTER 5

The Business Case

Paying Once for a Solution vs Paying Repeatedly for a Recurring Problem

PAYING ONCE FOR A SOLUTION VS PAYING REPEATEDLY FOR A RECURRING PROBLEM

Middle management often gets trapped between two realities:

- Operations need reliability now.
- Leadership wants justification for any additional spend.

This chapter gives you a practical way to explain proactive maintenance in business terms, not as "maintenance cost," but as **recurrence reduction, risk reduction, and predictable execution.**

THE STRONGEST BUSINESS CASE IS NOT FEWER INCIDENTS IN GENERAL. IT IS FEWER REPEAT INCIDENTS.

5.1 THE COST MODEL THAT MAKES RELIABILITY UNDERSTANDABLE (60/15/15/10)

A proactive program is not just labour. It is a reliability system. A practical breakdown for building and sustaining that system is the **60/15/15/10 model:**

- **60%** Staffing
- **15%** Technology and tools
- **15%** Training and certification
- **10%** Contingency

This model matters because it reflects how reliability is created:

- People execute and close the loop on findings
- Tools provide visibility and reporting
- Training reduces key-person dependency and speeds resolution
- Contingency acknowledges operational reality

5.2 THE ROI DRIVER LEADERSHIP UNDERESTIMATES: RECURRENCE

Most leadership conversations focus on the cost of a proactive program. A better conversation focuses on the cost of recurrence.

RECURRENCE COSTS COMPOUND BECAUSE EACH REPEAT ISSUE CARRIES OVERHEAD:

- **Rebuilding** context
- **Coordinating** stakeholders
- **Validating** under time pressure
- **Redoing fixes** that do not stick
- **Post-incident reporting** and **evidence reconstruction**

Even when the immediate fix is quick, the repeat overhead is not.

IF THE SAME CLASS OF SCADA ISSUE REPEATS, YOU ARE NOT PAYING FOR RELIABILITY.
YOU ARE PAYING FOR REPEAT LABOUR.

5.3 THE LEADERSHIP REFRAME: YOU ARE ALREADY SPENDING THE MONEY

RELIABILITY SPEND HAPPENS EITHER WAY:

- You can spend intentionally **on prevention.**
- or you can spend reactively, **on interruption.**

REACTIVE SPEND IS HARDER TO TRACK BECAUSE IT IS DISTRIBUTED:

- **Internal labor** gets absorbed into **"support time"**
- **Urgent changes** pull in cross-functional teams
- **Vendor calls** happen under support or emergency categories
- **Operational drag** is treated as **"the cost of doing business"**

IF YOU DO NOT PAY FOR PREVENTION, YOU WILL PAY FOR INTERRUPTION.
THE DIFFERENCE IS WHETHER YOU GET TO CHOOSE THE TIMING.

5.4 TRANSLATING PROACTIVE MAINTENANCE INTO MEASURABLE RETURN

THE OUTLINE HIGHLIGHTS ROI OUTCOMES THAT MATTER IN PIPELINE ENVIRONMENTS:

- **Reduced downtime**
- **Lower cost of ownership**
- **Better compliance posture**
- **Fewer emergency spend events**
- **Retained knowledge**
- **Fewer support tickets over time**

TO MAKE THIS MEASURABLE, ANCHOR ROI TO THREE CATEGORIES:

A) Avoided interruption

- Fewer P1 events
- Fewer after-hours callouts
- Fewer urgent change windows

B) Avoided repeat labour

- Fewer recurring incident classes
- Faster diagnosis due to trend context
- Less rework on patches and configurations

C) Avoided compliance scramble

- Clear patch posture
- Documented governance and evidence trails
- Validated redundancy and backup readiness

**THE FASTEST ROI IS NOT PERFECTION.
IT IS ELIMINATING THE REPETITIVE PROBLEMS
THAT CONSUME THE SAME HOURS EVERY MONTH.**

5.5 “PAY ONCE” VS “PAY TWICE” EXPLAINED SIMPLY

Here is the simplest version of the business case.

PAY ONCE:

- **Identify** a recurring problem class
- **Remediate** the underlying condition
- **Document** the solution
- **Add** the prevention step to your cadence

PAY TWICE:

- Stabilize symptoms
- Skip documentation
- The issue returns
- Repeat the cycle under pressure

PROACTIVE MAINTENANCE IS HOW YOU STOP PAYING REPEATEDLY FOR THE SAME INSTABILITY.

5.6 THE MULTIPLIER EFFECT MIDDLE MANAGEMENT CAN USE

The outline describes a simple multiplier chain:

Proactive Maintenance > Stability > Scalability > Strategic Advantage

STABLE SYSTEMS SCALE BETTER:

- **Easier onboarding**
- **Fewer fragile dependencies**
- **Fewer incidents triggered by routine change**
- **More time available for improvements instead of recovery**

STABILITY CREATES CAPACITY.
CAPACITY IS WHAT GIVES YOU OPTIONS.

5.7 WHAT TO BRING TO A BUDGET CONVERSATION

If you need to make the case in one meeting, bring three things:

1. **A RECURRENCE LIST**
   Top recurring incident classes from the last 90 days, with estimated internal hours spent.
2. **A PREVENTION PLAN**
   For each recurring class, list the prevention action that would reduce recurrence.
3. **A MEASUREMENT COMMITMENT**
   Define how you will measure improvement: fewer repeats, improved response time, improved patch compliance, reduced operational impact.

This moves the conversation from **"we want money for maintenance"** to **"we want to stop paying for the same problems repeatedly."**

LEADERSHIP FUNDS WHAT IT CAN MEASURE.
BUILD THE CASE AROUND RECURRENCE REDUCTION AND EVIDENCE, NOT INTENT.

CHAPTER 6

The Delivery Model

How Proactive Maintenance Becomes an Operating System

HOW PROACTIVE MAINTENANCE BECOMES AN OPERATING SYSTEM

Most pipeline operators have attempted proactive work at some point: a cleanup sprint, a health check, a push to patch more consistently. The program often fades when operational pressure returns because it was never built as a repeatable operating system.

This chapter defines a delivery model that makes proactive maintenance sustainable. The service model describes four stages:

1. ONBOARDING
2. ONGOING SUPPORT
3. DIGITAL EXPERIENCE
4. CONTINUOUS IMPROVEMENT

INTENT DOES NOT SUSTAIN RELIABILITY.
STRUCTURE DOES.

6.1 STAGE 1: ONBOARDING

Establish the baseline and define the rules of the road.

Onboarding is where proactive maintenance either becomes real or becomes "support on demand."

The purpose is to produce:

- A clear baseline of the environment today
- A prioritized view of reliability risks
- An agreed cadence of reviews and monitoring
- Clear ownership and escalation expectations

6.2 STAGE 2: ONGOING SUPPORT

Turn maintenance into cadence, not chaos.

Ongoing support is where proactive maintenance becomes execution: scheduled monitoring, health reviews, hygiene work, and evidence capture.

A practical baseline in the service model is **2 to 4 hours of Enterprise SCADA system monitoring on a twice-weekly basis.** The exact number matters less than the consistency. Cadence creates trend context, and trend context reduces recurrence.

THE MOMENT RELIABILITY WORK LOSES CALENDAR SPACE, INCIDENT WORK FILLS THE GAP.

6.3 STAGE 3: DIGITAL EXPERIENCE

Make reliability visible to operations and leadership

A proactive program gains support when results are visible. Digital experience is how you make progress easy to see and easy to defend:

- Health summaries with clear findings and actions
- Trend reporting that shows drift and improvement
- Simple evidence trails for patch posture, governance, and readiness

IMPROVEMENT IS NOT MEASURED BY TASKS COMPLETED. IT IS MEASURED BY RECURRENCE ELIMINATED.

6.4 STAGE 4: CONTINUOUS IMPROVEMENT

Convert findings into measurable stability

Continuous improvement prevents proactive maintenance from becoming maintenance theatre.

This stage focuses on:

- Converting recurring findings into remediation work
- Reducing repeat incident classes
- Prioritizing improvements that reduce operational drag
- Refining cadence based on trends

The outline frames the multiplier effect clearly:

Proactive Maintenance > Stability > Scalability > Strategic Advantage

6.5 OPERATIONALIZING THE MODEL INTERNALLY

Whether you run this internally or with a partner, the operating requirements are the same:

- A defined cadence
- Clear ownership and escalation
- A prioritized backlog
- A reporting rhythm leadership can understand
- Measures tied to operational outcomes

6.6 DEFINING SERVICE LEVELS WITHOUT CALLING THEM SLAS

Most reliability programs fail because expectations are vague.

Define service levels as operational commitments instead of contractual language:

- **Response expectations:** when an issue is acknowledged and triaged
- **Analysis windows:** when deeper investigation happens, and when findings are reported
- **Escalation triggers:** what qualifies as P1 treatment, and what happens when impact increases
- **Change discipline expectations:** how patches and hotfixes move from plan to execution with rollback readiness

CLARITY ON RESPONSE AND ESCALATION IS HOW YOU PREVENT URGENCY FROM BECOMING YOUR DEFAULT OPERATING MODEL.

6.7 KPIS THAT MATTER FOR PIPELINES

KPIs should translate maintenance into operational confidence.

The outline points to metrics such as response time targets, patch compliance, and customer impact scoring.

Use a short KPI set that leadership can track monthly:

- **Response time trend** (baseline and improvement trajectory)
- **Patch compliance** (planned vs completed)
- **Customer impact score** (operational disruption index)
- **P1 handling speed** (median and worst-case)
- **Recurrence rate** (repeat incidents by class)
- **Redundancy and backup readiness status** (latest validation and findings)

RESPONSE TIME MATTERS, BUT RECURRENCE REDUCTION IS WHERE OPEX IMPROVES.

6.8 BUILD VS PARTNER

This is a capacity decision, not a philosophy.

BUILD INTERNALLY WHEN:

- You have stable staffing and protected time for proactive routines
- You have deep Enterprise SCADA domain expertise across roles
- You can sustain cadence through operational peaks

PARTNER WHEN:

- Your team is overloaded and proactive work is consistently deferred
- You rely on one or two key people to keep the system stable
- You need stabilization without waiting for hiring cycles

THE RIGHT ANSWER IS THE ONE THAT PRODUCES CONSISTENT EXECUTION, EVEN UNDER OPERATING PRESSURE.

CHAPTER 7

Maturity Model

Self-Evaluation Checklist for Proactive Maintenance Readiness

DEXCENT.COM | (833) 482-4100 | SALES@DEXCENT.COM

MOST ORGANIZATIONS DO NOT NEED A COMPLEX SCORING SYSTEM TO UNDERSTAND WHERE THEY STAND.

They need a clear way to identify what is missing, what is inconsistent, and what is strong enough to scale.

This chapter gives you a self-evaluation checklist aligned to the Four Pillars so you can benchmark your current posture and identify what to fix first.

> **MATURITY IS NOT ABOUT HAVING MORE PROCESSES. IT IS ABOUT REDUCING RECURRENCE AND MAKING RELIABILITY REPEATABLE.**

7.1 HOW TO USE THIS CHECKLIST

HOW TO SCORE:

- **0** = not in place
- **1** = partially in place or inconsistent
- **2** = defined, consistently executed, and measured

Answer quickly and honestly. The value comes from what you do next, not the number.

7.2 SELF-EVALUATION CHECKLIST

A) VISIBILITY AND EARLY DETECTION

1. [0|1|2] We review Enterprise SCADA logs on a defined cadence and track recurring warnings and patterns.
2. [0|1|2] We trend alarm behaviour (not just spikes) and investigate drift and recurrence.
3. [0|1|2] We perform routine application perform ance checks and track performance drift over time.
4. [0|1|2] We maintain a routine database hygiene process (cleanup, growth control, unused point identification).
5. [0|1|2] We produce a weekly or bi-weekly health summary with clear findings and action items.

IF YOU CANNOT SHOW TRENDS, YOU ARE FORCED TO ARGUE RELIABILITY FROM MEMORY.

B) STABILITY THROUGH GOVERNANCE AND PATCH DISCIPLINE

1. [0|1|2] We maintain a defined patch and hotfix cadence with planned windows.
2. [0|1|2] We use documented change governance, including expected impact and validation steps.
3. [0|1|2] We have documented rollback procedures for critical changes and we can execute them if needed.
4. [0|1|2] We track patch posture and compliance in a way that can be reported quickly when asked.
5. [0|1|2] We manage version alignment across Enterprise SCADA and associated applications as part of stability, not as a one-off event.

IF PATCHING ONLY HAPPENS WHEN URGENCY FORCES IT, YOU ARE OPERATING IN FORCED CHANGE MODE.

C) PERFORMANCE OPTIMIZATION

1. [0|1|2] We routinely identify slow points and remediate root causes, not just symptoms.
2. [0|1|2] We maintain scripts, ACE, and action sequences with standards and periodic review, not "do not touch" rules.
3. [0|1|2] We refactor high-friction displays and capture best practices to prevent recurring design issues.
4. [0|1|2] We have defined performance thresholds and investigate drift early, before it becomes an operator complaint.

OPERATOR WORKAROUNDS ARE OFTEN THE FIRST SIGN OF PERFORMANCE DEGRADATION.

D) DOCUMENTATION AND REPEATABILITY

1. [0|1|2] We maintain current SOPs for recurring maintenance routines and reliability checks.
2. [0|1|2] We conduct routine redundancy and backup health checks, including confirmation of recovery readiness.
3. [0|1|2] We can produce evidence of maintenance activities and governance without reconstructing it after the fact.
4. [0|1|2] We have a knowledge retention process that survives turnover and does not rely on one person.
5. [0|1|2] We train new team members using documented workflows, not shadowing alone.
6. [0|1|2] We review reliability KPIs monthly and adjust priorities based on trends and recurrence patterns.

DOCUMENTATION IS NOT OVERHEAD.
IT IS WHAT MAKES RELIABILITY REPEATABLE UNDER PRESSURE.

7.3 SCORING AND INTERPRETATION

0 to 15:	Reactive and fragile
16 to 25:	Stabilizing but inconsistent
26 to 34:	Proactive foundation in place
35 to 40:	Predictable reliability by design

7.4 WHAT TO DO WITH YOUR SCORE

IF YOU SCORED 0 TO 15: BUILD CADENCE FIRST

- Schedule monitoring and health review time
- Create a backlog from findings
- Fix one recurring issue class end-to-end
- Capture evidence as you work

IF YOU SCORED 16 TO 25: TIGHTEN STABILITY AND EVIDENCE

- Formalize patch cadence and rollback planning
- Improve governance documentation
- Reduce key-person dependency with SOPs and knowledge capture

IF YOU SCORED 26 TO 34: FOCUS ON PERFORMANCE AND RECURRENCE ELIMINATION

- Prioritize slow points and high-friction operator experiences
- Quantify recurrence reduction by incident class
- Build a quarterly improvement roadmap

IF YOU SCORED 35 TO 40: SCALE AND OPTIMIZE

- Refine KPIs and reporting
- Expand preventative routines
- Build strategic advantage by using stability to accelerate improvements

THE GOAL OF MATURITY IS NOT TO SCORE HIGH.
THE GOAL IS TO ELIMINATE RECURRENCE AND PROTECT OPERATIONAL CONFIDENCE.

7.5 YOUR NEXT BEST STEP

If you want to move quickly, choose one recurring problem class and drive it to completion: **remediate the underlying condition, document the fix, and add the prevention step into your cadence.** That creates evidence, builds internal confidence, and frees time for the next improvement.

ONE SOLVED CLASS OF PROBLEMS BEATS TEN PARTIAL FIXES.

BOOK A PROACTIVE MAINTENANCE STRATEGY SESSION

If you're responsible for AVEVA™ Enterprise SCADA reliability, you do not need another reminder that reactive work is expensive. You need a practical path to reduce repeat incidents, protect operational confidence, and make reliability predictable.

A PROACTIVE MAINTENANCE STRATEGY SESSION IS DESIGNED TO HELP YOU:

- Identify the highest-cost recurring problem classes in your Enterprise SCADA environment
- Pinpoint where drift is creating forced change windows and operational drag
- Define a realistic maintenance cadence your team can sustain
- Align service levels, KPIs, and evidence so reliability is measurable and defensible
- Leave with a clear next-step plan that prioritizes recurrence reduction

THE FASTEST WAY TO IMPROVE OPEX IS TO ELIMINATE THE RECURRING ISSUES THAT QUIETLY CONSUME THE SAME HOURS EVERY MONTH.

Book your strategy session here:
dexcent.com/contact-us

dexcent
STRATEGIZE | TRANSFORM | EVOLVE

STRATEGIZE. TRANSFORM. EVOLVE.

(833) 482-4100 | DEXCENT.COM | SALES@DEXCENT.COM

APPENDIX A:

Proactive Maintenance Inspection Checklist (Practical)

DEXCENT.COM | (833) 482-4100 | SALES@DEXCENT.COM

USE THIS CHECKLIST TO TURN "PROACTIVE" INTO SCHEDULED EXECUTION.

The goal is consistency and follow-through, not perfection.

WEEKLY

ERROR LOG REVIEW

- Review Enterprise SCADA error logs for recurring warnings and errors.
- Capture patterns and open actions for repeat items.

ALARM TREND SPOT-CHECK

- Identify top contributors to alarm noise and drift.
- Flag any trend changes that could become operational drag.

PERFORMANCE QUICK CHECKS

- Validate the responsiveness of key displays and operator-critical paths.
- Note emerging slow points and open remediation actions.

BACKLOG UPDATE

- Prioritize actions by recurrence risk and operational impact.
- Close completed actions with short documentation: what changed, why, and the result.

MONTHLY

PATCH AND HOTFIX POSTURE REVIEW

- Confirm patch cadence, governance steps, and rollback readiness.

DATABASE HYGIENE

- Review growth indicators, unused artifacts, cleanup needs, and any drift that impacts performance.

PERFORMANCE MAINTENANCE

- Deliver one improvement that reduces operator friction (slow-point remediation or display refactoring).

EVIDENCE CAPTURE

- Ensure maintenance actions produce simple proof artifacts: what was checked, what was changed, and the outcome.

QUARTERLY

READINESS VALIDATION

- Validate redundancy and recovery readiness as an operating habit, not an assumption.

GOVERNANCE REVIEW

- Confirm that change governance habits are consistent and evidence is retrievable.

TRAINING AND KNOWLEDGE RETENTION REFRESH

- Update SOPs and reinforce practices that reduce key-person dependency.

THE CHECKLIST MATTERS LESS THAN THE LOOP. FINDINGS MUST BECOME ACTIONS, AND ACTIONS MUST REDUCE REPEAT WORK.

APPENDIX B:

KPI Dashboard Mockup Description

(What It Should Show)

A KPI DASHBOARD SHOULD MAKE RELIABILITY AND COST VISIBLE WITHOUT BECOMING A VANITY REPORT.

Keep it short, trend-driven, and tied to operational impact.

RECOMMENDED DASHBOARD SECTIONS:

1) RESPONSE AND HANDLING

- Response time trend (baseline and improvement trajectory)
- P1 handling speed (median and worst-case)
- Recurrence rate (repeat incidents by class over 30 and 90 days)

2) PATCH AND CHANGE DISCIPLINE

- Patch compliance (planned vs completed)
- Change success rate (changes completed without causing incidents)
- Rollback readiness status (critical change categories)

3) OPERATIONAL IMPACT

- Customer impact score (operational disruption index)
- Operator friction trend (repeated pain points tied to alarms, displays, and latency)

4) RELIABILITY FUNDAMENTALS

- Availability trend (brief incident summaries only)
- Redundancy validation status (latest validation date and findings)
- Backup and recovery readiness status (latest confirmation and issues)

RESPONSE TIME IS VISIBLE.
RECURRENCE REDUCTION IS WHERE OPEX IMPROVES.

APPENDIX C:

High-Level AVEVA Enterprise SCADA Architectural Diagram Description

(RSA-aligned)

DEXCENT.COM | (833) 482-4100 | SALES@DEXCENT.COM

THIS APPENDIX DESCRIBES WHAT A HIGH-LEVEL ARCHITECTURAL DIAGRAM SHOULD COMMUNICATE AT A CONCEPTUAL LEVEL.

The goal is clarity on redundancy and resiliency, not an exhaustive technical design.

A HIGH-LEVEL DIAGRAM SHOULD SHOW:

- A Primary Data Centre (PDC) hosting Enterprise SCADA core services
- A Secondary Data Centre (SDC) designed to support resiliency, typically mirroring core architecture concepts
- RealTime services are configured for redundant behaviour
- Historical services implemented with resilience concepts such as redundancy and data protection strategies
- The relationship between server environments and operator consoles, recognizing that operator consoles may be geographically separate depending on the control center and data center layout

REDUNDANCY IS ONLY A RELIABILITY CAPABILITY WHEN IT IS MAINTAINED, VALIDATED, AND OPERATIONALLY READY.

APPENDIX D:

Glossary of SCADA Terms

DEXCENT.COM | (833) 482-4100 | SALES@DEXCENT.COM

AVEVA™ Enterprise SCADA (formerly OASyS)

A SCADA platform used in pipeline operations environments; RSA materials reference OASyS operator console configurations and architecture concepts.

OASyS

Legacy naming Open Architecture System referenced in RSA context for operator console and system architecture discussions.

RealTime (Service / Database)

The real-time data layer supporting live values and operational visibility, configured for redundant behaviour in RSA reference patterns.

Historical Service

The layer responsible for historical data storage and retrieval, supported through resilience concepts in RSA reference patterns.

HMI (Human Machine Interface)

Operator interface for monitoring and control, where performance and display behaviour affect operational decision-making.

PDC / SDC

Primary Data Centre and Secondary Data Centre concepts supporting resiliency and business continuity in Enterprise SCADA environments.

PHMSA

Pipeline and Hazardous Materials Safety Administration (USA), a regulatory context referenced in RSA materials.

API RP 1165

A recommended practice referenced in RSA regulatory readiness context connected to SCADA display considerations.

API 1167 / API 1168

Standards referenced in RSA readiness context are tied to alarm management and control room management practices.