RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: PS-F01

SDLC and 62443: Build It In, Don't Bolt It On

Shoshana Wodzisz

Global Product Security Leader
Rockwell Automation
@slwodzisz

Rockwell Automation

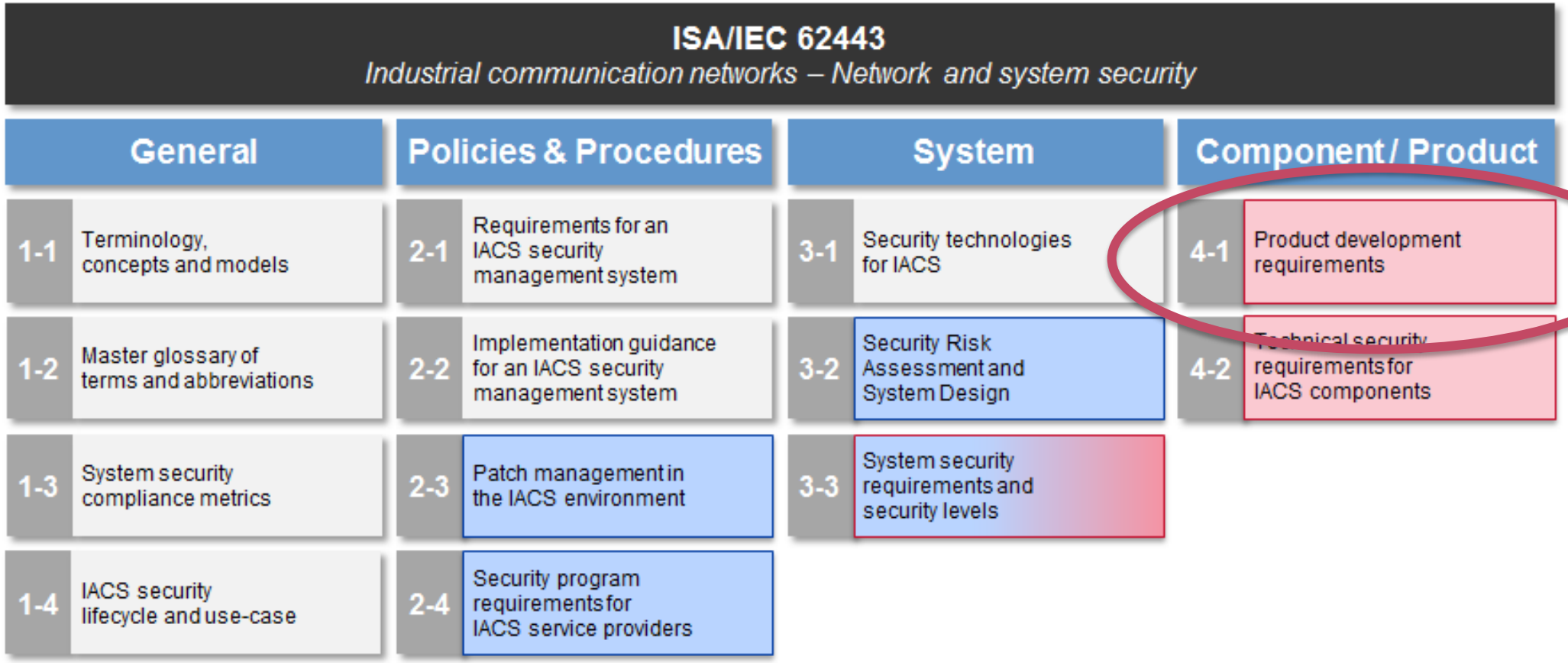
Rockwell Automation

What is IEC 62443?

Series of global standards that define requirements for implementing electronically secure Industrial Automation and Control Systems (IACS). It covers the entire lifecycle of a product.

In other words:	**International Standard** **Cybersecurity** **Industrial Control Systems**
Customers care because:	**Globally recognized standard** **Independently certified** **They now know what to ask for**

IEC/ISA 62443



Defense in Depth

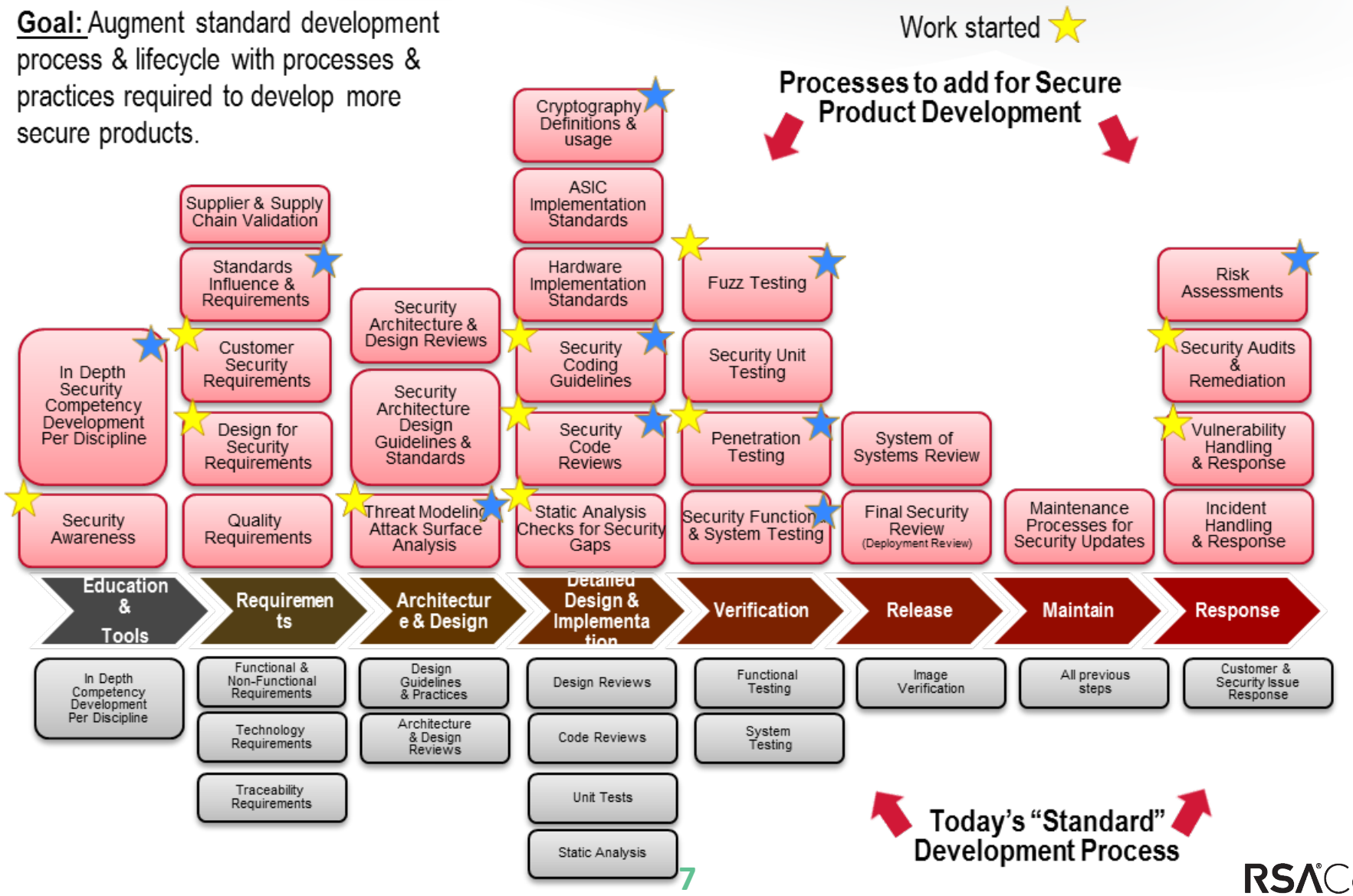
Risk Transference

How do companies start on the security journey ?

- Extra time they don’t know what to do with
- Value process over delivering products
- Love paying taxes
- Idolize Microsoft and their SDLC
- Industry standards
- Customer requests

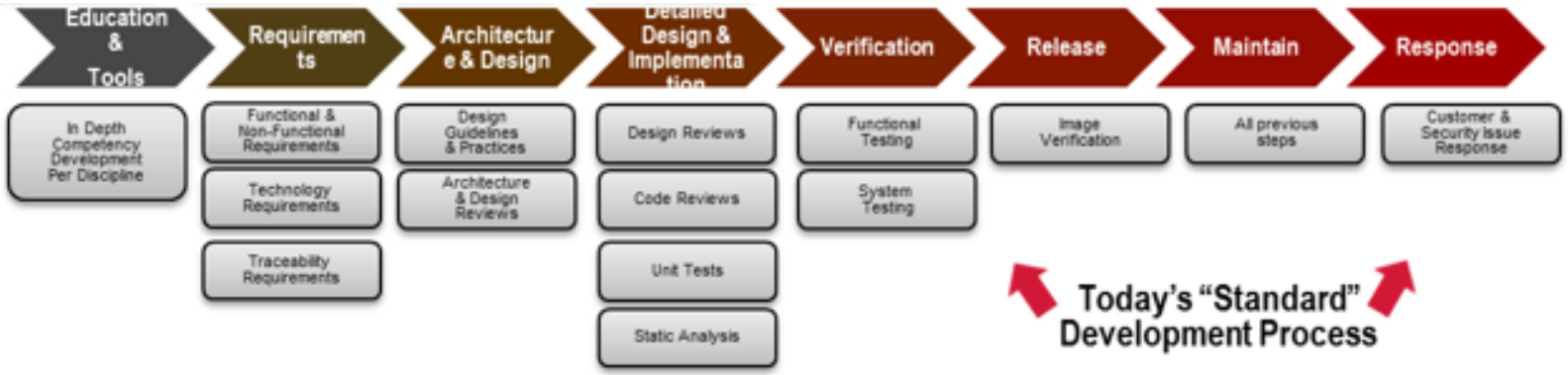
We started using the "Bolt On" method

Goal: Augment standard development process & lifecycle with processes & practices required to develop more secure products.



To add Security to your Development Process ….

You must have development processes to start with



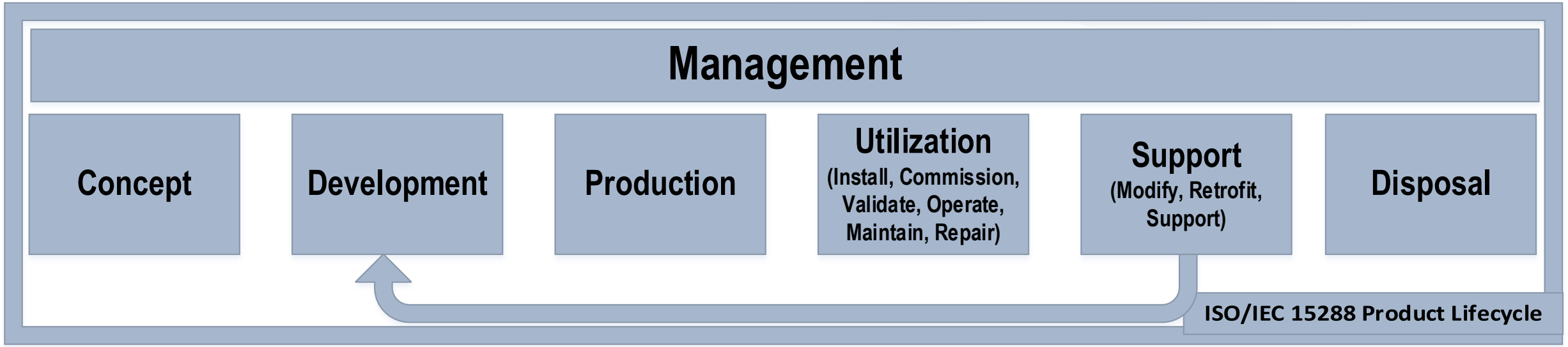
We do have development processes…..lots of them !!

We found that they were essentially all the same.

RSAConference2020

Our SDLC Evolution

Started with a Framework



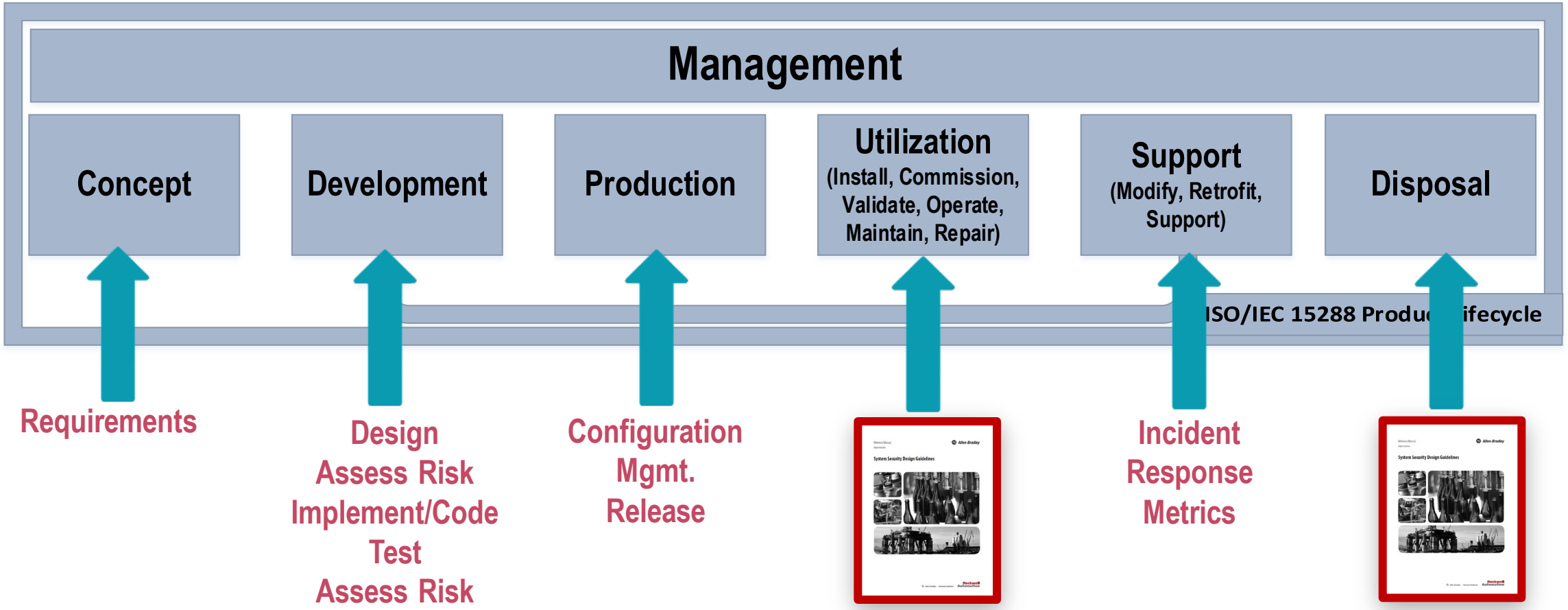
Product Lifecycle: Concept → Disposal

not just "development"

ISO/IEC 15288:2015 Systems and Software Engineering System Life Cycle Processes

Processes in the Framework

Reviews, Audits, Supply Chain, Skills/Training, Dev Environment, Governance

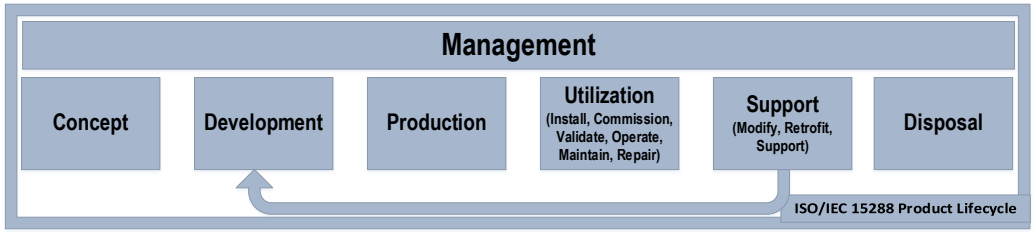


Defined the processes

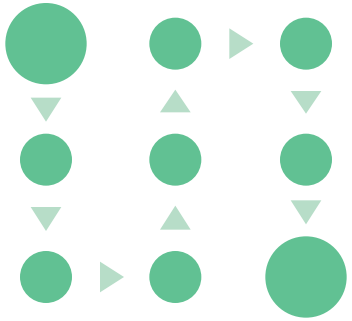
- Leveraged 24774 as guidance to developing a process
- Focused on activities and tasks
- Created a process template for the teams to use
- Wrote processes based on industry and internal best practices
- Etc.

ISO/IEC TR24774 Systems and software engineering – Life cycle management – Guidelines for process description.

Ideas & Theories



Frameworks



Consistent Processes

We really started here
Just above the details

The Nitty Gritty
Engineering Details

RSAConference2020

How we really built security in

Cultural "Experiences"

- "We already do this today – just clean up a few processes and get them certified!"
- "Make sure all groups have a voice and buy-in"
- "We do development differently than all other groups in the company – **our** products are different"
- "We already have processes, let me show you my 8 tab excel checklist."
- "We have a **stage gate process**. Get it – it's our process !"

Company Policy	Security is not optional.
Processes	Activities and tasks (IEC TR 24774)
Templates	Consistency in outputs
Job Aids Work Instructions Procedures	How we do our work
Checklists	Things we often forget

A note on process development

- Besides understanding what a Process is, these specific areas continue to trip people up
  - **Outcome of a Process** – what would it look like if the process were successfully executed?
    - Not: The design is signed off
    - Yes: Multiple design options are considered, documented, and communicated to help ensure that future engineers know why a design option was NOT chosen
  - **Roles and Responsibilities** – why are some roles involved in the process?
    - Not: Moderator: to moderate the review process
    - Yes: Moderator: to ensure that all aspects of the review are sufficiently covered, that time is allocated to do an effective review, and that all issues are dispositioned in a timely manner.

Timeless

Fluid

Company Policy

Processes

Templates

Job Aids
Work Instructions
Procedures

Checklists

Abstract out activities and tasks that are industry best practices, and do not change often.
Built in security and functional safety.

Allow (expect) teams the autonomy to define how they execute on the processes, what tools they use, and sometimes what order to do things in.

Company Policy

Processes

Focus our 62443-4-1 certification on the true common practices across the company.

Templates

Job Aids
Work Instructions
Procedures

Checklists

Keep the HOW out of the certification discussions. These are execution details.

The Results

- “Yes, those are the things we do when we design a product”
- “Thank you for not telling us how to do our day-to-day job”

- “Are you kidding, OMG, all of this is going to extend our project schedules by 20%!”
- “We do agile so……” (this seems to be a common answer)
- “We already have a (stage gate) process, why do we need this?”

"You are already following a large percentage of the best practices defined – and doing them well."

Expected Gap Analysis Results

More Results & Experiences

- The “textbook” or 15288/24774 definition of a process isn’t commonplace. And that is good and OK.
- But following a checklist “Did you do this?” “Did you do this?”, etc. isn’t a process either.
  - Did you do your requirements ? Check.
  - Did you do your design ? Check.
  - Did you think about security ? Check.
- Processes explain WHY the activity is important.
  - Understanding the context the component is used in provides ….
  - A security role in a review is to ensure….

Where do we go from here?

- We are still in the rollout, training, & evangelism stage
  - Why a checklist or template isn't a process
  - How a development process is different from a stage gate process
  - Please just try it, I suspect you will like it
  - How this will ease your journey to IEC 62443 certification
  - These are base lifecycle processes – security is a fraction of the content
- Building influencers in the company at all levels
- Getting into a cadence of continuous improvement

Apply What You Have Learned Today

- Next week you should:
  - Learn more about 62443 if you are in the ICS space. Lots of information on the internet available prior to purchasing the standard itself.
  - Browse through IEC/ISA 15288:2015 and IEC TR24774.
- In the first three months following this presentation you should:
  - Take an inventory of the number of product lifecycle or development “processes” your company has.
  - Evaluate if they are a mixture of process, templates, checklists, and job aids.
- Within six months you should:
  - Engage members from all functions and business units to abstract out the real “processes”.
  - Teams should create or update their own work instructions to reflect how they do their work.