Setting the Standard for Automation™

Beyond Modbus: Designing SCADA With Other Open Protocols

Jacob Brodsky, PE
Jacobs

2018 ISA Water/Wastewater & Automatic Controls Symposium (WWAC)
8-9 August 2018, Bethesda, Maryland USA

Copyright 2018. ISA All rights reserved. www.isa.org
No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

Agenda

- The Limitations of Real Time Reporting
- Real Time Vs. Event Reporting
- Performance Differences
- Object Orientation
- Authentication
- The Advantages of Standards-Based SCADA

Copyright 2018. ISA All rights reserved. www.isa.org
No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

Backdrop Issues

- Water Utility Experience over past 30 years:
  - Number of points doubles every five years
  - RTUs get “fatter”
    - More Features
    - More points
- Changing Telecom Infrastructure
- Need More Security

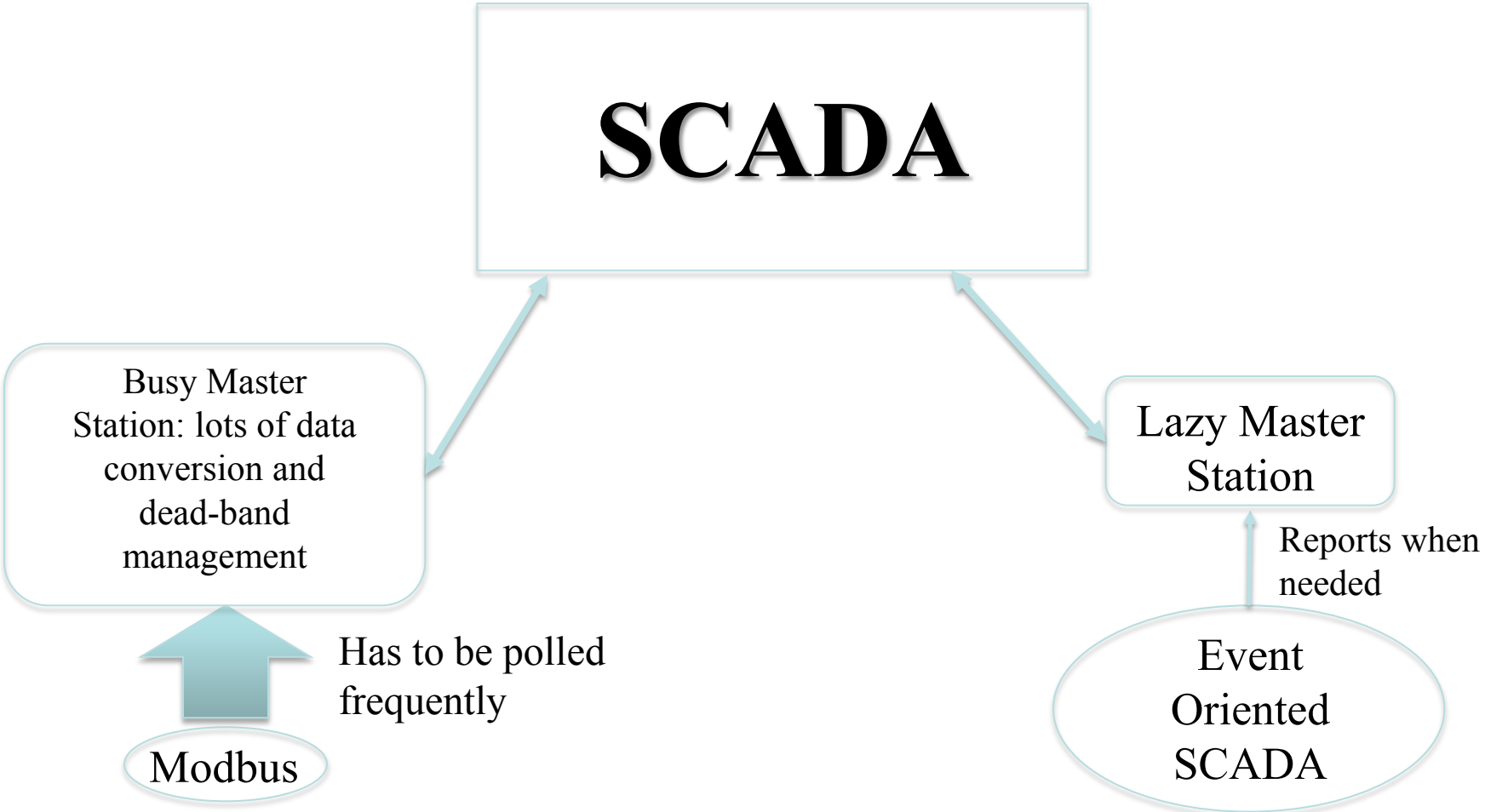
Copyright 2018. ISA All rights reserved. www.isa.org
No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

Modbus is a Thin Standard

Protocol	ModbusRTU	DNP3 (Serial)
Transport Layer	CRC every 253 bytes or less	CRC every 16 bytes or less
Commands	User-defined and Well-Known	No User Defined Commands
Data	16 Bit words and single bit states	Huge library of standard objects
Multi-Master	Yes	Complicated, but Possible
Time-Stamping	Make up your own	Part of Object Definitions
Endianness	Whatever Floats Your Boat	Little Endian Only

Copyright 2018. ISA All rights reserved. www.isa.org
No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

Compatibility



Copyright 2018. ISA All rights reserved. www.isa.org
No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

Real Time Reporting

- Simple: Ask what it is
  - It tells you what the readings are right now
  - No concept of time
- Must poll at least twice the rate of the shortest event time capture (Nyquist Theorem)
- Does not scale up well

Copyright 2018. ISA All rights reserved. www.isa.org
No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

Event Based

- Ask it what's new
  - Reports whatever is "notable"
  - Time is a component of the event
- More complicated at RTU end
- Can poll at whatever rate is adequate
- Scales up better
- Can still capture very fast events and report

Copyright 2018. ISA All rights reserved. www.isa.org
No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

Which is Better?

- Real Time:
  - Small Point Count
  - Simple Data Types
  - Simple functions
- Event Oriented:
  - Larger Point Count
  - Does NOT need to be polled at Nyquist Limit
  - Can show detail between reports
  - Complex Data Types
  - Expects local controls and automation
  - Irregular communications not a problem

Copyright 2018. ISA All rights reserved. www.isa.org
No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

What Triggers an Event?

- Change in Value
  - Deadband Types:
    - Absolute
    - Relative
    - Integrated
    - Swinging Door
    - Your idea goes here
- Timed Snapshot
  - Counters use these
    - Example: Tipping Bucket Rain Gauge
  - Volumetric calculations might use it
- Manual Request

Copyright 2018. ISA All rights reserved. www.isa.org
No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

OPC-DA Mapping

- OPC DA is a common driver API for most SCADA systems
- It was designed around real time protocols
- Event Oriented protocols may have an older time stamp than the arrival time
- OPC DA has no place to put that original time stamp
  - Everyone makes up their own method for handling the field time stamp

- Avoid using OPC-DA drivers with Event Oriented Protocols

Copyright 2018. ISA All rights reserved. www.isa.org
No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

Object Orientation

- Events include
  - Reported value
  - Data Quality/Flags
  - Time/Date
- Fundamental Data Types
  - State
  - Raw Analog Value (usually 16 bit register)
  - 32 bit counters
  - Floating Point Calculations
    - Local Volumetric Derived Flow
    - Scaled values
  - Strings

Copyright 2018. ISA All rights reserved. www.isa.org
No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

Authentication

- Data Provenance is becoming a larger concern
- Authentication proves the data and/or Command came from an authentic source
- Event Oriented Protocols can authenticate without the additional latency affecting the time stamp

Copyright 2018. ISA All rights reserved. www.isa.org
No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

Open Standard Protocol Advantages

- Portability
  - Data formats are well defined
  - Smoother System upgrades
  - Not tied to any one vendor
- Staff Training
  - Third party technical help can resolve problems
  - Training is readily available
  - Protocol can be discussed openly
- Open Source Software exists

Copyright 2018. ISA All rights reserved. www.isa.org
No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

For More Information:

JACOBS NSS – Sr. ICS Cybersecurity Engineer
Name: Jacob Brodsky, P.E.
Phone: (443) 285 -3514
Email: Jacob.Brodsky@jacobs.com

JACOBS®